FACULTEIT POLITIEKE EN SOCIALE WETENSCHAPPEN

NATO'S 'COLLECTIVE' CYBER DEFENCE

IS DE HUIDIGE STRATEGIE VAN DE NAVO DOELTREFFEND OM EEN OORLOG TE WINNEN IN HET VIJFDE DOMEIN?

Wetenschappelijke verhandeling
Aantal woorden: 21 250

Ellen Platteau
Stamnummer: 01701969

Promotor: Prof. dr. Sven Biscop

Masterproef voorgelegd voor het behalen van de graad master in de richting Politieke Wetenschappen afstudeerrichting Internationale Politiek

Academiejaar: 2020-2021

UNIVERSITEIT GENT

I. Dankwoord

Met dit dankwoord zou ik allereerst mijn oprechte dank willen betuigen aan mijn promotor Prof. dr. Sven Biscop voor zijn advies en begeleiding tijdens de voorbereiding van deze masterproef. Dankzij zijn vlotte feedback kon ik bijsturen waar nodig om mijn onderzoek tot een goed eind te brengen.

Daarnaast wil ik graag Prof. dr. Dirk Debeaussaert bedanken voor de interessante lessen en gastcolleges in het vak 'Nationale Veiligheid in een Hedendaags Perspectief'. Tijdens deze gastcolleges kon ik vragen stellen aan experts uit het cyberdomein en de NAVO. Hun input is van enorme meerwaarde voor deze scriptie, waar ik hen enorm dankbaar voor ben.

II. Abstract

De opkomst van cyber heeft ervoor gezorgd dat de manier van oorlogsvoering fundamenteel is veranderd. Staten met een zwakke militaire macht kunnen een strategisch voordeel verkrijgen door het uitbouwen van hun cybercapaciteit. Dit fenomeen zou in de toekomst kunnen resulteren in een cyberoorlog, waarbij bondgenoten van de NAVO het doelwit zijn van vijandige natiestaten. Deze masterproef onderzocht aan de hand van een uitgebreide literatuurstudie of de huidige NAVO-strategie over het vermogen beschikt om succesvol terug te slaan mocht er zich een internationaal gewapend conflict in het cyberdomein voordoen. Door middel van een evaluatie van voormalige cyberincidenten waarin NAVO-bondgenoten betrokken waren, en het onderzoeken van primaire en secundaire bronnen, werd tot de vaststelling gekomen dat het loutere defensieve mandaat van de NAVO onvoldoende doeltreffend is om vijandige natiestaten te vergelden.

Vanwege deze bevindingen werden enkele argumenten voor het uitbouwen van een collectieve offensieve cybercapaciteit binnen de NAVO gemotiveerd. Hoewel de NAVO een defensieve militaire macht is, kan een offensieve cybercapaciteit ook een defensieve rol spelen als instrument tijdens een internationaal gewapend conflict, door dienst te doen als een vergeldingsmechanisme. Bovendien zou het ten goede komen aan de geloofwaardigheid van het bondgenootschap op het internationale toneel, en de implementatie van het Artikel 5 in het cyberdomein. Het is de bedoeling van deze masterproef om met de bevindingen uit het onderzoek een publiek debat te openen over het uitbouwen van een collectieve offensieve cybercapaciteit ter voorbereiding van toekomstige dreigingen in het vijfde domein.

III. Lijst met afkortingen

ADIV	Algemene Dienst voor Inlichtingen en Veiligheid
AI	Artificial Intelligence
CyCon	Conference on Cyber Conflict
DdoS	Distributed-denial-of-Service
DIME	Diplomacy, Information, Military, Economics
EW	Electronic Warfare
NAVO	Noord-Atlantische Verdragsorganisatie
NATO CCDCOE	Cooperative Cyber Defense Center of Excellence
NCIRC	NATO Computer Incident Response Capability
RAT's	Remote Access Tools

IV. Inhoudsopgave

1. Inleiding

1.1. Achtergrond

Vandaag de dag voeren we ons leven steeds meer uit in de onlinewereld. Deze connectiviteit brengt veel voordelen met zich mee, maar er is ook een keerzijde van de medaille, namelijk de kwetsbaarheid voor cyberaanvallen. Met ruim drie miljard internetgebruikers en de groeiende aanwezigheid van technologie in de samenleving, is het niet te verwonderen dat het wereldwijde web een terrein van gestaag conflict is geworden. Het is duidelijk dat wat er in *cyberspace* gebeurt, niet volledig in *cyberspace* blijft, en dit kan weleens een grote impact hebben op ons dagelijks leven. Cyberdreigingen bevinden zich zowel binnen als tussen staten, en deze laatste brengt een nog groter risico met zich mee: het risico op cyberoorlogsvoering. *Cyberspace* is uitgegroeid tot een nieuw operationeel gebied waar regeringen over de hele wereld strijden om de digitale suprematie in een nieuw, meestal onzichtbaar, theater van operaties. Wat ooit beperkt was tot het terrein van opportunistische criminelen is nu een belangrijk wapen voor regeringen die hun soevereiniteit willen verdedigen en hun nationale macht willen vergroten.

> *"Cyber warfare is probably the greatest challenge that we have as far as our nation's national security is concerned. We have an advantage over every other form of competition with possible allies except one, that's cyber warfare. And when you see the potential of what a successful cyber-attack can achieve, it's enough to make you deeply concerned."* (Senator John McCain, 2017)

Hoewel een effectieve oorlog in dit domein nog heel onwaarschijnlijk lijkt, is het van essentieel belang om de ernst van deze dreiging onder ogen te zien, en werpt het een nieuw licht op de toekomst van de internationale betrekkingen. Hackers, gesteund door vijandige natiestaten, kunnen omwille van politieke motieven staten aanvallen met behulp van computer- of netwerksabotage. De voordelen om een strijd te voeren in *cyberspace* zijn legio en kunnen tot diepgaande gevolgen leiden voor de aangevallen staat. Cyberaanvallen zijn niet gebonden aan plaats en tijd, waardoor het doel binnen enkele minuten kan worden bereikt, zonder in directe confrontatie te gaan. Ze kunnen gebruikt worden voor verschillende doeleinden zoals het stelen van gegevens, het verstoren van een netwerk of het verspreiden van propaganda. Bovendien slagen deze aanvallen er vaak in om fysieke nevenschade aan te richten aan een land, door het beschadigen of vernietigen van kritieke infrastructuur.

In februari 2021 brachten de Estse inlichtingendiensten hun jaarlijkse veiligheidsbeoordeling uit. Het rapport (2021) stelde dat Russische staatsagenten hoogstwaarschijnlijk achter de beruchte *'SolarWinds'*-hack zaten eind vorig jaar. Tijdens deze cyberaanval werden interne e-mails van de Amerikaanse regering en andere westerse instellingen, waaronder die van het Europese Parlement, onderschept door kwaadwillige actoren. De aanval was van uitzonderlijk hoog niveau en waarschijnlijk gericht op het zoeken naar staatsgeheimen (Riley, 2021). Volgens Thomas Rid (2021), professor strategische studies aan de *Jon Hopkins University*, is dit een van de grootste spionagecampagnes die men in de afgelopen jaren heeft ontdekt. Hij schat de kans ook zeer klein dat de Russische speciale diensten hun cybertechnologie zullen ontmantelen, integendeel, het is aannemelijk dat het land de ontwikkeling ervan zal versterken. Hierdoor zullen staten hun veiligheidsnetwerken extra moeten bewapenen.

Gebeurtenissen van deze aard zorgen ervoor dat het ontwikkelen van offensieve en defensieve cybercapaciteiten wereldwijd hoog op de agenda staat. Naast natiestaten heeft ook de Noord-Atlantische Verdragsorganisatie (NAVO) baat bij het nastreven van een doeltreffende cybercapaciteit ter bescherming van haar bondgenoten. Tijdens de top in Warschau van 2016 bevestigden de geallieerde regeringsleiders dat cyberdefensie deel uitmaakt van de kerntaak van de NAVO met betrekking tot de collectieve defensie van Artikel 5. Hierbij wordt *cyberspace* als het vijfde operatiedomein erkend, waarin de NAVO zich even effectief moet verdedigen als in de lucht, te land, op zee en in de ruimte (Minárik, 2016).

Tot op de dag van vandaag steunt de NAVO op haar defensieve mandaat om cyberdreigingen tegen te gaan. Op militair niveau blijven de bondgenoten over het algemeen zeer terughoudend omtrent het uitbouwen van collectieve offensieve capaciteiten, wat ook geldt in het cyberdomein (NATO, Cyber defence, 2021). Het is zeker van belang dat de NAVO doeltreffend is in het beveiligen van haar netwerken en operaties, maar er moet wel nagedacht worden of het bondgenootschap geen strategisch nadeel ondervindt door het niet beschikken over een collectieve offensieve cybercapaciteit, mocht er zich werkelijk een internationale cyberoorlog afspelen?

1.2. Doelstelling

In het cyberdomein bevinden zich nieuwe dreigingen en kwetsbaarheden waar de NAVO in de toekomst mee zal worden geconfronteerd. Met de opmars van agressieve tegenstanders zoals Rusland en China zal het Westen hoogstwaarschijnlijk haar collectieve strategie moeten aanpassen. Hierdoor moeten we ons de vraag stellen of het geen tijd wordt om een offensieve cybercapaciteit uit te bouwen. Een offensieve cybercapaciteit mag niet geïnterpreteerd worden in de zin dat de NAVO zelf een aanval start tegen een vijandige natiestaat, aangezien het nog steeds een verdedigende militaire alliantie is. Het moet geïnterpreteerd worden als een potentieel middel om tegenmaatregelen te nemen.

De doelstelling van deze masterproef is om een antwoord te geven op de hypothetische vraag: *"In welke mate beschikt de NAVO over het vermogen om een cyberoorlog te voeren?"* Met andere woorden is het de bedoeling om te analyseren in hoeverre de huidige defensieve cyberstrategie van de NAVO effectief is om te reageren op vijandige natiestaten die gebruik maken van cyberoorlogsvoering tegen een of meerdere NAVO-lidstaten. Ook zal er worden nagegaan welke rol Artikel 5 van het Noord-Atlantisch Verdrag speelt in het cyberdomein, en in welke mate deze vandaag de dag doeltreffend is mocht er een internationaal conflict in *cyberspace* geschieden.

1.3. Onderzoeksvragen

De masterproef zal een antwoord geven op de hypothetische hoofdonderzoeksvraag, geïndiceerd met het cijfer 1. Deze wordt onderzocht aan de hand van enkele deelvragen:

1) In welke mate beschikt de huidige NAVO-strategie over het vermogen om een cyberoorlog te voeren?

2) Op welke manier reageerde de NAVO in het verleden op cyberaanvallen die haar lidstaten troffen?

3) Tot op welke hoogte ondervindt de NAVO een strategisch nadeel door zich louter te focussen op haar defensieve cybercapaciteit?

4) Hoe wordt de rol van Artikel 5 momenteel toegepast in het cyberdomein?

5) Welke rol zouden collectieve offensieve cyberoperaties kunnen spelen in de cyberstrategie van de NAVO?

1.4. Methodologie

Deze masterproef bestaat uit een uitgebreid literatuuronderzoek dat steunt op een analytische en beschrijvende benadering. Vanwege de gelimiteerde omvang wordt het onderzoek vanuit een zuiver politiekwetenschappelijke invalshoek behandeld, en gaat dus niet verder in op de complexe technische en juridische aspecten rond het cyberdomein.

In de literatuurstudie wordt er gebruikgemaakt van gerenommeerde secundaire bronnen, zoals Thomas Rid, Martin Libicki, John B. Sheldon en Joseph S. Nye. Ook twee primaire bronnen werden bevraagd tijdens een uiteenzetting over hun organisatie in de lessen 'Nationale Veiligheid in een Hedendaags Perspectief' van Prof. dr. Dirk Debeaussaert, namelijk: Timmie Bonneu, adjunct-directeur van het Cybercomponent van onze Algemene Dienst voor Inlichtingen en Veiligheid (ADIV), en Philippe Van Gyseghem, Permanente Vertegenwoordiger van België bij de NAVO. Hun bevindingen worden in dit onderzoek verwerkt en bieden een meerwaarde in het opvullen van verschillende hiaten omtrent dit onderwerp. De combinatie van deskundige secundaire en primaire bronnen draagt bij aan de adequaatheid van deze masterproef. Het antwoord op de hypothese wordt afgeleid uit de bevindingen van de literatuurstudie en is eerder een persoonlijke mening, wat een deur opent voor een publiek debat omtrent het onderwerp.

1.5. Overzicht

Het onderzoek is opgebouwd uit verschillende hoofdstukken, die elk een belangrijke meerwaarde bieden in het verkrijgen van antwoorden op de onderzoeksvragen. Het tweede hoofdstuk behandelt een uitgebreide bespreking over wat er momenteel al geschreven is over cyberoorlogsvoering, en hoe waarschijnlijk de kans is dat er in de toekomst van gebruik zal worden gemaakt. Er wordt verduidelijkt wat het precies inhoudt, en waarom het een toekomstige uitdaging vormt voor de wijze waarop staten met elkaar in conflict zullen gaan. Daarnaast worden de concepten 'grijze zone' en 'hybride oorlogsvoering' besproken om de context te schetsen van de periode waarin we momenteel leven. Ook wordt er nagegaan welke voor- en nadelen deze manier van oorlogsvoering met zicht meebrengt, en in welke mate deze verschilt met het voeren van een conventionele oorlog.

