Cyberoperaties en de EU

Een eerste stap naar strategische autonomie?

Peter B.M.J. Pijpers en Paul A.L. Ducheine*

FOTO EUROPESE COMMISSIE

'What's past is prologue.'[1]

Te midden van de geopolitieke spanningen klinkt de oproep dat ook de Europese Unie een vuist moet kunnen maken als het nodig is. 'Soft power is no longer enough', zei EU-buitenlandchef Josep Borrell. De evacuatie uit Afghanistan was de druppel waardoor de notie van een 'Europees leger' wederom op de agenda staat. Maar zit de kracht van de EU, in tegenstelling tot de NAVO, niet eerder in economische en diplomatieke dan in militaire macht? Bovenal is het de vraag of een toekomstig conflict wel een traditioneel kinetisch treffen zal zijn, of dat de nadruk zal liggen op hybride conflicten in de informatieomgeving (inclusief cyberspace). Hervorming van het veiligheidsdenken in de EU, inclusief meer strategische autonomie, is goed, maar de EU zou dat vanuit haar eigen kracht moeten doen en zich vooral richten op de trend van de toekomst, niet op de geest van het verleden.

Wanneer de Taliban zich in de zomer van 2021 heer en meester maken van Afghanistan, en buitenlandse vertegenwoordigers – militair en civiel – dwingen het land in hoog tempo te verlaten,[2] laait eens te meer de discussie op of de Europese Unie niet (permanent) een eigen krijgsmacht moet hebben.[3] Bij de evacuatie van landgenoten waren de Europese landen immers sterk afhankelijk van de Verenigde Staten. Bovendien was er een gebrek aan synergie door de unilaterale inzet van Europese landen.[4]

Maar is de oproep voor een 'Europees leger'[5] niet eerder te interpreteren als een oproep voor een grotere mate van strategische autonomie van de EU? Een wens die zeker leeft nadat de EU werd uitgesloten bij de besprekingen over de oplopende spanningen voorafgaande aan de oorlog in Oekraïne. Rusland wilde daarbij enkel met de VS of de NAVO praten.

In het Europese denken over strategische autonomie is echter een tegenstrijdige ontwikkeling zichtbaar. Hedendaagse conflicten, zoals de cyberaanvallen op Baltische staten of in de aanloop naar de oorlog in Oekraïne, verschillen van traditionele kinetische conflicten. De ontwikkeling in de aard en intensiteit van conflicten is daarmee aan het divergeren. En dat terwijl de EU en de NAVO juist naar elkaar toe lijken te bewegen of, zeker bij de roep om een Europees leger, deels overlappen.

De Adviesraad Internationale Vraagstukken (AIV) spreekt over een kantelend perspectief,[6] de impliciete taakverdeling tussen NAVO (voor afschrikking en territoriale verdediging) en EU (voor wederopbouw en civiel-militaire missies) wordt losgelaten. Een herbezinning kan geen kwaad, maar de vraag is welke kant het perspectief op moet? Die vraag is vooral relevant als in toekomstige conflicten de nadruk meer komt te liggen op hybride optreden waarbij confrontaties

* Kolonel dr. Peter B.M.J. Pijpers is universitair hoofddocent Cyber Operaties aan de Nederlandse Defensie Academie. Van 2015-2018 was hij gedetacheerd bij de Europese Dienst voor Extern Optreden (EDEO). Brigadegeneraal prof. dr. Paul A.L. Ducheine is hoogleraar Cyber Operaties aan de Nederlandse Defensie Academie en bijzonder hoogleraar Recht van Militaire Cyber Operaties aan de Universiteit van Amsterdam.

1 William Shakespeare, *The Tempest*, 2e Akte, 1e scène.

2 Hanneke Chin-A-Fo en Steven Derix, 'Zo verliep de chaotische evacuatie uit Kabul', *NRC Handelsblad*, 13 september 2021.

3 Romana Abels, 'Europa wil nu een eigen leger', *Trouw*, 23 augustus 2021.

4 Damijan Fiser, 'Defence Ministers Discuss How to Boost EU Defence', Slovenian Presidency of the Council of the EU, 2021. Zie: https://slovenian-presidency.consilium.europa.eu/en/news/defence-ministers-discuss-how-to-boost-eu-defence/.

5 De oproep voor een Europese krijgsmacht is in de media veelal betiteld als een Europees leger. Hoewel een leger ook refereert aan landstrijdkrachten, hanteren wij in dit artikel toch de notie Europees leger.

6 Adviesraad Internationale Vraagstukken, 'Europese veiligheid: tijd voor nieuwe stappen', 2020, 23-24.

in de informatieomgeving (waaronder cyberspace) niet als alternatief maar juist zij aan zij met traditionele fysieke activiteiten, inclusief kinetisch treffen, plaatvinden.

Dit artikel behandelt, vanuit een internationaal rechtelijk perspectief, de vraag of en in hoeverre de EU en de NAVO verschillen in verdedigingsmogelijkheden, in het bijzonder tegen cyberoperaties, en of de strijd tegen cyberoperaties wellicht een kans is voor de EU om een strategisch autonome positie in te nemen, weg van de traditionele kinetische conflicten.

Eerst komt de vraag aan de orde hoe een Europees leger te duiden is, gevolgd door het veiligheidsdenken bij de NAVO en EU. Vervolgens wordt kort aangegeven wat de implicaties zijn van cyberspace voor collectieve veiligheid, waarna een analyse volgt over de verdedigingsopties van de NAVO en de EU in cyberspace. Daarbij wordt een onderscheid aangehouden naar 1) een cyberaanval als een gewapende aanval, 2) een aanval met gebruik van geweld, 3) en een daad onder het niveau van geweld. Na de conclusie volgt een reflectie op de positie van de EU in cyberspace en op de vraag of het EU-cyberbeleid een opmaat kan zijn voor een sterkere strategische autonomie.