Het derde hoofdstuk gaat specifiek in op de NAVO en de huidige cyberdreigingen voor het bondgenootschap. Er wordt beschreven welke soorten dreigingen er in *cyberspace* bestaan, en welke impact deze kunnen hebben op onze alliantie. Vervolgens wordt ook in kaart gebracht welke natiestaten een vijandige en agressieve houding hanteren ten opzichte van de NAVO in het cyberdomein. Tot slot worden de vier bekendste en grootste cyberaanvallen ten opzichte van de NAVO besproken. Vanwege hun omvang en impact op het bondgenootschap hebben ze gezorgd voor een transitie in het cyberbeleid en de -strategie van het bondgenootschap. In dit deel wordt ook geanalyseerd op welke manier de NAVO heeft gereageerd op deze cyberaanvallen, en of haar reactie al dan niet doeltreffend was om de dreiging tegen te gaan.

In het vierde hoofdstuk wordt de cyberstrategie van de NAVO onder de loep genomen. Deze is momenteel gebaseerd op een defensief mandaat, dat vooral belang hecht aan het beveiligen van haar netwerken en kritieke infrastructuur. Hierin wordt de werking van de CCD COE en haar mechanismes verklaard: het Tallinn Manual, *Locked Shields*, en *CyCon*. Ook de rol van het sleutelartikel, Artikel 5, wordt in dit hoofdstuk geanalyseerd, en in welke manier het tot zijn recht komt in *cyberspace*. Tot slot wordt er verklaard waarom een offensieve cybercapaciteit zo moeilijk ligt binnen het bondgenootschap.

In het vijfde hoofdstuk wordt geargumenteerd waarom een collectieve offensieve cybercapaciteit een noodzaak is voor het bondgenootschap. Eerst wordt er een evaluatie gemaakt die afgeleid is van de bevindingen uit het onderzoek, en daarna wordt aan de hand van enkele argumenten gemotiveerd waarom het bezitten van een collectieve offensieve cybercapaciteit van cruciaal belang is indien het bondgenootschap zou te maken krijgen met een internationaal cyberconflict. Bijgevolg worden drie militaire en strategische doelstellingen beschreven die de NAVO zou kunnen hanteren in haar beleid.

Tot slot wordt in het zesde en laatste hoofdstuk de conclusie van dit onderzoek beschreven. Ook geeft het een kritische reflectie van de obstakels waarmee deze masterproef werd geconfronteerd en welke hiaten er nog moeten worden opgevuld.

2. Cyberoorlogsvoering: een nieuwe dimensie binnen conflicten

2.1. Een reële dreiging voor onze samenleving

De toenemende macht in *cyberspace* verandert het karakter van menselijke activiteit en zorgt daarbij voor een nieuwe soort militaire macht. Op het vlak van strategie zorgt cybermacht voor een reorganisatie van de context waarin alle strategische activiteit zich afspeelt, namelijk in de internationale politiek. In het onderzoek van Arquilla & Ronfeldt (1993) kwam men voor het eerst tot het besef dat de informatierevolutie de aard van oorlogsvoering drastisch kan veranderen. Het is ondertussen duidelijk dat individuen, organisaties, statelijke en niet-statelijke actoren continu bezig zijn met het versterken van hun macht in *cyberspace* (Sheldon, The Rise of Cyberpower, 2016, p. 284). De huidige ontwikkeling van cyberoorlogsvoering stelt de internationale vrede en stabiliteit voor vele uitdagingen. Dagelijks ontwikkelen natiestaten nieuwe, innovatieve middelen om hun politieke doelstellingen te bereiken (p.285). De toenemende kwantiteit en kwaliteit van cyberaanvallen vormen een bedreiging voor vele aspecten van de civiele samenleving, die grotendeels afhankelijk is van betrouwbare netwerken en informatiesystemen.

'Dreigingen in *cyberspace*', wat moet daar nu onder worden verstaan? Het lijkt een surrealistische gedachte dat een aanval op het web enorme schade kan toebrengen aan een staat en daarbij een groot deel van de bevolking kan treffen. Om hiervan een beeld te schetsen, werkten Simona R. Soare en Joe Burton (2020) een fictief scenario uit in het kader van de *'NATO 2030 Strategy'*. Het scenario toont aan welke impact een cyberaanval kan hebben op een grootstad, en hoe het kan bijdragen tot een ernstige ontwrichting van de sociale, politieke en technische structuren en processen van de stad. In hun scenario wordt de fictieve stad Megalopolinn, de hoofdstad van een belangrijke Europese NAVO-lidstaat, aangevallen door een netwerk van hackers dat banden heeft met een autoritaire, revisionistische staat.

Stel je eens voor, we zijn vandaag 2 februari 2030. Megalopolinn is de hoofdstad van Varmatië, en met ruim 10 miljoen inwoners genereert de stad meer dan 30% van het bbp van Varmatië (p.108-110). Het is een belangrijk knooppunt voor transport, alsook een spil voor de logistiek van de NAVO, de defensieplanning, de militaire mobiliteit en de versterking van de Oost-Europese bondgenoten. Omstreeks 19u43 worden de 5G-servers en zendmasten van Megalopolinn stilgelegd door massale *Distributed Denial of Service*

(DdoS)-aanvallen die worden ondersteund door *Artificial Intelligence* (AI). Het hoofdnetwerk is geïnfecteerd door een zelfreplicerende worm die zich enorm snel verspreidt doorheen het netwerk van de stad en haar kritieke infrastructuur. In amper enkele uren worden verschillende sectoren van het netwerk doorkruist door de malware met alle gevolgen van dien: de servers van het stadhuis vallen uit, de GPS-diensten waar de politie en hulpdiensten van gebruik maken worden uitgeschakeld, alsook de stroom- en watervoorziening van de helft van de stad. Hieruit volgt dat burgers geen toegang meer hebben tot proper water of elektriciteit. Ook het banksysteem is defect waardoor niemand nog de mogelijkheid heeft om geld af te halen. De communicatiemiddelen liggen volledig stil en de huizen kunnen niet meer worden verwarmd terwijl het putje winter is.

Het was niet de bedoeling van Soare en Burton om een beeld van de toekomst te schetsen, maar eerder om mensen bewust te maken van de onzichtbare risico's en kwetsbaarheden waarmee we mogelijk zullen worden geconfronteerd (p.110). De connectiviteit en onderlinge afhankelijkheid zorgen ervoor dat een gesofisticeerde aanval op korte tijd enorme schade kan veroorzaken. Cyberoorlogsvoering, internetaanvallen van staten op kritieke infrastructuur en kwaadwillige exploitatie van informatienetwerken vormen een groot risico waarmee we in de toekomst te maken zullen hebben, en hiermee moeten ook de NAVO-lidstaten rekening houden. De geopolitieke positie en het kwetsbare aanvalsoppervlak van het Westen staat voor bijzondere uitdagingen bij het tegengaan van dreigingen in *cyberspace*.

De groeiende betrokkenheid van staten bij cyberaanvallen is zorgwekkend, en zette reeds een 'cyberwapenwedloop' in gang (Hughes, 2009). We zien dat steeds meer landen een cybercomponent oprichten binnen hun krijgsmacht om zich ook online te kunnen weren tegen de vijand. Voor het eerst hebben staten met een geringe militaire capaciteit de mogelijkheid om hun aandeel in de internationale politiek te doen toenemen. Het is een zeer nuttige tool aangezien het wereldwijd met een zekere mate van anonimiteit kan worden ingezet en ook relatief goedkoop is. Dit zorgt ervoor dat zwakkere staten het machtsevenwicht kunnen doen kenteren in hun voordeel. Het is dan ook absoluut noodzakelijk dat de internationale gemeenschap cyberoorlogsvoering erkent als een gevaarlijk instrument voor agressieve natiestaten, schurkenstaten en andere vijandige actoren om economische of politieke voordelen te behalen ten opzichte van de huidige dominante structuur in de wereldpolitiek (Tsekov, 2017).

2.2. De opkomst van cyberoorlogsvoering

Tot enkele decennia terug bestond het voeren van oorlog louter uit kinetische oorlogsvoering waarbij men gebruikmaakte van speren, zwaarden, explosieven, tanks en andere conventionele wapens. Een manier om de vijand te verzwakken aan de hand van economische schade, zonder rechtstreeks levens op het spel te zetten, was toen niet in te beelden (Gazula, 2017). Zelfs wanneer men zich bij militaire inspanningen louter ging richten op het verstoren van commerciële activiteiten, waren burgerslachtoffers een onvermijdelijk gevolg. Tot en met het einde van de 20ste eeuw bleef dit feit van kracht en waren luchtaanvallen onder de vorm van bombardementen het meest voorkomende middel om commerciële entiteiten te beschadigen. Door de afwezigheid van digitale infrastructuur was het voeren van een niet-kinetische oorlog uitgesloten.

Alles veranderde met de opkomst van het internet. Vanaf toen werd het mogelijk om met niet-kinetische middelen aan te vallen, die als grote voordeel niet-dodelijk waren van aard. Het concept van cyberoorlogsvoering heeft wel een korte evolutie ondergaan (Kaplan, 2016, p. 28). Om deze te verklaren moet eerst het onderscheid met hackers verduidelijkt worden. De oorspronkelijke hackers hadden namelijk andere motivaties. Dit waren personen met veel kennis en expertise van informatica en voerden hun daden vooral uit vanuit altruïstische motieven. Het gebeurde zelfs regelmatig dat de hacker contact opnam met de systeembeheerder van het gehackte netwerk om hen te informeren over de manier waarop men in het systeem was binnen geraakt, en hoe dit in de toekomst kon worden vermeden. De belangrijkste motivatie voor de hackers was het doen toenemen van hun kennis en deskundigheid, in combinatie met een afwezig legitieme uitlaatklep voor hun vaardigheden (p.29). Hoewel deze daden volstrekt illegaal en verboden waren, ontstond er toch een soort respect voor deze personen, want ze richtten zelden schade aan ondanks ze er wel toe in staat waren.

Vanaf toegang tot het internet publiek werd, kwamen de eerste *'scriptkiddies'* tevoorschijn op het web (p.30). *Hackingtools* werden gedeeld waardoor er een lagere graad van bekwaamheid nodig was om in te breken in kwetsbare systemen. Deze personen misten het gebrek aan moraal en expertise zoals bij de voorgenoemde hackers, waardoor ze hun plezier hadden in het plaatsen van godslasterlijke boodschappen op websites. De dreiging die van hen uitging was niet bijzonder geraffineerd en kon makkelijk worden opgelost door het beter beveiligen van de websites en netwerken. Het is pas sinds de eeuwwisseling dat criminele organisaties zich naar het web hebben begeven om *hacking* in te zetten als middel om inkomsten te verkrijgen door afpersing,

verduistering en identiteitsdiefstal. De omvang en ernst van deze dreiging is alsmaar toegenomen en vormt de dag van vandaag nog steeds een uitdaging voor zowel individuen als organisaties (p.32).

Niet veel later genereerden ook natiestaten middelen om hun macht in het cyberdomein te doen toenemen. Een natiestaat die gebruikmaakt van offensieve cybercapaciteiten en vijandige bedoelingen heeft, representeert de slechtste eigenschappen van de drie groepen, namelijk de kennis en geraffineerdheid van de oorspronkelijke hacker, de reikwijdte van de *skriptkiddies* en de doelgerichte, vijandige intentie om maximale schade aan te richten zoals bij de cybercrimineel (Gazula, 2017). Daarnaast zijn de cybereenheden van militaire- en inlichtingendiensten, in tegenstelling tot de vorige drie groepen, voorzien van een veel groter budget en meer middelen om hun aanvallen te kunnen voorbereiden en uit te voeren. Ook bestaat er bij hen geen angst voor de vervolging van hun daden in *cyberspace*, omdat ze opereren vanuit veilige plaatsen met weinig tot geen kans op (militaire) vergelding. Bijgevolg is de moraliteit meestal beperkt tot die van de regering die zij dienen, en hier moeten we in de toekomst op voorbereid zijn.

2.3. De fundamentele bouwstenen van het cyberdomein

De eerste logische stap om de verwarring op het gebied van cyberoorlogsvoering weg te werken is het definiëren van de fundamentele bouwstenen die in de literatuur worden gebruikt. Sommige termen zijn zeer complex, waardoor een beknopte uitleg het lezen zal vergemakkelijken. Op basis van hun relevantie voor dit onderzoek werd er gekozen om volgende begrippen van elkaar te onderscheiden: *cyberspace*, cybermacht, cyberstrategie, en het onderscheid tussen cyberoorlog en cyberoorlogsvoering. In de literatuur bestaat er controverse omtrent deze begrippen, waardoor er een nauwkeurige selectie werd gemaakt uit de definities die het best van toepassing lijken binnen dit onderzoek.

Cyberspace

Eerst en vooral is het belangrijk om de term '*cyberspace'* te verklaren. Er bestaan verschillende definities omtrent dit concept, en in dit onderzoek wordt de definitie van Daniel Kuehl (2009) gehanteerd, omdat het de belangrijkste overeenkomsten uit verschillende andere definities bundelt tot een term. Om een alomvattende definitie te verkrijgen, maakte hij gebruik van een selectie aan bronnen, zoals documenten van het Amerikaanse Ministerie van Defensie en deskundigen in het vakgebied (Robinson, Jones,

& Janicke, 2014). Uit deze analyse concludeerde hij dat *cyberspace* meer is dan louter computers en digitale informatie. Het bevat namelijk vier aspecten (p.72):

1) Een operationele ruimte: mensen en organisaties maken gebruik van *cyberspace* om te handelen en effecten te creëren, hetzij uitsluitend in *cyberspace*, hetzij over de grenzen van andere domeinen heen.
2) Een natuurlijk domein: *cyberspace* bestaat uit elektromagnetische activiteit en wordt betreden aan de hand van elektronische technologie.
3) Informatie als doel: mensen maken gebruik van *cyberspace* om informatie te creëren, op te slaan, te wijzigen uit te wisselen en te exploiteren.
4) Onderling verbonden netwerken: *cyberspace* bestaat uit verbindingen die elektromagnetische activiteit mogelijk maken om informatie over te dragen.

Om deze vier aspecten te weerspiegelen in een term creëerde Kuehl zijn eigen definitie van *cyberspace*:

> *"Cyberspace is een internationaal domein binnen de informatieomgeving waarvan het onderscheidende en unieke karakter omkaderd wordt door elektronica en het elektromagnetisch spectrum om informatie te creëren, op te slaan, te wijzigen, uit te wisselen en te exploiteren via onderling afhankelijke en onderling verbonden netwerken aan de hand van informatie-en comunicatietechnologieën."* (Kuehl, 2009)

Cybermacht

Omwille van de elasticiteit van de term 'cyber' bestaan er verschillende uiteenlopende visies over het concept 'cybermacht'. Professor aan de Universiteit van Harvard, Joseph S. Nye (2010), geeft een eerder hollistische visie aan de term. Volgens hem wordt macht gemanifesteerd binnen *cyberspace* door vorm te geven aan de bredere sociale, politieke en economische uitkomsten die zich buiten het domein bevinden. Hij maakt bijgevolg ook het onderscheid tussen *'intra cyberspace power'* en *'extra cyberspace power'* die nog eens worden onderverdeeld in *hard* en *soft power*.

Andere gerenommeerde academici, zoals professor John Sheldon (2011) van de *School of Advanced Air and Space studies* geeft een andere betekenis aan het strategische doel van cybermacht (p.95). Hij vat het concept samen als:

> *"Het vermogen om de strategische omgeving via en vanuit cyberspace te manipuleren in functie van het beleid in zowel vrede- als oorlogstijd, en*

tegelijkertijd proberen de capaciteiten van de tegenstander te verstoren, of alleszins te belemmeren, om hetzelfde te doen."

Cybermacht kan dus gezien worden als het vermogen om *cyberspace* te hanteren om strategische voordelen te verkrijgen, en om gebeurtenissen in alle operationele omgevingen te beïnvloeden boven andere machtsinstrumenten heen, zoals de lucht- en zeemacht.

Cyberstrategie

Ook over deze term bestaat er nog geen gemeenschappelijke visie. Volgens het onderzoek van Hoffman (2019, p. 133) is dit te wijten aan de internationale betwisting omtrent de doelstelling en de middelen. Wat moet de exacte doelstelling van een cyberstrategie zijn? Over welke middelen moeten staten beschikken om een cyberstrategie te hanteren?

Voor sommige auteurs gaat een cyberstrategie over de instrumenten die aanwezig zijn, zoals het gebruik van offensieve en defensieve cyberoperaties om beleidsdoelstellingen te bereiken (p.135). Andere beleidsmakers en academici zien een cyberstrategie als een cruciaal element voor het domein ter bescherming van de economische welvaart, sociale stabiliteit en nationale veiligheid tegen dreigingen in en door *cyberspace* (p.136). In beide gevallen wordt er wel naar elkaar verwezen, maar hierdoor gaat het onderscheid vaak verloren waardoor er in debatten verwarring ontstaat.

Hoewel het concept kan benaderd worden vanuit verschillende invalshoeken, wordt er in deze masterproef gebruikgemaakt van een meer algemene definitie. Een cyberstrategie komt in principe neer op een plan dat is ontwikkeld op hoog niveau, waarin wordt bepaald op welke manier een overheid, organisatie of bedrijf zich zal beveiligen tegen dreigingen in *cyberspace*. Deze strategie moet snel kunnen worden aangepast, omdat technologie en cyberdreigingen onvoorspelbaar en op korte tijd kunnen veranderen (Scarfone, 2021).

Cyberoorlog versus cyberoorlogsvoering

Deze concepten worden volgens het onderzoek van Robinson, Jones & Janicke (2015) heel vaak door elkaar gebruikt. De auteurs halen de problematiek hiervan aan, omdat de termen 'oorlog' en 'oorlogsvoering' twee afzonderlijke begrippen zijn. Aan de hand van een 'Actoren- en Intentie definitiemodel' hebben ze dit probleem aangepakt om de

concepten duidelijker te definiëren (p.74). Dit model is ontworpen aan de hand van een methodisch proces waarin definities van schadelijke gebeurtenissen in *cyberspace* tot stand komen. Het model is gebaseerd op het idee dat alle vijandige cyberdreigingen kunnen worden onderverdeeld in twee basisconcepten, namelijk dat een bepaalde actor de cyberaanval lanceert en dit moet gebeuren met een of andere vorm van schadelijke intentie.

Bij het toepassen van dit model kwam volgende definitie van cyberoorlogsvoering tot stand (p.74):

> *"Cyberoorlogsvoering betekent het gebruiken van cyberaanvallen met een oorlogszuchtige intentie."*

Het concept cyberoorlog verschilt hiervan, omdat dit een staat van zijn is. Om het in de woorden van de auteurs te zeggen: *"An actor can be at war, but does not perform war - they perform warfare."* Na het toepassen van het Actoren- en Intentie definitiemodel werd het begrip als volgt gedefinieerd (p.75):

> *"Een cyberoorlog gebeurt wanneer een natiestaat de oorlog verklaart, en waarbij alleen cyberoorlogsvoering wordt gebruikt om die oorlog uit te vechten."*

Dit betekent dus dat het begrip cyberoorlog enkel mag worden gehanteerd wanneer cyberoorlogsvoering de enige manier van oorlogsvoering is die wordt gebruikt. Indien er tijdens de oorlog een kinetische aanval wordt gelanceerd, zoals een luchtaanval, mag de toestand niet als een cyberoorlog worden geclassificeerd, maar als een conventionele oorlog waarbij gebruik wordt gemaakt van cyberoorlogsvoering. Het maken van dit onderscheid is cruciaal voor dit onderzoek, omdat het nu duidelijk is op welke manier de hypothese moet worden begrepen: met name of de NAVO als organisatie het vermogen heeft om een oorlog tegen te gaan die zich volledig afspeelt op het web.

2.4. Hoe grijs is de zone tussen oorlog en vrede in *cyberspace*?

Generaal Curtis Lemay had een zeer eenvoudige visie over het winnen van een oorlog, namelijk dat eens je genoeg slachtoffers maakt, de tegenpartij wel zal stoppen met vechten (Rhodes, 2012, p. 586). Carl von Clausewitz definieerde 'oorlog' duidelijker in zijn befaamde werkstuk *'Vom Kriege'*, als een uitbreiding van een duel tussen twee partijen. *"Het is een daad van geweld, bedoeld om onze tegenstander te dwingen aan*

onze wil te voldoen" (von Clausewitz, 1982, p. 101). Deze definitie geldt inderdaad voor de meeste oorlogen gevoerd sinds de geschiedenis van de mensheid. Sinds de Peloponnesische Oorlog spreekt men van een oorlogstoestand wanneer er een bekende tegenstander is met duidelijke politieke doelstellingen die niet overeenkomen met de eigen doelstellingen. Ook bevat de definitie van Clausewitz verschillende kenmerken die onveranderlijk zijn: oorlog is gewelddadig, instrumenteel en politiek (Rid, 2012).

Momenteel is het aannemelijk dat we ons in een relatief vredevolle periode bevinden. Toch lijkt het voor sommige auteurs te kort door de bocht om het huidige tijdperk als 'vredevol' te beschouwen (Monaghan, 2019, p. 88). Het gebruik van 'onconventionele' en 'ongeregelde' tactieken is niet beperkt tot het strikte Clausewitziaanse oorlogsparadigma. Met een toename in dreigingen vanuit onconventionele hoek wordt er meer en meer aandacht geschonken aan het concept van de 'grijze zone'. Een grijze zone is de ondubbelzinnige zone die zich bevindt tussen vrede en oorlog. De acties die worden ondernomen gaan verder dan louter concurrentie in vredestijd, maar ze komen niet neer op een totale oorlog. Dit kan te wijten zijn aan de dubbelzinnigheid van het internationaal recht, de dubbelzinnigheid van de acties, het attributieprobleem of omdat de impact van de acties geen reactie rechtvaardigt (Dowse & Dov Bachmann, 2019). In deze zone hebben actoren hybride strategieën gecreëerd om nog meer invloed te kunnen uitoefenen. Staten maken gebruik van instrumenten in alle dimensies van macht om hun doelen te bereiken, zoals het inzetten van economische middelen of cyberaanvallen. Dit gebeurt vaak op een illegale wijze, maar het gebruik van direct geweld is hierbij niet van toepassing. Voorbeelden hiervan zijn de Russische poging tot moord op spion Sergei Skripal en het internationale debat over Huawei als instrument van de Chinese staatsmacht.

Conflicten in de grijze zone bevinden zich meestal binnen de diplomatieke, informatie/cyber, militaire en economische domeinen (DIME). Het is een manier om invloed en macht te verkrijgen of regeringen te verzwakken, destabiliseren, ondermijnen of omver te werpen, zonder de toevlucht te nemen naar een oorlog op het terrein (Robinson, Janicke, Jones, & Maglaras, 2018). Een tactiek die hier meer en meer aan belang wint is het opzetten van cyberoperaties (Fitton, 2016). Bekende voorbeelden waarbij deze tactiek gebruikt werd zijn de cyberaanvallen op de politieke campagne van de Franse president Emmanuel Macron, het cyberconflict tussen Rusland en Estland, en de Russische beïnvloedingscampagnes in Zweden, Oekraïne en Georgië. Dergelijke aanvallen en verstoringen door cybermacht kunnen het onderscheid tussen oorlog en

vrede enorm doen vervagen. Terrorisme, en daarbij het gebruik van terroristen als *proxies* van staten, zorgde er reeds voor dat dit onderscheid niet meer duidelijk was, maar het uitbouwen van een doeltreffende cybercapaciteit gaat hierin nog een stap verder (Sheldon, 2016, p. 292).

Als het domein van de grijze zone een werkelijk terrein van conflicten vormt, dan begint het er met deze illegale instrumenten erg druk uit te zien. Wanneer is een daad nu oorlogszuchtig en wanneer niet? Wordt er niet louter gebruik gemaakt van niet-gereguleerde concurrentie in plaats van hybride oorlogsvoering? Het is duidelijk dat deze term een bepaalde mate van theoretische kwetsbaarheid inhoudt en er geen consensus bestaat of we ons nu al dan niet in een grijze zone bevinden (The Cormorant's Nest, 2020). Het beschrijft geen conceptuele ruimte, maar eerder het karakter van de tactiek die wordt gebruikt in een conflict tussen twee of meerdere entiteiten. In principe is zowel het concept van de grijze zone als dat van hybride oorlogsvoering een westerse creatie (Galeotti, 2018). Ze krijgen een nieuwe geloofwaardigheid, omdat ze voornamelijk worden toegepast op conflicten waarbij onze vijanden China en Rusland aanwezig zijn. Toch ontstaat er twijfel over de relevantie van deze concepten. Allereerst zijn ze niet nauwkeurig gedefinieerd (Stoker & Whiteside, 2020). Ten tweede lijken deze concepten geen nieuwe realiteit van conflicten te duiden (Ong, 2018). China maakte al gebruik van milities in de tijd van de Ming- en Tangdynastieën, en de informatieoorlogvoering door Rusland dateert al sinds de Koude Oorlog.

Er kan dus gesteld worden dat de ‘grijze zone’ en ‘hybride oorlogsvoering’ nog geen alomvattende realiteit is die door iedereen wordt aangehangen. Het gebruik ervan hangt grotendeels af of je gelooft in deze staat van zijn of niet. Het is wel een feit dat met deze tendensen het onderscheid tussen oorlog en vrede alsmaar moeilijker te definiëren wordt. Volgens John Raine (2019), onderzoeker aan het *International Institute for Strategic Studies* (IISS), brengt dit het gevaar met zich mee dat er op het internationale toneel wordt geaccepteerd dat deze ‘grijze zone’ een plek is waar regels niet van toepassing zijn. Dit moedigt bij alle actoren slecht gedrag aan en verhoogt het risico op misrekening en escalatie. Hierdoor is het van belang om als staat of internationale organisatie te bepalen wat kan en wat niet kan, ter bescherming van haar bevolking en kritieke infrastructuur. Indien deze soort aanvallen, verstoringen en misleidende operaties de norm worden kan dit leiden tot een soort van achtergrondruis in de dagelijkse dynamiek van de internationale betrekkingen, en lijkt het erop dat een tijdperk met constante verstoringen uitgebroken is.

2.5. Conventionele en cyberoorlogsvoering: een vergelijking

> *"Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks."* (Juncker, 2017)

Deze quote komt van de voormalige voorzitter van de Europese Commissie, Jean-Claude Juncker, die hij in zijn *State of the Union* van 2017 vermeldde. Aangezien dit toch wel een opmerkelijke uitspraak is, wordt er in deze alinea een vergelijking gemaakt van beide manieren van oorlogsvoering om te achterhalen of de stelling al dan niet gegrond is. Binnen de literatuur bestaat er een debat of oorlogsvoering in het cyberdomein al dan niet de toekomst is (Rowe N. C., 2015). Zowel conventionele als cyberoorlogen bevatten dezelfde fundamentele elementen om van een oorlog te kunnen spreken: een conflict tussen twee of meerdere actoren, het gebruik van wapens, slachtoffers, motieven en een doel. Om te onderzoeken of cyberaanvallen geschikt zijn als instrument om politieke en/of militaire doelstellingen te bereiken, is het interessant de afweging te maken waarom een natiestaat eerder *cyberspace* zou verkiezen boven conventionele technieken. Om dit te verklaren worden hieronder de voordelen tegen de nadelen afgewogen.