De duiding van een Europees leger

De discussie over een Europees leger, al dan niet ingebed in een Europese Politieke of Defensiegemeenschap, leeft al sinds 1950.[7] Net als de vraag wat die notie precies inhoudt.

Waar het in 1950 om een daadwerkelijk Europees leger ging, onder meer om de heroprichting van het Duitse leger in te bedden, gaat het tegenwoordig veeleer, net als bij de VN en de NAVO, om een concept of denkraam.[8] De NAVO heeft weliswaar een gezamenlijke 'command structure', maar geen eigen leger; de 'force structure' (de legers) zijn soevereine middelen van de individuele bondgenoten.[9] Deze 'force' is, op basis van een soeverein besluit van

7 Theo Brinkel en Trineke Palm, 'De actualiteit van de Europese Defensiegemeenschap (1950-1954). Vreemd en fantastisch?', in: *Militaire Spectator* 191 (2022) (1) 8-17.

8 Alhoewel Artikel 45 en 46 van het VN-Handvest wel verwijzen naar een 'immediately available' 'armed force' is dit nooit verwezenlijkt.

9 De NAVO heeft in haar Command Structure meerdere hoofdkwartieren op strategisch, operationeel en tactisch niveau. Daarnaast heeft de NAVO een systeem van snel beschikbare eenheden (forces) onder meer in de NATO Response Force (NRF), oplopend tot 30.000 militairen. De EU heeft ook een 'Command Structure', ingebed in de EDEO en een EU Battle Group. Beide zijn substantieel kleiner dan de NAVO-capaciteit.

de lidstaten, in te zetten voor de NAVO, de VN, een *coalition of the willing*, of voor EU-missies. De soevereine flexibiliteit van deze 'single set of forces'-gedachte staat haaks op het permanent alloceren van schaarse gevechtskracht bij een van deze internationale organisaties.[10]

De politiek-strategische context is bovendien sinds de oprichting van de NAVO in 1949 danig veranderd. Daarnaast erodeert de relatie tussen de VS en de Europese NAVO-bondgenoten. Europese landen hebben altijd zwaar geleund op de nucleaire afschrikking van de VS en onvoldoende reciprociteit ten toon gespreid. Daar komt bij dat de Amerikaanse dreigingsanalyse zich de laatste jaren richt op de Aziatische regio in de Stille Oceaan. De VS richt zich daardoor minder op de NAVO en Europa, wat in Europees verband heeft geleid tot het nadenken over een grotere strategische autonomie, zoals weergegeven in de *EU Global Strategy* van 2016.[11]

De oproep voor een Europees leger is daarmee vooral te interpreteren als een oproep voor een grotere mate van strategische autonomie van de EU. Dit houdt in dat de EU in staat moet zijn zelfstandig, met gebruikmaking van de gecoördineerde inzet van middelen van (individuele) lidstaten, een militaire inzet te plannen en uit te voeren.[12] Het gaat daarbij dus veel eerder om het integreren van de bevel- en commandovoeringssystemen en het gezamenlijk garanderen van benodigde militaire middelen, dan om een staand leger van 60.000 militairen én materieel.[13]

10 Het Strategisch Kompas spreekt van *Rapid Deployment Capacity* van 5.000 militairen. Council of the European Union, 'Strategic Compass for Security and Defence', *EU RELEX 7271/22*, no. March (2022), 14.

11 European Union, 'Shared Vision, Common Action: A Stronger Europe – A Global Strategy for the European Union's Foreign And Security Policy', *European Union*, 2016, 20.

12 Voor meer achtergrond hierover zie: Luis Simón, *Command and Control? Planning for EU Military Operations*, *Occasional Paper EU ISS*, 2010; Council of the European Union, 'Taking Forward the EU's Comprehensive Approach to External Conflict and Crises – Action Plan 2015', *Joint Staff Working Document 7913/15*, 2015.

13 De oorsprong van dit getal komt uit de Helsinki Verklaring van de EU naar aanleiding van de zogeheten Petersbergtaken. Zie: WEU Council of Ministers, 'Petersberg Declaration', 1992.

Amerikaanse schepen in de Filipijnse Zee. De VS richt zich meer op de Aziatische regio en minder op de NAVO en Europa, wat in Europees verband heeft geleid tot het nadenken over een grotere strategische autonomie

FOTO U.S. PACIFIC FLEET

Traditioneel veiligheidsdenken bij NAVO en EU

De NAVO is een intergouvernementele organisatie,[14] opgericht in 1949 om de notie van collectieve veiligheid gestalte te geven, vooral in relatie tot de Sovjet-Unie en het Warschaupact. Collectieve verdediging, zoals verwoord in Artikel 5 van het Noord-Atlantisch Verdrag (NAV), is de hoeksteen van dit collectieve veiligheidssysteem waarbij de Europese NAVO-partners zwaar leunen op het nucleaire vermogen van de VS.[15]

Bij de EU is de collectieve verdediging, zoals neergelegd in de 'wederzijdse bijstandsclausule' in Artikel 42(7) van het Verdrag van de Europese Unie (VEU), eerder de laatste loot aan de veiligheidstak. De EU is opgericht om via onderlinge (economische) afhankelijkheden conflicten tussen staten te minimaliseren. De Europese Gemeenschap voor Kolen en Staal (EGKS) van 1952 en de Europese samenwerking op het gebied van atoomenergie (Euratom) zijn functioneel van aard en meer gestoeld op interdependentie dan op harde *realpolitik*. De EU is in essentie een supranationale organisatie waarbij de lidstaten delen van hun soevereiniteit, onder meer op het gebied van economie en financiën, hebben overgedragen. Daarnaast heeft de EU ook een intergouvernementeel deel om de functionele samenwerking op het gebied van buitenlandse zaken, defensie en rechtshandhaving vorm te geven.

Hoewel de NAVO en de EU in thematiek en lidmaatschap deels overlappen, verschillen de organisaties fundamenteel in oorsprong, wat doorsijpelt in het veiligheidsdenken. Strategische autonomie bij traditionele veiligheidsvraagstukken is voor de EU daarom gemakkelijker gezegd dan gedaan. EU-landen missen, voor de inzet bij grootschalige of specialistische militaire operaties,[16] belangrijke capaciteiten zoals strategisch (lucht)transport, geïntegreerde inlichtingen,[17] *command & control*-capaciteit, en logistiek inclusief *air-to-air*

In het Europese gedachtengoed daalt het veiligheidsdomein langzaam in, denk daarbij aan de oprichting van het European Defence Agency (EDA), de 46 projecten (waaronder meerdere cyber-gerelateerde) in het kader van de Permanent Structured Cooperation (PESCO),[I] of de instelling van het Europees Defensie Fonds. Met het Verdrag van Maastricht (1993) – waarbij Euratom, EGKS en de Europese Economische Gemeenschap tot één Europese Gemeenschap (EG) werden samengevoegd – is daarnaast een separaat Gemeenschappelijk Buitenlands- en Veiligheidsbeleid (GBVB) ingesteld. Dit fungeerde naast het (sluimerende) systeem van Europese collectieve veiligheid zoals neergelegd in het verdrag van Brussel van 1948 en de daarbij opgerichte West-Europese Unie (WEU).[II] Met het Verdrag van Lissabon (2009) – waarbij de EG overging naar de EU – zijn de GBVB- en WEU-taken grotendeels samengegaan en, in 2012 na het opheffen van de WEU, opgenomen in titel V van het VEU,[III] inclusief de wederzijdse bijstandsclausule van Artikel 42(7).

I PESCO Secretariat, 'PESCO: Member States Driven', 2021. Zie: https://pesco.europa.eu.

II J.F.R. Boddens Hosang en Paul A.L. Ducheine, 'Implementing Article 42.7 of the Treaty on European Union: Legal Foundations for Multual Defence in the Face of Modern Threats', *ACIL*, no. Research Paper 2020-71 (2020), 3-4. Zie: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3748392. De WEU is sinds 1949 overschaduwd door de NAVO.

III Europese Unie, 'Verdrag Betreffende de Europese Unie (Geconsolideerde Versie)', C326/13 Publicatieblad van de Europese Unie, 2012. Titel V luidt: 'Algemene bepalingen inzake het extern optreden van de Unie en specifieke bepalingen betreffende het Gemeenschappelijk Buitenlands en Veiligheidsbeleid'.

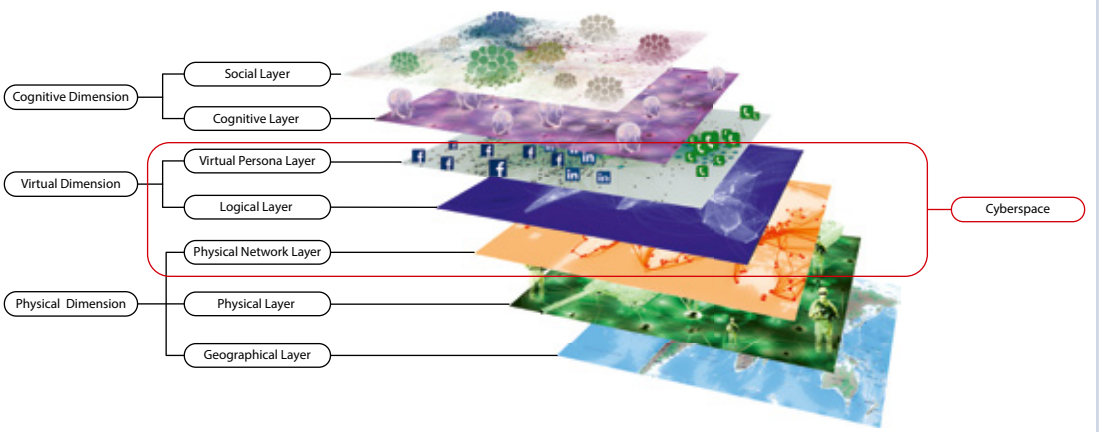
14 Intergouvernementeel houdt in dat landen als soevereine entiteiten samenwerken, terwijl bij supranationaliteit een deel van de soevereiniteit is overgedragen aan een internationale organisatie.

15 Naast collectieve verdediging is de NAVO ook belast met crisismanagement en coöperatieve veiligheid. Hierbij gaat het om het uitvoeren van expeditionaire militaire missies en het samenwerken met partnerlanden. Zie: North Atlantic Treaty Organisation, 'Warsaw Summit Communiqué', juli 2016, bullet 2.

16 Zoals KFOR, ISAF, Enduring Freedom, SFIR en Iraqi Freedom.

17 Zie AIV, 'Europese Veiligheid : Tijd Voor Nieuwe Stappen', 20; Ilkka Salmi, 'Why Europe Needs Intelligence and Why Intelligence Needs Europe: "Intelligence Provides Analytical Insight into an Unpredictable and Complex Environment"', *International Journal of Intelligence and CounterIntelligence* 33 (2020) (3) 464-470.

Cyberspace is een domein waarin actoren met elkaar communiceren, concurreren en waar nodig conflicten uitvechten, net als in het land, maritieme, lucht- of ruimtedomein. Cyberspace is dus geen instrument of 'wapen', maar maakt met de andere domeinen deel uit van de informatieomgeving. Die laatste bestaat uit een fysieke, een virtuele en een cognitieve dimensie.[18]



Cyberspace omvat drie lagen uit de informatieomgeving: (1) de fysieke netwerklaag (hardware, computers, routers), (2) de logische laag ofwel de virtuele objecten (data, software, applicaties) en (3) de virtuele identiteiten ofwel virtual-personalaag (zoals socialemedia-accounts).