2.5.1. Voordelen cyber- over conventionele oorlogsvoering

Gebruik maken van het internet tijdens een militaire operatie brengt vele voordelen met zich mee. Het is namelijk heel moeilijk voor een aangevallen staat om na te gaan wie de cyberaanvallen pleegt en dit te bewijzen aan de rest van de wereld (Goel, 2011). Neil C. Rowe (2015) lijstte de verschillende elementen op die in het voordeel zijn van cyberoorlogsvoering.

Eerst en vooral beschikken cyberwapens over meer variatie dan instrumenten die worden ingezet in conventionele conflicten. Cyberaanvallen kunnen computers en netwerken op verschillende manieren uitschakelen en maken intrinsieke attributiegegevens meestal niet publiek (p.61). Hierdoor is het voor de aangevallen staat moeilijk om na te gaan door wie het wordt aangevallen. Het niet kunnen toekennen van cyberaanvallen is momenteel zowel het grootste voordeel als het grootste probleem, afhankelijk vanuit welk oogpunt de cyberaanval bekeken wordt (Mudrinich, 2012). Bij een conventionele oorlog kennen de tegenstanders elkaar wel en zijn beide actoren makkelijk te ondescheiden. Het leger draagt een uniek uniform en de militaire voertuigen zijn gemarkeerd met kentekens van hun staat. Doordat het zo moeilijk is om een staat te beschuldigen van een cyberaanval, is het aantrekkelijk voor de aanvallende staat om cyberaanvallen te gebruiken in een conflict. Geers *et al.* (2013) voorspellen dat het gebruik van cyberaanvallen alleen maar

zal toenemen. Toch is het niet onmogelijk om cyberaanvallen aan een staat toe te kennen (Mena, 2003). Het bewijs zal juridisch dan wel indirect zijn, omdat cyberaanvallen niet binnen computers kunnen worden waargenomen, maar er zijn reeds enkele sterke rechtzaken gevoerd aan de hand van deze indirecte bewijzen. Ook ontwikkelen de technieken van *datamining* uit de informatica zich in toenemende mate om cyberaanvallen op te sporen.

Het speelt ook in het voordeel van de aanvallende staat dat er geen fysieke nabijheid van het slachtoffer vereist is (Rowe N. C., 2015, p. 61). Hierdoor kan de aanvaller als een onzichtbare vijand te werk kan gaan (Brenner, 2007). Frontlinies moeten niet worden doorkruist, waardoor een aanval op een staat aan de andere kant van de wereld zonder fysieke problemen kan worden uitgevoerd.

In tegenstelling tot een conventionele oorlog zal er bij een cyberaanval geen blijvende sporen zoals DNA, vingerafdrukken, chemisch afval of dergelijke te vinden zijn (Rowe N. C., 2015, p. 62). Digitale gegevens kunnen eenvoudig worden vervalst waardoor de oorspronkelijke gegevens geheim blijven. Het is moeilijk om cyberwapens van legitieme gegevens en programma's op het internet te onderscheiden, omdat het slechts abstracte patronen van bits zijn. Ze zien er net hetzelfde uit en kunnen pas aan de hand van gedetailleerde inspectie worden onderscheiden. Hierdoor kunnen cyberwapens, zoals malware, eenvoudig via het internet verhandeld worden met tot gevolg dat kleine, minder machtige staten en terroristische groeperingen ook in de mogelijkheid zijn om deze te bemachtigen. Deze staten hebben vaak niet de middelen om conventionele wapens aan te schaffen en versterken hierdoor hun cybercapaciteit. De technologie van cyberaanvallen en cyberspionage lijken sterk op elkaar. Beide hebben de doelstelling om toegang te verkrijgen tot het computersysteem van de vijand. Vandaar is het voor een staat moeilijk te onderscheiden of de vijand een tegenaanval pleegt of aan routine spionage doet (p.62). Bovendien zijn het aantal cyberwapens en de bestaande cybercapaciteiten van een staat niet meetbaar, wat wel het geval is bij conventionele middelen.

Tot slot worden cyberaanvallen, in tegenstelling tot conventionele aanvallen, meestal niet uitgevoerd met het oogmerk om te doden (Kelsey, 2008). Hoewel dit in bepaalde gevallen wel mogelijk is, door met behulp van *hacking* de luchtverkeersleiding te verstoren, is dit meestal niet de beoogde doelstelling. Cyberaanvallen hebben vaak tot doel specifieke aanvallen te plegen op traditioneel beschermde objecten of individuen. Het doelwit kan dus sneller en eenvoudiger worden bereikt dan bij conventionele oorlogvoering. Doordat een cyberaanval niet wordt uitgevoerd om te doden, vervaagt de beoordeling of de aanval

al dan niet wettig is. Dit heeft tot gevolg dat het principe van onderscheid, tussen burgers en burgerlijke objecten enerzijds en strijders en militaire doelwitten anderzijds, veel meer wordt geschonden dan bij een conventionele aanval. Zo worden bijvoorbeeld gewone burgers ook onrechtstreeks getroffen bij een cyberaanval op het nationaal bankensysteem. Aan de ene kant is het dus een voordeel dat cyberaanvallen niet het potentieel hebben om te doden, maar aan de andere kant zorgt dit er juist voor dat er minder rekening gehouden wordt met het principe van onderscheid. Door het onderscheidingsbeginsel te negeren wordt ook het internationaal humanitair recht geschonden, dat geldt tijdens een gewapend conflict.

2.5.2. Nadelen cyber- over conventionele oorlogsvoering

Nu de voordelen van cyberoorlogsvoering aangegeven zijn, is het belangrijk om de vraag te stellen of een cyberoorlog dezelfde effecten zou bereiken als een conventionele oorlog. Binnen de literatuur zijn verschillende auteurs het hier niet mee eens (Rid, 2012), en in deze paragraaf wordt verklaard waarom.

Een van de kernelementen van een conventionele oorlog is de eindigheid ervan. Zoals de vorige definitie van Clausewitz omtrent het concept ‘oorlog’ al zei, eindigt een oorlog meestal als de ene partij de andere heeft verslagen of wanneer beide partijen oorlogsmoe zijn en vrede sluiten door een wapenstilstand (von Clausewitz, 1982, p. 101). De tegenpartij moet worden vernietigd of in een toestand gebracht waarbij ze het gevecht niet langer willen aanhouden. Om dit te bereiken moet er een bepaald niveau van fysieke vernietiging zijn. Bij een cyberaanval is er geen waarneembaar aantal dodelijke slachtoffers en is de fysieke vernietiging bijgevolg afwezig. Een eerste nadeel van cyberaanvallen is dat ze slechts, in het beste geval, een netwerk kunnen terugbrengen naar de toestand van voor het netwerk. Dit betekent de eliminatie van het netwerk. Om effectief te zijn moeten cyberaanvallen niet alleen hun doelwitten uitschakelen, maar ook de back-upmogelijkheden ervan vernietigen. Indien het doelwit eenvoudig het netwerk terug actief krijgt door een back-up, was de cyberaanval niet doeltreffend (Libicki, 2014, p. 26).

Een tweede nadeel is dat cyberaanvallen een omgekeerd effect kunnen hebben op een conflict. Ze kunnen de aangevallen staat triggeren om een conventionele oorlog te starten. Er is geen enkele regel of wet die verbiedt dat een partij niet mag reageren met conventionele middelen op een cyberaanval (Rowe N. , 2010). Een enkele cyberaanval

bereikt bovendien niet hetzelfde resultaat als een nucleaire aanval zou doen. De tegenpartij zal de cyberaanval niet zomaar langs zich laten passeren en mogelijk wraak nemen met andere middelen die ze ter beschikking hebben. Ook is de schade die conventionele wapens met zich meebrengen makkelijker in te schatten dan bij cyberwapens, waardoor staten niet altijd geneigd zijn deze risico's te nemen. De effecten van cyberaanvallen zijn vaak onvoorzien en pas waarneembaar op lange termijn (Stimpson, 2015).

Cyberaanvallen worden vanuit academisch en militair perspectief vaak gezien als strategische, asymmetrische wapens. Zoals eerder aangegeven kunnen cyberaanvallen het slagveld tussen machtige staten en staten zonder sterke militaire macht egaliseren. Toch zijn er tot op heden weinig voorbeelden van cyberaanvallen die als enige militaire optie werden gebruikt in een staat-op-staat conflict (Stimpson, 2015). De verklaring hiervoor is dat de staat geen strategisch voordeel zou winnen bij het gebruik van cyberaanvallen in het conflict. Cyberaanvallen leveren niet exact dezelfde resultaten op als conventionele wapens en trekken op die manier de doeltreffendheid van een cyberoorlog, zoals eerder gedefinieerd, in twijfel (Rid, 2012). Bij daadwerkelijke militaire operaties, zoals in Afghanistan of Irak, is er weinig tot geen bewijs dat een leger louter gebruik maakt van cyberaanvallen tegen de vijand. Israël combineerde in 2007 zowel cyberwapens als conventionele wapens in een conflict met Syrië (Stimpson, 2015). De staat verblindde Syrische luchtverdedigingsstations tijdens een bombardement door een cyberaanval. Israël maakte gebruik van het *'Suter'*-netwerkaanvalsysteem om het communicatienetwerk van Syrië binnen te dringen. Via deze technologie kon Israël het netwerk overnemen als systeembeheerder, en manipuleerden ze de sensoren in posities waarbij de naderende vliegtuigen niet in beeld werden gebracht. In dit proces moeten de vijandelijke sensoren nauwkeurig gelokaliseerd worden om deze vervolgens binnen te dringen en gegevensstromen in te sturen die misleidende data met zich meebrengt. Vervolgens wordt er met behulp van algoritmes die deze data bevat, controle over het netwerk verkregen (Gasparr, 2008).

Uit de analyse van Emilio Lasiello (2015) blijkt dat cyberaanvallen succesvoller zijn bij niet-militaire activiteiten in vredestijd. Volgens hem is het beter om de cybercapaciteit in te zetten als geheime, anonieme wapens voor het uitschakelen van systemen zonder de slachtoffers op de hoogte te brengen van de aanval. Het gebruik van cyberwapens is doeltreffender in tijden van nationale diplomatieke spanningen dan bij militaire conflicten. Het fundamentele principe van asymmetrische wapens is om de waargenomen sterkte van de tegenstander om te zetten in zijn zwakte. Dit kan door middel van

cyberaanvallen, maar software- en hardware complexiteiten, die de militaire en maatschappelijke effectiviteit en productiviteit vergroten, zijn zelf kwetsbaar om misbruikt te worden.

2.5.3. Besluit

We kunnen dus besluiten dat een staat die vandaag in bezit is van een gemilitariseerde cybercapaciteit vaak niet als een dreiging wordt ervaren, vanwege de dubbelzinnigheden over *cyberspace* en het onvermogen om fysieke schade te veroorzaken. Het is voor staten mogelijk om van cyberaanvallen gebruik te maken, maar het resultaat van de aanval zal grotendeels afhangen van de voorbereidingstijd, financiering, expertise en het profijt dat er gehaald wordt uit de kwetsbaarheden van het vijandelijke netwerk. Vanwege de verschillende factoren die noodzakelijk zijn voor een geslaagde cyberoorlog, kunnen we veronderstellen dat cyberwapens momenteel nog geen gelijke alternatieven zijn voor conventionele wapens, en dat een cyberoorlog niet volledig de fysieke oorlogsvoering zal vervangen.

Toch mogen cyberaanvallen niet onderschat worden en kunnen ze van meerwaarde zijn tijdens een militaire operatie (Stimpson, 2015), want wat zal de impact zijn van een cyberaanval die een stad of regio langer dan 24 uur onthoudt van elektriciteit of internet? Bovendien verandert technologie constant en worden offensieve cyberaanvallen steeds meer gesofisticeerd. Het is niet omdat het momenteel nog onmogelijk lijkt, dat de kans op een cyberoorlog in de toekomst een uitgesloten zaak is. De doelstellingen zullen hoogstwaarschijnlijk anders zijn dan bij een conventionele oorlog, maar het is daarom geen minder grote dreiging voor de veiligheid van een staat of organisatie. Het is dus zeer belangrijk dat de lidstaten van de NAVO niet naïef zijn in het erkennen van deze dreiging, en zich voorbereiden op deze toekomstige uitdaging.

3. De NAVO en cyberoorlogsvoering

3.1. De NAVO in *cyberspace*

Cyberspace is een geïntegreerd deel van de veiligheidsomgeving en speelt een belangrijke rol bij het verbeteren van onze operationele vermogens. De ontwikkeling van het internet zorgt ervoor dat *cybersecurity* een centraal thema binnen de internationale veiligheid is geworden. Het oude dreigingsscenario met directe interventie is vervangen door een onzichtbare vijand op het net, van wie de geografische oorsprong onbekend is (Hasanov, Iskandarov, & Sadiyev, 2019). Het alarmerendere gevoel over de zich ontwikkelende cyberdreiging tegen de geallieerde naties en de NAVO zelf, mag geen afbreuk doen aan de stappen die het bondgenootschap al heeft ondernomen om een bekwame cybercapaciteit uit te bouwen. De NAVO verklaarde in juli 2016, tijdens haar top in Warschau, dat het bondgenootschap *cyberspace* vanaf nu beschouwt als het vijfde operationeel domein naast het land, de zee, de ruimte en de lucht. Dit zorgde ervoor dat de NAVO zich naast de bescherming van haar interne netwerk ook gaat richten op de cyberverdediging van elke militaire activiteit (Shea, 2017). Shea stelt ook dat de dreigingen die *cyberspace* met zich meebrengt problematisch zijn voor onze toekomst, omdat we naast het strategische gebruik van cyber, nog steeds geconfronteerd worden met de conventionele problemen en dreigingen die we de afgelopen decennia jaar hebben proberen te bestrijden.