18 Paul A.L Ducheine en Jelle van Haaster, 'Cyber-Operaties en militair vermogen', in: *Militaire Spectator* 182 (2013) (9) 368-387; Willemijn A. Bos en Peter B.M.J. Pijpers, 'Cyberoperaties in de gray zone. Juridische overwegingen omtrent de rol voor de krijgsmacht', in: *Militaire Spectator* 190 (2021) (10) 511-513.

Figuur 1 Informatieomgeving en cyberspace[21]

refuelling. De EU is daarvoor vooralsnog afhankelijk van niet-EU NAVO-bondgenoten zoals de VS en in mindere mate het Verenigd Koninkrijk. Dat verklaart mogelijk het EU-standpunt dat *soft power* alleen niet genoeg is en waarom zij naarstig op zoek is naar *hard power*-capaciteiten.[19]

Cyberspace en cyberoperaties

De EU mist specifieke capaciteiten om effectief te zijn in traditionele kinetische conflicten, maar de vraag is of toekomstige confrontaties vergelijkbaar zijn met (traditionele) veiligheidsvraagstukken uit het verleden? De crux van een menselijk conflict – de wil opleggen aan de ander – is niet veranderd door de komst van hybride oorlogvoering,[20] of de confrontaties en competitie in de informatieomgeving en cyberspace, maar de aard en intensiteit van de conflicten zijn dat hoogstwaarschijnlijk wel.

Activiteiten in cyberspace richten zich enerzijds op de lagen in cyberspace zelf, zoals het vernietigen of veranderen van de software of data met aanzienlijke gevolgen, ook (indirect) in de fysieke omgeving. Denk daarbij aan de Stuxnet-aanval op de Iraanse nucleaire verrijkingszinstallaties in de periode 2007-2010,[22] of het platleggen van het Oekraïense elektriciteitsnetwerk in 2015 en 2016.[23] Naast deze zoge-

19 Josep Borrell en Thierry Breton, 'For a United, Resilient and Sovereign Europe', European Commission, 2020).

20 Robert Johnson, 'Hybrid Warfare and Counter-Coercion', in: *The Conduct of War in the 21st Century*, 2020.

21 Figuur is samengesteld door Van Haaster, voor de ontstaansgeschiedenis zie voetnoot 898 uit: Jelle van Haaster, 'On Cyber: The Utility of Military Cyber Operations During Armed Conflict' (2018)173.

22 Jon R. Lindsay, 'Stuxnet and the Limits of Cyber Warfare', in: *Security Studies* 22 (2013) (3) 365-404.

23 Robert Lee, Michael Assante en Tim Conway, 'Analysis of the Cyber Attack on the Ukrainian Power Grid', *SANS Industrial Control Systems Security Blog*, 2016.

Het verleden is qua conflictvormen niet de voorbode van de toekomst. Toekomstige conflicten zijn eerder een (hybride) samengaan van confrontaties in het spectrum tussen oorlog en vrede

noemde *hard cyber*-operaties, kunnen ook acties *via* cyberspace plaatsvinden die een effect hebben op de cognitieve dimensie.[24] Deze zogeheten *soft cyber*-operaties beïnvloeden mensen of groepen via het manipuleren van informatie.[25] *Soft cyber*-operatie zijn enerzijds te zien als traditionele psychologische operaties die nu via cyberspace plaatsvinden.[26] Anderzijds zijn ze van een geheel andere omvang door de snelheid waarmee berichten verspreiden, het gemak waarmee actoren tot cyberspace toetreden, het bereik en de penetratiegraad van de berichten die via cyberspace worden verspreid. Denk hierbij aan het beïnvloeden van de Amerikaanse presidentsverkiezingen van 2016 en 2020.[27]

Cyberoperaties, in het bijzonder digitale beïnvloedingsoperaties, zijn fundamenteel anders dan kinetische operaties en verre van 'traditioneel'. Cyberoperaties vinden over het algemeen al plaats voorafgaand aan een gewapend conflict, zoals recentelijk in Oekraïne. Cyberoperaties zijn daarnaast niet langer het prerogatief van statelijke actoren: óók niet-statelijke actoren manifesteren zich. Het is daarbij soms onduidelijk welke kwaadwillende actor optreedt en vanuit welk land, waardoor interne en externe veiligheidsvraagstukken in elkaar overlopen. En als de actor al bekend is, is deze lastig te attribueren aan een specifieke staat.[28] Ook de grens tussen oorlog en vrede vervaagt omdat ongewenste inmenging veelal plaatsvindt zonder daarbij de drempel van (fysiek) geweld – zoals bedoeld in het interstatelijke geweldsverbod van Artikel 2(4) van het VN-Handvest – te overschrijden.[29]

Verdedigingsopties in cyberspace

De opkomst van (operaties in) cyberspace is illustratief voor de veranderende veiligheidsdreiging sinds het oprichten van de NAVO en de EU; zeker na het einde van de Koude Oorlog. Cyberspace laat grenzen letterlijk en figuurlijk vervagen. Hierdoor ontstaat een diffuse en hybride situatie die soms is aangeduid als 'de permanente staat van competitie',[30] wat ook in het *EU Strategic Compass* een centraal thema is.[31]

Om de responseopties op een cyberaanval te analyseren behandelen we hieronder drie situaties: een cyberaanval die gelijk staat aan een gewapende aanval, een cyberaanval die gelijk staat aan het gebruik van geweld, en een cyberaanval onder de drempel van geweld.

24 Peter B.M.J. Pijpers en Kraesten L. Arnold, 'Conquering the Invisible Battleground', in: *Atlantisch Perspectief* 44 (2020) (4) 12-14; Ducheine en van Haaster, 'Cyber-Operaties en militair vermogen', 378.

25 Hard- en soft cyber slaat terug op het verschil in hard- en soft power als gemaakt door Joseph Nye, zie: Joseph S. Nye Jr., 'Soft Power', in: *Foreign Policy* 80 (1990) 153-171; Joseph S. Nye Jr., 'Cyber Power', 2010.

26 Zie onder andere Nomen Nescio, 'Verdediging door spionage. Waarom U.S. Cyber Command in feite een contra-inlichtingenstrategie uitvoert', in: *Militaire Spectator* 190 (2021) (7/8) 356-369..

27 Office of the Director of National Intelligence, 'Assessing Russian Activities and Intentions in Recent US Elections', 2017; Office of the Director of National Intelligence, 'Foreign Threats to the 2020 US Federal Elections', 2021.

28 Dennis Broeders, Els de Busser, en Patryk Pawlak, 'Three Tales of Attribution in Cyberspace: Criminal Law, International Law and Policy Debates', *The Hague Program for Cyber Norms*, 2020.

29 Artikel 2(4) van het VN-Handvest luidt: 'Alle Leden zullen in hun internationale betrekkingen zich onthouden van bedreiging met of gebruik van geweld tegen de territoriale integriteit of politieke onafhankelijkheid van enige Staat, of op enige andere wijze, die onverenigbaar is met de Doeleinden van de Verenigde Naties'.

30 Ronald Smit, 'Manoeuvreren in de informatieomgeving. Informatiegestuurd optreden voor de landmacht', in: *Intercom* 49 (2020) (3) 96.

31 Council of the European Union, 'Strategic Compass for Security and Defence'.

Een cyberaanval als een gewapende aanval

Met Artikel 42(7) VEU heeft de EU, net als de NAVO, de collectieve verdedigingsgedachte, gebaseerd op het internationale gewoonterecht en Artikel 51 van het VN-Handvest,[32] opgenomen in haar verdrag. De essentie van Artikel 51 is dat een staat zich (individueel en collectief) mag verdedigen met gebruikmaking van geweld, na een gewapende aanval door een andere actor. Een gewapende aanval geldt als deze grensoverschrijdend militair geweld omvat van een zekere 'scale and effect'.[33]

De NAVO en de EU hebben de collectieve verdediging slechts éénmaal ingeroepen; de VS riep Artikel 5 NAV in na de aanslagen op de Twin Towers op 11 september 2001, en Frankrijk heeft Artikel 42(7) VEU ingeroepen na de terroristische aanslag in Parijs (op onder meer het Bataclan theater) op 13 november 2015.[34] Dit wil echter niet zeggen dat de wederzijdse bijstandsclausule van de EU en de collectieve verdediging van de NAVO exact hetzelfde zijn.[35] De overeenkomst tussen NAVO en EU is dat, wanneer het op veiligheidsbeleid aankomt, de beslissingen zijn gestoeld op soevereine besluiten van de lidstaten en niet op supranationale besluiten van de organisatie. Het laatste is bij de EU wel het geval bij besluiten op het gebied van economie, landbouw of financiën. Maar er zijn meer verschillen, zoals nuanceverschillen in bewoording, reikwijdte, *casus foederis* (de concrete gebeurtenis die het recht inroept) en de verplichting naar bondgenoten.[36] Het belangrijkste verschil is echter dat de NAVO bekwaam is in, maar tegelijkertijd beperkt tot, het genereren van militaire effecten, terwijl de EU alle machtsinstrumenten tot haar beschikking heeft;[37] Het militaire effect is eerder een 'last resort',[38] niet in de laatste plaats omdat sommige EU-leden (militair) neutraal zijn.

De idee van collectieve zelfverdediging is ook van toepassing bij een actie in cyberspace. Bij een cyberaanval op een kerncentrale of een waterkering waardoor dodelijke slachtoffers, maatschappelijke ontwrichting en grote economische schade ontstaan, zou een staat zich op zelfverdediging via Artikel 51 VN-Handvest kunnen beroepen.[39] Zowel bij de NAVO als de EU

FOTO EUROPESE COMMISSIE

'Soft power is no longer enough', zei EU-buitenlandchef Josep Borrell

gaat het hierbij om de collectieve zelfverdedigingsreactie van soevereine staten en niet om een supranationale inzet.[40]

Tot op heden is nog geen cyberaanval als een gewapende aanval gekwalificeerd en hoewel dit niet is uit te sluiten,[41] ligt het niet voor de hand dat dit snel gebeurt. Enerzijds omdat de kwalificatie in cyberspace door bijvoorbeeld maskering, anonimiteit en modus operandi voor

32 Terry D. Gill en Paul A.L. Ducheine, 'Anticipatory Self-Defense in the Cyber Context', in: *International Law Studies (Naval War College)* 89 (2013) 438-471, 441-443.

33 Het verbod op het gebruik van geweld is dwingend recht (*jus cogens*). Een van de uitzonderingsgronden is het gebruik van geweld uit zelfverdediging na een gewapende aanval. Zie ook: Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports (1986), Paragraaf 190.

34 ECFR, 'Article 42.7: An Explainer', *European Council on Foreign Relations*, 2015; Anne Bakker et al., 'The EU's Mutual Assistance Clause', in: *Spearheading European Defence*, red. Clingendael Institute, 2016.

35 P.A.L. Ducheine en J.F.R. Boddens Hosang, 'Implementing Article 42.7 of the Treaty on European Union: Legal Foundations for Mutual Defence in the Face of Modern Threats', Amsterdam Center for International Law No. 2020-35, 14 december 2020. Zie: SSRN: https://ssrn.com/abstract=3748392.

36 Aurel Sari, 'Mutual Assistance Clauses of the North Atlantic and EU Treaties', in: *Harvard National Security Journal* 10 (2019) 405-460.