In hun boek *Cyber Warfare* verklaren Andress en Winterfield (2013) dat organisaties als de NAVO zeer uitgebreide cybergemeenschappen hebben. Zo werd in 2008 het *Cooperative Cyber Defense Center of Excellence* (NATO CCDCOE) in Tallinn opgericht om de defensieve cybercapaciteit van de NAVO uit te bouwen *(infra.)*. Enkele gebeurtenissen waarbij de NAVO en een van haar lidstaten betrokken raakte, liggen aan de oorsprong van de oprichting (p.68). In 1999 werd voor het eerst het systeem van het bondgenootschap zelf aangevallen door Servische hackers, toen de NAVO militaire operaties in Kosovo aan het uitvoeren was. In 2007 werd Estland aangevallen, waarbij de Russische overheid hoogstwaarschijnlijk steun verleenden aan de hackers. Ook Georgië, dat eerder het lidmaatschap van de NAVO had aangevraagd, werd het slachtoffer van verschillende cyberaanvallen tijdens het militaire treffen met Rusland (p.293-294). Deze incidenten tonen aan hoe kwetsbaar organisaties zijn die in grote mate afhankelijk zijn van informatietechnologieën. Veel lidstaten mankeren een adequaat juridisch kader om deze aanvallen het hoofd te bieden. Ook hebben deze gebeurtenissen de noodzaak voor

verandering van de cyberstrategie van de NAVO blootgelegd (Tikk, Kaska, Kadri, & Vihul, 2010, p. 101).

De geschiedenis heeft aangetoond dat het internationaal recht staten niet kan beletten van met elkaar in oorlog te gaan (p.6). Toch kan het hun gedrag bijstellen indien de vijandelijkheden zouden escaleren tot een echte oorlog. Er is dus ook nood aan een uitvoerige regulering in het cyberdomein. Hoewel het niet eenvoudig te voorspellen is of een rampzalige cyberaanval werkelijk zal leiden tot een kinetische oorlog tussen staten, is het feit dat deze dreiging überhaupt bestaat al voldoende om een doeltreffend beleid of juridisch kader uit te werken. Zowel op vlak van strategisch denken als tactische innovatie moeten deze niveaus bereid zijn met elkaar in dialoog te gaan. Technologie heeft de mensheid veranderd en bijgevolg ook de manier waarop oorlog zal worden gevoerd. Uiteindelijk zal zowel de aard van oorlog als die van veiligheid veranderen. Hoewel cyberaanvallen niet zo dodelijk zijn als strategische bommen, moet de NAVO in staat zijn om veel gecompliceerdere situaties te bestrijden zoals cyberdreigingen die uitgaan van haar rivalen (Hasanov, Iskandarov, & Sadiyev, 2019). Ook moet het bondgenootschap ervan bewust zijn dat de kans reëel is dat vijandige staten hun cybercapaciteit optimaliseren in die zin dat ze bekwaam zijn om een cyberoorlog te voeren. Hierop zal het de NAVO moeten voorbereid zijn, en blijft de vraag of een louter defensieve cybercapaciteit het hoofd kan bieden aan deze dreiging.

3.2. Soorten cyberdreigingen

Allereerst is het van essentieel belang om te duiden wat cyberaanvallen precies inhouden. Een cyberaanval bestaat uit het opzettelijk, ongelegitimeerd lanceren van een cyberwapen in software gestuurde machines. Het heeft als doel taken te vervullen aan de hand van een code die de opdrachtgever heeft ontworpen. Het concept is relatief modern en omvat een breed scala aan criminele activiteiten die uitgevoerd worden met behulp van geavanceerde informatie- en communicatietechnologieën (Albahar, 2017). Deze aanvallen vereisen minder persoonlijk contact, minder nood aan een formele organisatie en geen controle over een geografisch gebied van waaruit de activiteiten worden uitgevoerd.

Om een cyberaanval te kunnen uitvoeren heb je wapens nodig, net als bij een conventionele oorlog. De algemene term definieert wapens als gebruiksmiddelen die worden ontworpen als middel om te dreigen of om fysieke, mentale of functionele schade

aan te richten aan levende wezens of systemen (Rid & McBurney, Cyber-Weapons, 2012). Het grootste deel van de wapens zijn niet ontworpen om aan oorlogsvoering te doen, en werden tot op heden niet ingezet tijdens een interstatelijke oorlog. Dit geldt ook bij cyberwapens. De reden hiervoor is dat malware, of dergelijke kwaadaardige codes die binnen de parameters van cyberwapens vallen, ontworpen zijn om een indirecte kinetische uitkomst te verkrijgen die al dan niet kan resulteren in schade aan het doelwit. Met andere woorden, malware is op zich niet ontwikkeld om iemand te doden, te verwonden of uit te schakelen of tastbare eigendommen te beschadigen of te vernietigen (Arimatsu, 2012). In 2011 werd 'Duqu' ontdekt, een vorm van malware met als doel gegevens en middelen te verzamelen als voorbereiding op een aanval door een worm met dezelfde capaciteit als Stuxnet *(infra.).* Dit cyberwapen was niet ontworpen om fysieke schade aan te richten aan een persoon of groep, maar om informatie te accumuleren. Er zijn dus verschillende vormen van cyberwapens die staten ter beschikking hebben om hun doel(en) te bereiken.

3.2.1. Wapens aan het *high- en low potential end*

Binnen de ICT-termen worden cyberwapens geordend langs een spectrum (Rid & McBurney, Cyber-Weapons, 2012). Aan het *low-potential end* van het spectrum bestaat er kwaadaardige software, beter bekend als malware, dat ontworpen is om een systeem van buitenaf te beïnvloeden. Deze *malware* is technologisch niet in staat om het systeem binnen te dringen en directe schade aan te richten. Dit wapen kan spreekwoordelijk vergeleken worden met een paintballgeweer die iemand aan de buitenkant kan raken, maar geen fysieke schade aanricht. Aan de hand van een kwaadaardige code kan een computer geïnfecteerd worden wanneer de gebruiker een e-mailbijlage opent of op een link van een website klikt. Deze malware kan de gegevens van de computer scannen op gevoelige informatie, die vervolgens online worden doorverkocht of gebruikt bij het ontwikkelen van valse identiteitsdocumenten. Bijgevolg kunnen hackers en insiders wereldwijd toegang krijgen tot gevoelige informatie (Alexander, 2014).

Aan het *high-potential end* van het spectrum, kan malware optreden als een *intelligent agent* wat betekent dat het virus wel het vermogen heeft om binnen te dringen in een systeem, zelfs in beschermde en fysiek geïsoleerde systemen. Ook kan het op zelfstandige basis de outputprocessen gaan beïnvloeden om directe schade aan te richten. Dit soort malware kan vergeleken worden met een *unmanned automatic vehicle* (UAV), wat inhoudt dat een wapen geen ondersteuning meer nodig heeft indien het geactiveerd wordt

en zelfstandig kan opereren. Binnen het spectrum van de *low- en high-potential ends* bestaan er nog kwaadaardige software varianten die generieke systemen kunnen binnendringen, maar geen invloed hebben op het doelwit, alsook specifieke malware die wel functionele en fysieke schade kan aanrichten (Rid & McBurney, Cyber-Weapons, 2012).

3.2.2. DdoS-aanvallen en *Botnets*

Een DdoS-aanval, is een van de krachtigste wapens die kunnen worden ingezet op het internet (Weisman, 2020). Deze cyberaanvallen zijn meestal gericht op websites, netwerken en online services, waarbij hackers proberen de website onbeschikbaar te maken door deze te laten crashen. Vaak wordt er van DdoS-aanvallen gebruikgemaakt om de aandacht van het aangevallen slachtoffer af te leiden. Terwijl deze zich richt op het bestrijden van de DdoS-aanval, kan de hacker een primaire motivatie gaan nastreven, zoals het installeren van kwaadaardige software of het stelen van gegevens. Dit cyberwapen wordt vaak gebruikt door op winst gerichte cybercriminelen en natiestaten.

Een van de belangrijkste manieren waarop een DdoS-aanval kan worden uitgevoerd, is met behulp van op afstand bestuurde en gehackte computers of *'bots'*. Deze computers worden door IT-gebruikers 'zombiecomputers' genoemd en vormen een netwerk van *bots*. Het aantal kan variëren van duizenden tot miljoenen gehackte computers. Aan de hand van deze bots worden de aangevallen websites of netwerken overspoeld met meer gegevens dan haar capaciteit kan dragen, met een crash tot gevolg. Cybercriminelen gebruiken *bots* voor verschillende doeleinden, waaronder het verzenden van spamberichten en het ontwikkelen van malware zoals *ransomware*, een chantagemiddel op het internet. Vijandige natiestaten maken vaak gebruik van deze cyberwapens om de tegenstander te sabotteren. Verder in dit hoofdstuk worden enkele voorbeelden beschreven waarin NAVO-lidstaten het slachtoffer werden van DdoS-aanvallen.

3.2.3. Cyberterrorisme

Ook terroristische organisaties kunnen achter cyberaanvallen zitten die heimelijk door een natiestaat worden gesponsord, of die worden gesteund door organisaties met specifieke religieuze, politieke of culturele ideologieën. Hierbij maken Islamitische terroristische organisaties die een heilige oorlog of 'jihad' tegen het Westen hebben verklaard gebruik van het internet om hun ideologie te verspreiden, aanhangers te hersenspoelen en subversieve activiteiten te plannen om hun normale leven te verstoren

(Rollins & Wilson, 2007). Een terroristische organisatie met beperkte mankracht en infrastructuur kan met behulp van cyber vanop elke locatie aanvallen en daarbij enorme schade aanrichten. Reeds bij aanvang van de *Global War on Terror* omschreef James Lewis, onderzoeker aan het Centrum voor Strategische en Internationale Studies (CSIS), deze dreiging als "een enorme elektronische achilleshiel" (2002).

Er zijn ondertussen al verschillende terroristische cyberaanvallen gepleegd. In juli 2007 werden Younes Tsouli, Waseem Mughal en Tariq Al-Daour in het Verenigd Koninkrijk schuldig bevonden aan het aanzetten van een andere persoon tot het uitvoeren van een terroristische daad (Alexander, 2014). Deze vond plaats buiten het Verenigd Koninkrijk, maar zou, indien gepleegd in het Verenigd Koninkrijk, onder moord vallen. Hierbij gaven ze ook toe te hebben samengewerkt met andere terroristen om banken, bancontact en creditcardmaatschappijen te misleiden, alsook websites en onlineforums te hacken om literatuur en video's te verspreiden ter ondersteuning van de gewelddadige jihad. De mannen hadden een bijzondere relatie met Al Qaida in Irak en maakten van het hacken gebruik om video's de wereld in te sturen met onthoofdingen en handleidingen over het maken van een bomgordel. Een ander voorbeeld van cyberterrorisme vond plaats in 2011. Toen maakte het Turkse ministerie van Financiën bekend dat de Koerdische Arbeiderspartij, bekend als PKK, de overheidswebsite had aangevallen en propaganda op de webpagina's had geplaatst.

Ook voor ons is cyberterrorisme een reële dreiging. Nu de terroristische aanslagen op het land zijn afgenomen, werken jihadistische organisaties en groeperingen aan het verbeteren van hun offensieve en defensieve cybercapaciteit waarbij ze gebruikmaken van cybercriminele instrumenten en diensten op het *dark web* (Zerzri, 2017). Tot nu toe zijn ze er enkel in geslaagd om websites te bekladden en kleine inbraken te plegen, maar het is slechts een kwestie van tijd tegen dat deze terroristische organisaties cybercriminelen zullen rekruteren en meer geavanceerde technologie zullen aanschaffen. Hierdoor zullen ze ernstige aanvallen met een negatieve impact kunnen uitvoeren waar onder meer het Westen het doelwit zal zijn.

3.2.4. Cyberspionage

Traditioneel betekent spionage dat een natiestaat agenten (spionnen) gaat sturen naar het grondgebied van een andere natie met als doel gevoelige informatie te verkrijgen. Volgens het Handvest van de Verenigde Naties valt dit niet onder dreigingen of gebruik

van geweld, met tot gevolg dat staten geen militair geweld kunnen gebruiken uit zelfverdediging om de spionage te vergelden (Wortham, 2012, p. 652). Echter, binnen de meeste jurisdicties is spionage een strafbaar feit, omdat deze personen de territoriale integriteit van een vreemd land gaan schenden. Dit zorgt ervoor dat spionnen wel op het buitenlands grondgebied kunnen worden aangehouden en strafrechtelijk vervolgd (Scott, 1999).

Sinds de komst van het internet wordt er ook gebruikgemaakt van *cyberspace* om de tegenstander te gaan bespioneren. Hierbij worden computers of digitale communicatieactiviteiten opzettelijk ingezet om gevoelige informatie te verkrijgen over de vijand. Dit is een zeer interessant instrument voor natiestaten, omdat ze op die manier geen spionnen naar het buitenland hoeven te sturen en dus vergelding kunnen ontwijken. Sommige wetenschappers zoals Melnitzky (2012, p. 536), zijn ervan overtuigd dat het gebruik van cyberspionage indringender is dan traditionele spionage, omdat het de spionerende staat in staat stelt om herhaaldelijk grote hoeveelheden aan informatie te infiltreren zonder dat hun personeel gevaar loopt. Hij vindt ook dat cyberspionage moet vallen onder (dreiging met) gebruik van geweld of als gewapende aanval onder het Handvest van de VN. Het is echter nog steeds de opinie van de meerderheid om cyberspionage niet anders te berechten dan traditionele spionage, omdat het slechts een andere vorm van spionage is ondanks de kans op vervolging kleiner wordt (Dominik, 2019, p. 84).