37 Paul A.L. Ducheine en Peter B.M.J. Pijpers, 'The Missing Component in Deterrence Theory: The Legal Framework', in: Frans P.B. Osinga en Tim Sweijs (red.), *Deterrence in the 21st Century–Insights from Theory and Practice*, (Springer, 2021) 475-500, 481-482.

38 Michael Smits en Peter B.M.J. Pijpers, 'Persistent Engagement. De nieuwe cyberstrategie voor Nederland?', in: *Militaire Spectator* 191 (2022) (2) 76-89, 88.

39 Ferry M.E. Oorsprong, Paul A.L. Ducheine, en Peter B.M.J. Pijpers, 'Armed Attack in Cyberspace: Clarifying and Assessing When Cyber-Attacks Trigger the Netherlands' Right of Self-Defence', *ACIL Research Paper 2021-27*, 2021.

40 Elie Perot, 'The Art of Commitments: NATO, the EU, and the Interplay between Law and Politics within Europe's Collective Defence Architecture', in: *European Security* 28 (2019) (1) 40-65, 52.

41 Gill en Ducheine, 'Anticipatory Self-Defense in the Cyber Context', 459-460.

een slachtoffer lastiger te maken is. Maar ook omdat de inzet van (kinetische) middelen – buiten cyberspace – voor een aanvaller sneller de beoogde effecten op zal leveren.

Een cyberaanval als gebruik van geweld
Niet iedere inzet van geweld is te kwalificeren als een gewapende aanval (Artikel 51 VN-Handvest). Maar ook (het dreigen met) militair geweldgebruik dat de drempel van een gewapende aanval niet haalt, is verboden. Het dreigen met, of gebruik van gewapend geweld, of het nu met kinetische of cybermiddelen is, is niet toegestaan volgens het geweldsverbod zoals neergelegd in Artikel 2(4) VN-Handvest. De cyberaanval met de Stuxnet-worm op de Iraanse verrijkingsinstallaties (Operatie Olympic Games) met aanzienlijke schade tot gevolg, heeft bijvoorbeeld de drempel van het geweldsverbod overschreden.[42]

Een legitieme reactie tegen het gebruik van geweld van een staat is het nemen van tegenmaatregelen (*countermeasures*). Dit zijn maatregelen die normaliter onrechtmatig zijn in het internationale verkeer, maar geoorloofd als reactie op een eerdere internationale onrechtmatige daad die aan een andere staat is toe te

In het hybride scala aan veiligheidsdreigingen dienen NAVO, EU en de individuele staten complementair aan elkaar op te treden en niet met elkaar te concurreren

rekenen.[43] Een represaille in de vorm van een tegenmaatregel is ook na een gewapende aanval in te roepen. De countermeasure moet proportioneel zijn, maar gebruik van geweld is daarbij niet toegestaan.[44] Daarnaast mag enkel de slachtofferstaat een tegenmaatregel uitvoeren. Een collectieve actie zoals na een gewapende aanval is hierbij niet geoorloofd.[45]

De kans dat een cyberaanval voldoet aan de criteria van een dreiging met of inzet van (gewapend) geweld (Artikel 2(4)) is groter dan de kans op een gewapende aanval (Artikel 51). Net als bij een reactie op een gewapende aanval, gaat het ook hier primair om een reactie van een soevereine staat. Countermeasures, in tegenstelling tot zelfverdediging, zijn echter niet collectief uit te voeren.

Een cyberaanval onder de drempel van gebruik van geweld
Tot slot een cyberaanval die het geweldsverbod niet schendt. Dit geldt voor het gros van alle nu bekende cyberaanvallen,[46] en zeker voor digitale beïnvloedingsoperaties. Het feit dat een cyberactie onder het niveau van geweld ligt, betekent echter niet dat deze geoorloofd is. Onder de drempel van geweld gelden regels van internationaal gewoonterecht gerelateerd aan soevereiniteit en non-interventie.[27] De variëteit aan mogelijke maatschappelijke verstoringen of inbreuk op soevereiniteit en het interventieverbod via cyberspace is niet beperkt tot *gewapende* verstoring; ook een onrechtmatige economische, politieke of ondermijnende beïnvloedingsoperatie kan een schending van de soevereiniteit of van het non-interventieverbod opleveren.[48]

42 Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Second ed. (Cambridge, UK, Cambridge University Press, 2017) regel 71 (10), 342.

43 Michael N. Schmitt, '"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law', in: *Virginia Journal of International Law* 54 (2014).

44 James Crawford, *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries*, red. James Crawford (Cambridge, Cambridge University Press, 2002). Artikelen 22, 50 en 51.

45 André Nollkaemper, *Kern van het internationaal publiekrecht*, *Boom Juridisch*, 8th ed (Den Haag, Boom juridisch, 2019) 213-217.

46 Denk aan de aanval op het Amerikaanse *Office of Personnel Management* (2014), de hack op de Duitse *Bundestag* (2015), *(Not)Petya* van (2016)2017, de hack op de OPCW (2018), *SolarWinds* (2020) en *Colonial Pipelines* (2021).

47 P.A.L. Ducheine, 'Military Cyber Operations', in: Terry D. Gill en Dieter Fleck (red.), *Handbook of the International Law of Military Operations* (2nd ed., Oxford University Press, 2015). Hoofdstuk 23, 456-475. Indien cyberacties (onder het niveau van geweld) plaatsvinden tijdens een gewapend conflict dan geldt tevens het Humanitair Oorlogsrecht, zie: Bart G.L.C van den Bosch, *Oorlog voeren zonder geweld. Onderzoek naar de regels binnen het humanitair oorlogsrecht voor militaire cyberoperaties die de drempel van aanval niet halen* (dissertatie, Universiteit van Amsterdam, 2019).

48 Peter B.M.J. Pijpers, *Influence Operations in Cyberspace. On the Applicability of Public International Law during Influence Operations in a Situation Below the Threshold of the Use of Force* (Dissertatie, Universiteit van Amsterdam, 2021). 2021, 274-278.