3.2.5. Cyberoorlogsvoering

Cyberspace wordt door veel staten beschouwd als het vijfde domein van oorlogsvoering na land, zee, lucht en ruimte. NAVO-secretaris-generaal Jens Stoltenberg kondigde in juni 2016 aan dat "de alliantie is overeengekomen om cyber tot een operationeel domein te verklaren, ongeveer zoals de zee, de lucht en het land dat zijn" (Minárik, 2016). Het introduceren van het cyberdomein als nieuw slagveld voor militaire organisaties, brengt enkele problemen met zich mee. Door gebruik te maken van cybermacht tijdens militaire operaties, zou dit in de hedendaagse militaire doctrines als een machtsvermenigvuldiger kunnen dienen. Omwille van de toenemende afhankelijkheid van informatietechnologieën en computernetwerken tijdens militaire operaties, zou de ontwrichting ervan een strategisch voordeel kunnen bieden aan de tegenstander (Korns & Kastenberg, 2008). Daarom is het verdedigen van nationale defensiesystemen tegen

cyberaanvallen, met betrekking tot cyberoorlogsvoering, van groot belang voor de NAVO.

3.3. Vijandige natiestaten van de NAVO in *cyberspace*

De NAVO en haar bondgenoten krijgen te maken met steeds capabelere en agressievere vijanden in *cyberspace,* en moeten samenwerken en van elkaar leren om deze te kunnen tegengaan. Vijandige landen maken steeds meer gebruik van grootschalige cyberoperaties tegen Amerikaanse en Europese staten met het doel hun economieën te ontwrichten, hen te bespioneren, de militaire paraatheid te ondermijnen en de publieke opinie te manipuleren door het verspreiden van desinformatie (Holcomb, 2020). Er wordt aangenomen dat er momenteel meer dan 100 landen beschikken over een bedreigende cybercapaciteit. Voor de NAVO zijn China en Rusland momenteel het meest zorgwekkend (Alexander, 2014). Cyberconflicten tussen natiestaten zijn vaak een afspiegeling van de traditionele conflicten. Zo maakt China bijvoorbeeld gebruik van cyberaanvallen op een grote schaal, juist zoals het gebruik maakte van de infanterie op grote schaal tijdens de Koreaanse oorlog (Geers K. , Kindlund, Moran, & Rachwald, 2013). De Chinese soldaten werden toen het slagveld ingestuurd met slechts een handvol kogels, maar vanwege hun sterkte in aantal, waren ze toch in staat om de tegenstanders te verslaan. Daarnaast heb je ook Rusland, de Verenigde Staten en Iran. Hun tactieken in *cyberspace* zijn eerder afhankelijk van geavanceerde technologieën en vooruitstrevende werk van werknemers die gedreven worden door concurrentie en financiële prikkels. Hieronder wordt een kort overzicht gegeven van enkele opkomende cybermachten die in het oog moeten worden gehouden door de NAVO, namelijk: China, Rusland, Iran en Noord-Korea.

3.3.1. China

De Volksrepubliek China is momenteel de grootste cybermacht die een bedreiging vormt voor het Westen. De enorme bevolking en snelgroeiende economie liggen hiervoor aan de basis. Door gebruik te maken van deze troeven, voert het land een geduldig en assertief buitenlands beleid dat bepaalt hoe informatie- en communicatietechnologieën moeten worden bestuurd en ingezet (Inkster, 2016, p. 9). China heeft in het verleden al verschillende westerse multinationals zoals Google en Intel gehackt (Geers K. , Kindlund, Moran, & Rachwald, 2013). Ook verschillende mediakanalen zoals de New York Times en Washington Post werden reeds het slachtoffer van Chinese cyberaanvallen. Door het

gebruik van cyberaanvallen kreeg China toegang tot vertrouwelijke informatie, zoals gegevens over onderzoek en ontwikkeling of tot gevoelige communicatie van hoge overheidsfunctionarissen en Chinese politieke dissidenten.

China's agressieve aanpak om cyberoperaties te gebruiken met de intentie om nationale en politieke doelen te bereiken is drastisch verschillend van de cyberstrategie van de meeste andere landen. Deze laatsten maken eerder gebruik van een voorzichtige en weloverwogen aanpak. Aanvallers die gesteund worden door China proberen persoonlijke informatie over Amerikaanse en Europese burgers te verkrijgen, alsook handelsgeheimen en intellectuele eigendom van deze overheidsinstanties. Naarmate de doelstellingen van China verschuiven om haar reikwijdte op het internationale toneel te vergroten, is haar cybercapaciteit meer en meer gericht op het onderdrukken van buitenlandse en binnenlandse tegenstanders die kritisch staan tegenover de Chinese Communistische Partij (Intsights, 2020). Het regime in Peking heeft de laatste jaren geavanceerde cyberoperaties uitgevoerd met behulp van *hacking,* op zoek naar manieren om belangrijke politici in Europa te chanteren of te overtuigen om de Chinese geopolitieke belangen welwillender te benaderen (Bugajski, 2019). Bovendien heeft China sinds het begin van de coronacrisis bijgedragen aan het verspreiden van COVID-gerelateerde desinformatie, en hebben verschillende EU-leiders verbanden gesuggereerd tussen China en pogingen op het hacken van Europese ziekenhuizen. Hierdoor liggen de inspanningen van China, om de 5G-capaciteit van het aan de staat gelieerde bedrijf Huawei in Europa in te voeren, onder vuur (Holcomb, 2020).

Ook wordt er in China gebruikgemaakt van publiek-private partnerschappen bij cyberspionage (Kaska, Beckvard, & Minarik, 2019). Hierdoor gaan private actoren ten behoeve van de Chinese overheid aan economische spionage en beïnvloedingsoperaties gaan meewerken. Chinese bedrijven zijn in principe wettelijk verplicht om samen te werken met de regering ter ondersteuning van de Chinese nationale belangen, en hieronder valt ook de deelname aan activiteiten om inlichtingen te onderscheppen. China maakt er op het internationale toneel dan ook geen geheim van dat het de ambitie heeft om het door het Westen gedomineerde wereldsysteem opnieuw vorm te geven. Een onderzoek van verschillende FireEye-experten ontdekte dat China vaak gebruikmaakt van *brute-force attacks* (Geers, Kindlund, & Moran, 2014). Hierbij maken hackers gebruik van een bepaalde software die verschillende combinaties inlognamen- en wachtwoorden uitprobeert, totdat het de juiste combinatie heeft bereikt om te kunnen inloggen in het systeem of netwerk (Petters, 2020). Chinese cyberaanvallen vormen niet

enkel een groot risico voor het primaire doelwit, maar ook voor landen die economische, sociale, militaire of politieke landen hebben met de aangevallen staat. Het lijkt dus duidelijk dat een multinationale aanpak nodig is om de westerse landen te beveiligen in *cyberspace*.

3.3.2. Rusland

Vandaag de dag is Rusland de thuisbasis van de meest complexe en geavanceerde cyberaanvallen die tot op heden zijn ontdekt. De cybermacht maakt gebruik van gesofisticeerde malware die zelfs heimelijker is dan die van haar Chinese tegenhanger. De Russische *'Red October'*-campagne uit 2012 is hier een prominent voorbeeld van (Geers K. , Kindlund, Moran, & Rachwald, 2013). Dit was een cyberaanval gericht op miljoenen burgers wereldwijd, maar voornamelijk landen uit de voormalige Sovjet-Unie werden getroffen. Onder meer ambassades, onderzoeksbedrijven, militaire bases, energieleveranciers, nucleaire agentschappen en infrastructuur waren doelwitten van de cyberaanval. Vanwege de zogenaamde 'digitale soevereiniteit' creëert Rusland een asymmetrisch voordeel in *cyberspace*. Deze 'structurele cyberasymmetrie' is zowel een defensief als offensief middel van hun nationale cybermacht. Door *cyberspace* op technisch, syntactisch en semantisch niveau vorm te geven en het nationaal netwerk te begrenzen met technische, administratieve en politieke instrumenten, verkrijgt Rusland een onevenredig militair voordeel op strategisch niveau (Kukkola, 2018). In het Russische buitenlandse beleid hebben informatieoperaties namelijk een strategische betekenis als onderdeel van 'informatie-psychologische onderdelen' om de internationale politiek te beïnvloeden (Ford, 2010).

Bij de NAVO staat Rusland bekend voor zijn onwettige inmenging in het cybernetwerk van westerse democratieën, en als agressor van cyberaanvallen op (militaire) instellingen en bedrijven die verantwoordelijk zijn voor kritieke nationale infrastructuur en burgers (Machiels, 2019). Valeray Gerasimov, generaal van de Russische defensie, wordt gezien als de architect van de hybride tactieken van het land. Zijn Gerasimov-doctrine is een combinatie van informatieoperaties en cyberaanvallen met conventionele hefbomen om de agressieve geopolitieke doelen van Rusland te bereiken (Parsons & Raff, Understanding the Cyber Threat From Russia, 2019). Op deze manier loopt het land geen risico op een gewapend conflict met de vijandelijke NAVO-leden. Deze aanpak is al meerdere keren met succes getest bij aanvallen op Estland, Georgië en Oekraïne *(infra.)*. De doelstellingen van Rusland zijn niet per se destructief. In plaats hiervan probeert het

Kremlin toegang te krijgen tot organisaties, onder meer om macht te projecteren, maar ook ter voorbereiding voor mochten de vijandelijkheden toch escaleren. In Rusland is er ook een duidelijke trend naar het 'bewapenen' van informatie. Hierbij gaat het Kremlin misbruik gaan maken van mediakanalen zoals sociale-mediaplatforms met als doel de publieke opinie te beïnvloeden en ook de geloofwaardigheid van bepaalde bronnen te verzwakken.

Rusland heeft naast politieke tegenstanders ook publieke en private organisaties als doelwit. Zo lekten Russische cybercriminelen gestolen e-mails van de Democratische presidentskandidate Hilary Clinton met als doel haar kandidatuur te ondermijnen. Met behulp van deze e-mails werd de aandacht gevestigd op haar banden met een Amerikaanse investeringsbank (Whittaker, 2019). Dit betekent ook dat organisaties en bedrijven het risico van bijkomende schade moeten erkennen bij pogingen van Rusland om zijn tegenstanders te destabiliseren.

In januari 2021 sloot Rusland een samenwerkingsakkoord met Iran omtrent cyberveiligheid en informatie- en communicatietechnologie. Deze overeenkomst is vooral gericht op het delen van inlichtingen en het verbeteren van de offensieve cybercapaciteit, in plaats van het delen van offensieve capaciteiten. Deze samenwerking zou weleens een nieuwe bedreiging kunnen vormen voor de veiligheid van het bondgenootschap, meer bepaald van de Verenigde Staten, alsook van het Midden-Oosten (Net Politics, 2021).

3.3.3. Iran

Toen de Verenigde Staten zich in 2018 terugtrok uit de nucleaire deal met Iran, hingen er geruchten rond over Iraanse vergeldingsacties in het cyberdomein (Brennan, 2018). Het Iraanse regime heeft de laatste decennia duidelijk een grotere honger naar destructieve of ontwrichtende cyberaanvallen in vergelijking met andere landen in de wereld. Dit mede, omdat haar nucleaire installaties in 2010 zelf het slachtoffer werden van het Amerikaanse en Israëlische Stuxnet-virus. Sindsdien heeft Iran een sterk motief om te investeren in offensieve cybercapaciteiten (Gulf International Forum, 2020). In 2012 infecteerde Iran de toen recente 32-bits NT-besturingssystemen van Microsoft Windows. In 2016 werd het virus tijdens een nieuwe cyberaanval gebruikt, gericht op het beschadigen van de nationale oliemaatschappijen Saudi Aramco (Saudi-Arabië) en RasGas (Qatar). Duizenden werkstations van Saudi Aramco werden onbruikbaar, alsook verschillende

Saudische ministeries en andere grote organisaties. Deze agressieve cyberaanval werd niet vergolden door Iraanse tegenstanders, waardoor het regime zich gestimuleerd voelt om zijn cyberoperaties en -capaciteiten verder uit te bouwen (Parsons & Michael, 2019).

Iran heeft een goed inzicht in het gebruik van cyberaanvallen als instrument van de nationale macht. Het land heeft reeds ervaring met geheime activiteiten en op deze manier bepaalt het de strategie en operaties. Hierbij wordt cyber meer en meer ingezet als instrument voor dwang en geweld, en heeft het een geraffineerde organisatiestructuur gecreëerd om cyberconflicten te domineren (Lewis J. A., 2019). Iran staat erom gekend geavanceerde en offensieve technieken van andere prominente cybermachten over te nemen. Hierdoor kan de ontwikkeling van haar cybercapaciteit versneld worden, en tegelijkertijd bemoeilijkt het de attributie, wat de NAVO en haar bondgenoten voor unieke uitdagingen stelt (Parsons & Michael, 2019).

3.3.4. Noord-Korea

Noord-Korea is tot slot ook een opkomende en bedreigende cybermacht. De afgelopen zes jaar werd het land al meerdere keren verantwoordelijk gehouden voor een aantal cyberaanvallen die enorm veel schade hebben veroorzaakt, zoals ontwrichting en financiële verliezen (Parsons & Bureau, 2019). Noord-Korea heeft haar cybercapaciteit doorheen de jaren uitgebreid. In het verleden hield het land zich vooral bezig met het bespioneren van Zuid-Korea (Soendergaard Larsen, 2021). De laatste jaren is het overgegaan tot cybercriminaliteit, zoals het stelen van grote sommen geld en geavanceerde technologie. In de context van een multidimensionale machtsstrijd, zijn de cyberaanvallen van Noord-Korea op instellingen voor financiële dienstverlening een middel om de economische druk te verlichten. Dit wordt veroorzaakt door de enorme sancties, opgelegd door internationale organisaties en natiestaten als vergelding voor het Noord-Koreaanse kernwapenprogramma (Parsons & Bureau, 2019). De uitbreiding van de cybercapaciteit wordt enorm gesteund door de Noord-Koreaanse leider Kim Jong Un. Volgens de Zuid-Koreaanse Nationale Inlichtingendienst, verklaarde hij in 2013 dat hij cyberoorlogsvoering, naast kernwapens en raketten, als een potentieel middel ziet om alle doelwitten te verslaan die de Noord-Koreaanse Volksstrijdkrachten een meedogenloze slagvaardigheid garandeert (Ji Young, Kyoung Gon, Kim, & Jong In, Lim, 2019).

Eind 2017 werd Noord-Korea ervan beschuldigd dat het achter de *WannaCry-ransomware* zat. Hierbij werden er ruim 230 000 computers geaffecteerd in meer dan 150

landen. De schade was ongekend in omvang. Zo vielen er ziekenhuizen uit in Groot-Brittannië, telefoonmaatschappijen in Spanje en transportbedrijven in Amerika (Innvolve, 2017). De verwoestende impact die de *ransomware* met zich meebracht in combinatie met Noord-Korea's kernwapenprogramma winden er geen doekjes om dat het conflict zich stilaan aan het uitbreiden is naar het cyberdomein. De reden waarom Noord-Korea erin slaagt een serieuze cyberdreiging te worden is zeer simpel. Technisch gezien is het misschien niet de meest geavanceerde en gesofisticeerde speler, maar andere landen hebben niet veel mogelijkheden om het land zowel binnen als buiten *cyberspace* af te schrikken. Dit geeft het land een uniek asymmetrisch voordeel in *cyberspace* (Jun, 2018).

3.4. Cyberaanvallen tegen NAVO-lidstaten

Nu er een evaluatie gemaakt is van de soorten cyberdreigingen en welke vijandige natiestaten in *cyberspace* actief zijn, heerst de vraag of we al reeds een cyberoorlog hebben meegemaakt? Deze vraagt wordt door academici nog enorm betwist. Als we kijken naar de definitie van cyberoorlog die in deze dissertatie wordt gehanteerd, kan er gesteld worden dat er tot op heden nog geen cyberoorlog heeft plaatsgevonden. Ook heeft geen enkele statelijke actor officieel een oorlog in *cyberspace* verklaard, maar in 2007 werden een reeks ernstige cyberaanvallen uitgevoerd tegen Estland, die een enorme impact hadden op de samenleving. Amper een jaar later werd ook Georgië getroffen door een combinatie van gecoördineerde cyber- en kinetische aanvallen. Bij deze incidenten was de kritieke infrastructuur van natiestaten het doelwit en kan militaire vergelding in het cyberdomein een mogelijkheid zijn om terug te slaan. Doordat Estland een bondgenoot is van de NAVO en Georgië een kandidaat-lidstaat, hadden deze aanvallen zeker een impact op de organisatie en haar beleid. Nog andere cyberincidenten hebben het bondgenootschap getroffen, en om deze cyberdreigingen en actoren beter te begrijpen zal deze sectie enkele cyberaanvallen analyseren waarin de NAVO direct of indirect getroffen werd.

3.4.1. Servië (1999)

Achtergrond

Kosovo is gelegen in het zuiden van Servië en heeft een gemengde bevolking waarvan de meerderheid van Albanese afkomst is. De regio was in grote mate autonoom binnen het voormalige Joegoslavië, tot in 1989, de Servische leider Slobodan Milosevic de status van de regio veranderde door de autonomie op te heffen en het land onder directe controle van Servië te brengen (Tikk, Kaska, Kadri, & Vihul, 2010). De Albanese Kosovaren

waren het hier niet mee eens en verzetten zich hiertegen. In 1998 leidde een open conflict tussen Servische militaire troepen en de politie enerzijds en Kosovo-Albanese troepen anderzijds, tot de dood van meer dan 1500 Kosovaarse Albanezen en het verdrijven van meer dan 400 000 mensen uit hun thuisland. De escalatie van het conflict baarde de internationale gemeenschap zorgen, voornamelijk om humanitaire redenen, maar ook voor het risico op uitbreiding naar andere landen uit het voormalige Joegoslavië.

Binnen de Organisatie voor Veiligheid en Samenwerking in Europa (OVSE) werd overeengekomen een verificatiemissie in Kosovo op te zetten, om ter plaatse toe te zien of de regels werden nageleefd en het conflict niet verder escaleert. Hierbij werden ook NAVO-troepen ingezet om toezicht te houden vanuit de lucht (NATO, NATO's role in relation to the conflict in Kosovo, 1999).

Cyberaanvallen

In 1999 werd de NAVO voor het eerst geconfronteerd met een resem cyberaanvallen (Hasanov, Iskandarov, & Sadiyev, 2019). De website en e-mailservers van de organisatie werden toen geblokkeerd als reactie op de luchtaanvallen boven Servië. Deze aanvallen werden uitgevoerd door Russische, Chinese en Servische hackers. De aanval was gericht tegen de webserver van het NAVO-hoofdkwartier in Brussel en omvatte een DDoS-aanval waarbij de e-mailserver van de NAVO werd overbelast (Verton, 1999). Volgens Denning (1999) verspreidden hacktivisten ook online propaganda en beschadigden ze de computersystemen van de NAVO met behulp van malware. De schade voor de ontvanger kwam voort uit virussen die als bijlage in een e-mail waren gevoegd, en bevatte een platte tekst of een anti-NAVO cartoon. Op deze manier werd de NAVO voor het eerst zelf getroffen in *cyberspace*. Er kan gesteld worden dat het bondgenootschap een strategisch nadeel ondervond in het cyberdomein, omdat het nog geen capaciteit had om terug te slaan.

Reactie NAVO

Vanaf toen werd het duidelijk dat de NAVO tekortschoot in het beveiligen van haar onlinenetwerk. Als reactie op de cyberaanvallen ondernam de NAVO verschillende stappen om haar servers te upgraden. Chris Scheurweghs, toenmalig hoofd van de NAVO's Integrated Data Service, verklaarde toen: *"There are two lessons that governments everywhere have learned from these attacks. First, we will have to invest much more in security, and... the Internet is no longer just a side issue"* (Verton, 1999).

Sinds de eeuwwisseling heeft de NAVO verschillende toppen gehouden om onder andere de uitdagingen in *cyberspace* in kaart te brengen en hun beleid hieraan bij te stellen. De *Prague Summit* (2002) was de eerste NAVO-top die plaatsvond met de leden van de voormalige Sovjet-Unie, en had tot doelstelling de toekomstige uitdagingen in kaart te brengen, en na te gaan op welke manier er in collectief verband op kon gereageerd worden. De aandacht werd grotendeels gevestigd op het bestrijden van terrorisme en de verspreiding van massavernietigingswapens. Wat deze top zo relevant maakt voor dit onderzoek is de eerste verwijzing naar 'cyberaanvallen' als een potentiële dreiging. In de verklaring van deze top werd aangegeven dat de NAVO-lidstaten besloten om *'hun mogelijkheden te versterken in de verdediging tegen cyberaanvallen.'* (NATO, 2002) Naast deze korte verwijzing werd er geen duiding meer gegeven over wat hier precies van verwacht werd. Toch is deze top essentieel geweest in het erkennen van cyberaanvallen als een toekomstige uitdaging voor de alliantie (Hasanov, Iskandarov, & Sadiyev, 2019). In 2003 ondertekenden negen NAVO-lidstaten (Canada, Frankrijk, Duitsland, Italië, Nederland, Noorwegen, Spanje, het Verenigd Koninkrijk en de Verenigde Staten) een akkoord om informatie over cyberveiligheid te delen. Later dat jaar werd de *NATO Computer Incident Response Capability (NCIRC)* opgericht. Deze instantie staat in voor de bescherming van de NAVO-netwerken en het behandelen en rapporteren van incidenten, waarbij de informatie wordt doorgespeeld naar het systeem- en beveiligingsbeheer van de organisatie.

3.4.2. Estland (2007)

Achtergrond

Op 27 april 2007 werd Estland getroffen door een reeks cyberaanvallen (Ottis, 2018). De aanleiding van deze aanvallen was het verhuizen van een Russisch standbeeld, *'The Bronze Soldier'* van het centrum van Tallinn naar een minder prominente militaire begraafplaats aan de rand van de hoofdstad. Dit standbeeld is een gedenkteken voor het Rode Leger van de voormalige Sovjet-Unie en werd gemaakt om de bevrijding van Estland te vieren. Helaas ziet de Estse bevolking dit standbeeld niet als een bevrijding, omdat het land net als Polen, Letland en Litouwen in het begin van de jaren '40 werd binnengevallen door de Sovjet-Unie toen deze nog een bondgenoot was van nazi-Duitsland. Toen de regering besloot het standbeeld te verplaatsen, ontstond er een opstand vanuit de Russische gemeenschap die ongeveer een kwart van de Estse bevolking bedraagt. Jonge Russen die zich door het nationalisme lieten meeslepen, kwamen op straat om te betogen tegen de verplaatsing, waardoor er rellen ontstonden met de politie.

Het werd een bloederige betoging, waarbij meer dan 800 demonstranten werden gearresteerd.

Cyberaanvallen

Enkele dagen later kwam de echte aanval: een elektronisch bombardement met een ongeziene omvang (Tikk, Kaska, Kadri, & Vihul, 2010). Om middernacht op 9 mei, de dag waarop de Russen de overwinning op nazi-Duitsland vieren, werd de wereld op het internet plots donker. *Bots* van over heel de wereld lanceerden plotseling een DdoS-cyberaanval die tot doel had het hele land plat te leggen. Dit was de eerste cyberaanval die gericht was tegen één land. Het had een enorme impact op de kritieke infrastructuur van het land. Dagenlang lag het e-bankingsysteem stil, alsook de online banktransacties en de websites van ministeries en verschillende politieke partijen. Internetsites die normaal duizend hits per dag krijgen, kregen plots honderdduizenden hits per seconde. Hierdoor lag heel het land elektronisch plat en werd de hele Estse bevolking zwaar getroffen.

Al snel wezen Estse functionarissen, zoals minister van Buitenlandse Zaken Urmas Paet, met de vinger naar Rusland (Herzog, 2011, p. 51). Hoewel technische deskundigen van de Europese Commissie en de NAVO geen geloofwaardig bewijs vonden voor de deelname van het Kremlin aan deze DDoS-aanvallen, had het wel een zeker motief (p.53). Na het verplaatsen van de Bronzen Soldaat en de rellen tussen de Russische demonstranten en de politie, beschuldigden Russische functionarissen Estland van mensenrechtenschendingen en eisten dat toenmalig premier Andrus Ansip zijn excuses aanbood en aftrad.

Ondanks Rusland elke betrekking met de cyberaanvallen ontkende, werd het er toch van verdacht door de NAVO. Het was voor het bondgenootschap duidelijk dat dit een gecoördineerde cyberaanval was. Vanwege de economische interdependentie en de dreiging van nucleaire escalatie, kan Rusland geen aanvallen op NAVO-lidstaten riskeren, en ook het feit dat de conventionele NAVO-strijdkrachten aanzienlijk groter zijn dan die van Rusland, zorgt ervoor dat aanvallen in *cyberspace* een zeer aantrekkelijk alternatief is. Een conventionele aanval op Rusland zou namelijk Artikel 5 van de NAVO in gang zetten, dit zou de energierijkdom in gevaar kunnen brengen die aan de basis ligt van de groeiende Russische invloed op het internationale toneel (Tikk, Kaska, Kadri, & Vihul, 2010).

Reactie NAVO

Hoewel de NAVO na de Servische cyberaanvallen acht jaar de tijd heeft gehad om zich voor te bereiden en de bondgenoten beter te beveiligen, is zij er in 2007 niet in geslaagd om Estland te behoeden voor cyberaanvallen. De impact van deze cyberaanvallen op de samenleving van Estland, werd een *wake-up call* voor de internationale gemeenschap (Herzog, 2011, p. 56). Vanaf toen was het duidelijk dat lidstaten van de NAVO en haar kritieke infrastructuur het doelwit kunnen worden van een cyberaanval, en dat ze zichzelf veel beter moeten beschermen. Het bondgenootschap had geen cyberstrategie, noch een cyberbeleid. Er werd ook aangetoond dat zelfs Artikel 5 van de NAVO geen garantie was om de soevereiniteit van een natiestaat in *cyberspace* te kunnen waarborgen, want vanwege het attributieprobleem kon het artikel niet van kracht gaan. Bovendien kan deze gebeurtenis andere actoren zoals hackers en natiestaten aanmoedigen in de verdere ontwikkeling en verbetering van hun eigen cybercapaciteit.

De geallieerde ministers van defensie kwamen na het incident bijeen om werk te maken van een concrete cyberdefensie (Joubert, 2012). Het bondgenootschap had zijn les geleerd en verbeterde zowel het vermogen om te reageren op cyberaanvallen, als de beleidsprocedures. Helaas speelde er een jaar na de cyberaanval op Estland een gelijkaardig scenario af in Georgië.