De NAVO is primair een militair machtsinstrument en daarmee minder geschikt om bij een daad onder het niveau van geweld op te treden. Een militaire (kinetische) reactie op een ontwrichtende maar geweldloze cyberaanval is veelal disproportioneel en een inbreuk op het geweldsverbod. De NAVO kan wel overgaan tot beperkte diplomatieke maatregelen.[49]

Daar waar de EU matig geëquipeerd is bij traditionele (kinetische) conflicten, omdat zij in mindere mate beschikt over de capaciteiten om militaire effecten te genereren, of niet bereid is dat te doen, zou dit juist een voordeel kunnen zijn bij het tegengaan van kwaadwillende activiteiten in cyberspace. De verdediging tegen hybride activiteiten of cyberoperaties, onder het niveau van geweld, is mogelijk effectiever met maatregelen in de diplomatieke, economische, juridische en financiële sfeer. Daar waar de NAVO de middelen ontbeert, heeft de EU deze wel.

Als onderdeel van het Gemeenschappelijk Buitenlands en Veiligheidsbeleid (GBVB) heeft de EU een raamwerk voor een gemeenschappelijke diplomatieke respons tegen kwaadwillende acties in cyberspace aangenomen. Dit raamwerk, ook wel de Cyber Diplomacy Toolbox geheten, is een samenraapsel van verschillende statelijke, supranationale en intergouvernementele acties – waaronder sancties – die de EU (of haar individuele lidstaten) kan nemen om de gevaren van cyberdreigingen tegen te gaan. Om de Cyber Diplomacy Toolbox verder te ontwikkelen heeft de EU een Joint Cyber Unit opgericht. Deze unit is een netwerk van *cybersecurity communities* die de EU weerbaarder wil maken tegen cyberaanvallen, en om de rechtsopsporing, de cyberverdediging en -diplomatie te verbeteren. Dit met als doel door afschrikking cyberaanvallen te voorkomen, en waar afschrikking faalt op die aanvallen te reageren.[50]

In tegenstelling tot de NAVO heeft de EU, naast de wederzijdse bijstandsclausule van Artikel 42(7) VEU, meer instrumenten die zij kan inzetten bij de verdediging tegen ongewenste cyberoperaties of inmenging van een andere staat of actor. Hierbij gaat het om instrumenten waar de EU 'supranationaal' over kan beschikken: de solidariteitsclausule, en sancties en diplomatieke maatregelen.

De solidariteitsclausule (Artikel 222 van het Verdrag betreffende de Werking van de EU – VWEU) handelt over bijstand van de EU en haar lidstaten in geval van een terroristische aanval, een natuurramp of een door de mens veroorzaakte ramp.[51] En hoewel lidstaten onder deze clausule (vrijwillig) militaire middelen ter beschikking kunnen stellen, komt de solidariteitsclausule niet voort uit het inherente recht op zelfverdediging. De solidariteitsclausule is in te zetten tegen 'any situation which has or may have a severe impact on people (…)'.[52] De EU *Cybersecurity Strategy* (2013) gaf expliciet aan dat Artikel 222 VWEU ook bij een serieuze cyberaanval in te roepen is.[53]

Daarnaast is de EU ook in staat om economische en diplomatieke sancties op te leggen. Staten hebben over het algemeen meer juridische armslag om te ageren tegen ongewenste inmenging via een cyberoperatie dan internationale organisaties. Staten kunnen naast de bovengenoemde represailles in de vorm van tegenmaatregelen ook zogeheten retorsies inroepen.[54] Represailles zijn alleen rechtmatig na een eerdere onrechtmatige daad van een andere staat, en erop gericht die onrechtmatige daad te stoppen. Een retorsie is een vergeldingsmaatregel die ongewenst maar niet op voorhand onrechtmatig is,[55] zoals het verbreken van diplomatieke banden, het opleggen van sancties

49 Zie bijvoorbeeld: NATO, 'North Atlantic Council Statement Following the Announcement by the United States of Actions with Regard to Russia', 2021, 5-6.

50 European Union, 'Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")', *Draft Council Conclusions*, no. June (2017); European Commission, 'Joint Cyber Unit', *Factsheet*, 2021.

51 Council of the European Union, 'Decision on the Arrangements for the Implementation by the Union of the Solidarity Clause', *Official Journal of the European Union* 415 (2014) 56-57.

52 Council of the European Union, Article 3 (a), 55; Patryk Pawlak, 'Cybersecurity and Cyberdefence EU Solidarity and Mutual Defence Clauses', no. June (2015) 4.

53 European Commission and High Representative, 'Cybersecurity Strategy of the European Union', in: *Official Journal of the European Union* JOIN (2013) (1) 19.

54 Terry D. Gill, 'Non-Intervention in the Cyber Context', in: *Peacetime Regime for State Activities in Cyberspace* (2013) 217-238, 230.

55 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 20 (4).

Nederlandse en Belgische militairen trainen samen voor de EU-Battlegroups. Cyberaanvallen blijven mogelijk niet altijd geweldloos, waardoor de theoretische optie van zelfverdediging open moet blijven

of beëindigen van economische hulp. In tegenstelling tot een represaille is een retorsie wel uit te voeren door een collectief aan landen of een supranationale organisatie zoals de EU. Een retorsie is ook bij een gewapende aanval of na gebruik van geweld in te zetten. Tot slot kunnen staten zich ook beroepen op enkele rechtvaardigingsgronden zoals force majeur, 'distress' als mensenlevens in gevaar zijn, of een beroep op 'necessity' wanneer de essentiële belangen in 'grave and imminent peril' zijn.[56] In de cybercontext is een 'plea of necessity' mogelijk in te roepen bij een zeer ernstige dreiging tegen de vitale infrastructuur. Hierbij is het niet noodzakelijk dat er al een eerdere internationale onrechtmatige daad heeft plaatsgevonden, of dat de dreiging van een staat komt.

De EU kan, net als een staat, zelfstandig sancties (of beperkende maatregelen) opleggen, in reactie op een cyberaanval, gebaseerd op Artikel 215 VWEU. Sancties hebben tot doel het beleid of gedrag van een staat of actor te veranderen en in lijn te brengen met de doelstellingen van het GBVB. In strikte zin hebben sancties een economische of financiële impact tegen staten, organisaties of individuen, zoals een wapenembargo, (in)reisverbod, het bevriezen van deviezen, of een import- of investeringsverbod.

In bredere zin vallen ook diplomatieke maatregelen onder retorsies. Maatregelen die te nemen zijn na een cyberaanval behelzen onder meer een diplomatieke demarche, het beëindigen van diplomatieke relaties tussen de EU als organisatie en niet-EU-landen, en in het uiterste geval diplomaten uitwijzen. Deze diplomatieke maatregelen vinden meestal samen plaats met, of ter ondersteuning van, acties van individuele EU-lidstaten.

Conclusie

Toekomstige conflicten of competities zullen niet louter traditionele kinetische confrontaties omvatten. Het verleden is qua conflictvormen niet de voorbode voor de toekomst. Toekomstige conflicten zijn eerder een (hybride) samengaan van verschillende soorten confrontaties en agitaties, waaronder interacties in cyberspace, in het spectrum tussen oorlog en vrede. Cyberoperaties vinden over het algemeen (en vooralsnog) onder het niveau van het geweldge-

56 Crawford, *The International Law Commission's Articles on State Responsibility : Introduction, Text and Commentaries*, 178-86.

FOTO MCD, EVA KLIJN

bruik plaats. Daarnaast zijn cyberoperaties niet altijd afkomstig van staten, klassiek de primaire actoren in het internationale verkeer.

De NAVO en de EU kennen, vanuit hun ontstaansgeschiedenis, een verschillende benadering van veiligheidsvraagstukken. Het primaire verschil tussen NAVO en EU is dat de capaciteit van de NAVO zich vooral richt op statelijke actoren, in een situatie van geweld en gewapend conflict ter verdediging van het bondgenootschappelijke grondgebied. De NAVO heeft daarom een instrumentarium dat gericht is op collectieve zelfverdediging. De EU kan zich op staten én op natuurlijke personen of organisaties richten, zowel binnen als buiten het EU-verdragsgebied. De EU richt zich bovendien ook op situaties onder het niveau van geweld.

De EU lijkt, op basis van haar institutionele constellatie, beter geschikt hedendaagse cyberaanvallen tegen te gaan, gebruikmakend van de solidariteitsclausule en sancties. En bovendien, waar de EU bij de inzet van traditionele kinetische middelen verschillende militaire capaciteiten mist, vallen deze bij het reageren op cyberaanvallen weg – denk aan de behoefte voor strategisch transport of air-to-air refuelling.

Maar het verschil tussen beide organisaties is minder groot dan vaak aangenomen. Het geheel aan supranationale EU-maatregelen, intergouvernementele maatregelen en maatregelen van separate EU-lidstaten (variërend van collectieve verdediging, tegenmaatregelen en retorsies in reactie op kwaadwillende cyberaanvallen) is opgesomd in de Cyber Diplomacy Toolbox. Dit is geen staand EU-beleid maar eerder een potpourri aan maatregelen zoals ook de NAVO die mogelijk zou kunnen opstellen. De cyber toolbox beroept zich immers deels op soevereine instrumenten, inclusief de inzet van de krijgsmacht als 'a single set of forces', van individuele lidstaten.

Daarnaast is de EU niet in staat op alle fronten te ageren. Cyberaanvallen blijven mogelijk niet altijd geweldloos, waardoor de theoretische optie van zelfverdediging open moet blijven. Het verdedigingsinstrumentarium tegen cyberoperaties zou een constellatie van capaciteiten van de EU, de NAVO en de lidstaten moeten zijn. De EU heeft een groot scala aan instrumenten die vooral geschikt zijn buiten een situatie van geweld of gewapend conflict. Wanneer de EU in dat geval het voortouw heeft kan de NAVO aanvullen en ondersteunen, gebruikmakend van haar inlichtingenpositie en geïntegreerde command & control-structuur. Ook als een cyberoperatie geweld omvat is het effectiever om de NAVO in te zetten, zeker vanwege de aanvullende capaciteiten van landen als de VS, Canada en het VK. Tot slot kunnen individuele lidstaten actief zijn door diplomatieke acties te ondernemen, en lidstaten kunnen countermeasures nemen na een eerdere internationale onrechtmatige daad. In het hybride scala aan veiligheidsdreigingen moeten NAVO, EU en de individuele staten complementair aan elkaar optreden, niet met elkaar concurreren.[57]

Reflecties op de rol van de EU

Terugkomend op het Europese leger, of liever op strategische autonomie: het spectrum van conflicten zal in de toekomst divergeren; traditionele conflicten – zie de oorlog in Oekraïne – zijn niet uit te sluiten, maar erop blindstaren is ook niet nuttig.

Aangezien de NAVO, waar veel EU-lidstaten al deel van uitmaken, haar ontstaan ontleent aan het voorkomen van gewapend conflict, is het voor de EU wellicht beter juist niet een militaire macht *à la* de NAVO – inclusief een eigen leger – te willen zijn, maar haar strategische autonomie te zoeken in hybride en cyberconflicten onder het niveau van geweld. De Cyber Diplomacy Toolbox is dan te hervormen van een lijstje met 'nieuwe-kleren-van-de-keizer' naar een effectief instrument dat cyberaanvallen kan tegengaan. ■

57 Zie ook: Sabine N. Mengelberg, 'EU En NAVO: concurrerend of complementair?'. in: *Militaire Spectator* 191 (2022) (3) 158-160.