3.4.3. Georgië (2008)

Achtergrond

Deze cyberaanvallen moeten in de context geplaatst worden van het jarenlange conflict tussen Rusland en Georgië, kandidaat-lidstaat van de NAVO (Hollis, 2011). De oorlog in Zuid-Ossetië in 1992 en de Abchazische oorlog in 1993 resulteerden in het verlies van Georgische regio's aan pro-Russische de facto staten. Na enkele weken van groeiende onenigheid over de toekomst van het Zuid-Ossetische grondgebied, ontaarde het conflict in een oorlog. Op 7 augustus 2008 lanceerden Georgische troepen een militaire aanval op Zuid-Ossetië en beschoten de stad Tskhinvali als reactie op de vermeende Russische provocatie. Als reactie zette Rusland ook gevechtstroepen en strijdkrachten op zee in om Georgië te bestrijden. Georgië kende een strategische nederlaag, waardoor ongeveer 25 000 inwoners Zuid-Ossetië moesten ontvluchten en terugkeren naar eigen land. De Russisch-Georgische oorlog schreef om verschillende redenen geschiedenis, onder

andere omdat deze aanval de eerste gecoördineerde aanval was in het cyberdomein gecombineerd met conventionele technieken uit andere oorlogsdomeinen.

Cyberaanvallen

Drie weken voordat de schietoorlog tussen Georgië en Rusland aanving, werden Georgische websites voor getroffen door cyberaanvallen. Deze aanvallen omvatten diverse DdoS-aanvallen met de bedoeling communicatie onmogelijk te maken of te verstoren, alsook informatie over militaire en politieke inlichtingen te exfiltreren (Hollis, 2011). Onder meer de website van de Georgische president Mikheil Saakashvili werd meer dan 24 uur stil gelegd, door middel van een DdoS-aanval. Ook tijdens het conflict, op 8 augustus, werden sites van de regering, verschillende ministeries, nieuwsplatforms, en commerciële banken aangevallen (Tikk, Kaska, Kadri, & Vihul, 2010). Doordat de *cybersecurity* experten deze aanvallen maar niet onder controle kregen, bracht het Georgische ministerie van Buitenlandse Zaken op 11 augustus een persbericht uit, waarin werd meegedeeld dat een cyberoorlogscampagne van Rusland vele Georgische websites treft, waaronder die van het ministerie van Buitenlandse Zaken. De verklaring kon worden verspreid via een vervangende website die het ministerie had opgebouwd op de *blog hosting* dienst van Google.

Pas op 12 augustus nam het aantal waargenomen botnetaanvallen tegen overheidswebsites af, en veranderde het aanvalsmodel in het gebruik van een Microsoft Windows batchbestand dat speciaal ontworpen was om Georgische websites aan te vallen (Hollis, 2011). Nog een dag later meldde beveiligingsorganisatie Shadowserver dat enorm veel aanvallen op Georgische overheidswebsites van Russische computers afkomstig waren. Uiteindelijk vond op 27 augustus de laatste cyberaanval plaats, waarbij het Georgische Ministerie van Buitenlandse Zaken het doelwit was. De webserver werd overbelast met een resem aanvallen. Sindsdien nam het aantal aanvallen af, omdat ze met succes werden geblokkeerd.

Reactie NAVO

Aangezien Georgië nog geen lid was van het bondgenootschap, kon de NAVO niet rechtstreeks ingrijpen (Hasanov, Iskandarov, & Sadiyev, 2019). Het was op initiatief van de Estse regering dat een groep onderzoekers naar Georgië werd gestuurd om de toenemende aanvallen te bestrijden. Dankzij hen werd het informatiesysteem van Georgië genormaliseerd. Hierna kwamen de NAVO-lidstaten terug samen tijdens de Top van Boekarest (2008) om het concept ‘cyberdefensie’ concreet vorm te geven. Er werd

overeengekomen dat de nationale autoriteiten op het gebied van cyberdefensie moest worden versterkt, en dat lidstaten elkaar moeten bijstaan in *cyberspace*, alsook bij het delen van hun ervaringen omtrent cyberkwesties. In het kort bestonden de hoofdlijnen van het cyberbeleid, dat tijdens deze top ontstond uit: *'het benadrukken van de bescherming van belangrijke informatiesystemen'; 'optimale werkmethoden voor de verdediging in cyberspace met elkaar delen'; 'het ontwikkelen van de capaciteit om geallieerde naties, op verzoek, te steunen bij het bestrijden van cyberaanvallen'; 'het uitbouwen van optimale cyberverdedigingscapaciteiten van de NAVO'; en 'de koppeling tussen de NAVO en de nationale autoriteiten versterken'* (Caton, 2016).

Na deze top vonden er twee belangrijke ontwikkelingen plaats. Er werd een *NATO Cyber Defense Management Authority* opgericht met als doel de cyberdefensiecapaciteit te centraliseren onder één autoriteit om zo de operationele slagkracht te vergroten. Daarnaast was er ook de totstandkoming van het Cooperative Cyber Defense Center of Excellence (CCD COE) in Estland (Bicakci, 2014). In 2009 vond er opnieuw een top plaats in de Franse stad Strasbourg-Kehl. Hier besloten de geallieerde leiders om hun reactievermogen op cyberincidenten te verbeteren. Tijdens deze top bracht de Parlementaire Vergadering van de NAVO een gedetailleerd rapport uit genaamd *'NATO and Cyber Defense'*. In dit rapport werden kritieke kwesties in het cyberdomein met betrekking tot de NAVO besproken (Caton, 2016). Voor het eerst had de NAVO significante beleidsimplementaties en institutionele ontwikkelingen doorgevoerd om zichzelf te beschermen tegen cyberdreigingen. Het bondgenootschap streefde ook een strategie na om de veiligheid van haar leden in *cyberspace* te verbeteren, met zowel coördinerende maatregelen als afschrikking.

3.4.4. Oekraïne (2014)

Achtergrond

Vanwege zijn strategische en geopolitieke betekenis is de Krim al lang het toneel van politieke en militaire strijd. Zo vochten de toenmalige grootmachten tussen 1853 en 1856 in de Krimoorlog, wat tot op heden nog steeds gekend is als een van de meest kritieke oorlogen uit de moderne geschiedenis. In het najaar van 2013 laaiden de gemoederen terug op (Dennekamp, 2020). Oekraïne kreeg namelijk de kans om een associatieverdrag te tekenen met de Europese Unie, maar op het laatste moment werd het door Moskou overtuigd om hier niet mee in te stemmen, en in de plaats een economische deal met Rusland te sluiten. Al snel volgde een pro-Europese opstand op het schiereiland. Rusland

en de pro-Russische rebellen vonden deze opstand zeer bedreigend voor de Russische inwoners van de Krim, waardoor ze van mening waren dat het schiereiland annexeren een legitieme optie was om hen te beschermen. In de zomer van 2014 escaleerde het conflict nadat de Russische rebellen dachten een transportvliegtuig te hebben neergehaald, maar in werkelijkheid was het het passagiersvliegtuig MH17.

Cyberaanvallen

Vanwege de Euromaidan-protesten in het voorjaar van 2014 en het daaruit voortvloeiende conflict, werden instellingen en mediakanalen in zowel Oekraïne als Rusland getroffen door DdoS-aanvallen, *defacement* (aanpassen) van websites en *Remote Access Tools* (RAT's) om gehackte computers vanop afstand te beheren (Baezner & Robin, 2018). Deze cyberaanvallen werden ingezet om de vijand te ontwrichten, te bespioneren en schade toe te brengen. Niet-statelijke actoren werden gebruikt als proxies om deze aanvallen uit te voeren, waardoor de strijdende partijen hun betrokkenheid bij de acties in *cyberspace* konden ontkennen. Hackers voerden ook een campagne tegen de NAVO door haar overheidswebsites en e-mailnetwerken te verstoren, en mediakanalen te blokkeren (Croft & Apps, 2014). Een groep die zichzelf 'Cyber Berkut' noemt, claimde dat de cyberaanvallen werden uitgevoerd door Patriottische Oekraïners die kwaad waren over de inmenging van de NAVO in hun land.

Deze cyberaanvallen hadden enorme sociale en politieke effecten op Oekraïne. Zo was er een overaanbod van nieuws- en informatiebronnen over de Krim en Rusland, en lag de geloofwaardigheid en het vertrouwen in de Oekraïense regering lag onder vuur. Ook mogen de economische effecten niet onderschat worden zoals de bijkomende reputatieschade, de schade aan websites en de kosten om apparatuur te vervangen na cyberaanvallen op het Oekraïense elektriciteitsnet.

Reactie NAVO

Net zoals bij de cyberaanvallen op Estland en Georgië is er opnieuw geen concreet bewijs wie er achter de aanvallen zat. Toch was het opnieuw overduidelijk dat alle cybercampagnes en -aanvallen in functie waren van het dienen van de strategische en operationele doelen van Rusland. In de nasleep van deze cyberaanvallen op Oekraïne, veroordeelde de NAVO de onwettige acties en riep Moskou op om zijn militaire bezetting weg te halen uit de Krim en langs de Oekraïense grenzen. Onmiddellijk na de top in Wales (2014) bevestigden de geallieerde regeringsleiders hun steun voor de soevereiniteit van Oekraïne, en richtten ze vijf veiligheidsfondsen om met als doel de defensiecapaciteiten

van Oekraïne te versterken (NATO, 2016). Een van deze fondsen was bestemd voor de oprichting van een doeltreffende cyberdefensie, en hieronder viel het verstrekken van technische opleiding, uitrusting en bijstand door de bondgenoten.

Medvedev (2015) concludeerde bij het analyseren van dit conflict dat deze cyberoperaties, uitgevoerd door Russische surrogaten, de legitimiteit van Oekraïne hebben ondermijnd, alsook de NAVO in verlegenheid heeft gebracht en de oppositiekrachten heeft geïntimideerd (p.26). Het is opnieuw duidelijk dat zowel staten, individuele actoren, en collectieve organisaties zoals de NAVO doeltreffendere maatregelen moeten nemen om zich te verdedigen in *cyberspace* en eventueel kunnen terugslaan.

3.4.5. Andere cyberincidenten

Er werd bewust gekozen voor het beschrijven van deze vier incidenten, omdat ze een verandering betekenden voor de NAVO haar beleid en strategie. Toch zijn deze cases maar een glimp van het aantal cyberaanvallen waarmee de NAVO en haar lidstaten reeds werd geconfronteerd.

In 2010 infecteerde NAVO-lidstaat de Verenigde Staten en Israël een nucleaire kerncentrale in Iran met succes. De Amerikaanse en Israëlische betrokkenheid werd onthuld in het boek *Confront and Conceal* van de Amerikaanse journalist David Sanger. Volgens Sanger (2012, p. 190) had de offensieve cyberaanval een tweeledige politieke en militaire doelstelling: ten eerste wilden beide staten de vooruitgang van het Iraanse kernwapenprogramma saboteren, en ten tweede trachtte de VS Israël ervan te overtuigen dat het gebruik van cyberaanvallen een veel efficiëntere en gunstigere manier was om het probleem aan te pakken, in plaats van een luchtaanval te lanceren of een ander oorlogsmiddel te gebruiken die zou kunnen resulteren in een nieuwe oorlog in het Midden-Oosten. De auteurs die de *Tallinn Manual* hadden geschreven konden niet tot een consensus komen over de vraag de Stuxnet-zaak al dan niet een gewapende aanval was, ze waren het er wel over eens dat de aanvallen een illegaal gebruik van geweld waren (Caso, 2014, pp. 252-257). De actor die dit cyberwapen kon ontwikkelen, beschikt ook volgens Langner (2011) ook over de middelen om ‘cyberwapen van massavernietiging’ te ontwikkelen. Stuxnet heeft Iran succesvol getroffen, door haar kerncentrale enorm te beschadigen. Ook is het volgens hem zeker mogelijk dat vijandige natiestaten van dezelfde methode zullen gebruikmaken om doelwitten in het Westen aan te vallen.

Hierdoor moeten de bondgenoten zich voorbereiden op cyberaanvallen van die aard, en een capaciteit uitbouwen om ze te kunnen counteren.

In juni 2017 ontdekte het beveiligingsbedrijf Kaspersky Lab dat er een wereldwijde cyberaanval aan de gang was (Kaspersky, 2017). Door middel van de malware 'NotPetya' werden honderden bedrijven geïnfecteerd in onder andere Frankrijk, Italië, Duitsland, Polen, het Verenigd Koninkrijk, de Verenigde Staten, en voornamelijk in Oekraïne. De malware was gericht op het beschadigen van energiemaatschappijen, bus- en benzinestations, luchthavens en nationale banken (Greenberg, 2018). Deze aanvallen werden toegeschreven aan Rusland (National Cyber Security Centre, 2018). Doordat 80% van de aanvallen op Oekraïne waren gericht, was het duidelijk dat er een voortdurende minachting bestond voor de Oekraïense soevereiniteit. Volgens juridisch onderzoeker aan de CCD COE Tomás Minárik (2017) kunnen de cyberaanvallen als "een schending van de soevereiniteit" worden beschouwd. Indien deze aanval door een staat werd gesponsord en gesteund, zou dit de mogelijkheid van tegenmaatregelen kunnen openen. Hoewel een cyberaanval een gewapende reactie van de NAVO, onder de vorm van Artikel 5, kan uitlokken, lijkt dit waarschijnlijk niet van toepassing bij dit incident, omdat NotPetya net voldoende schade heeft aangericht om dergelijke escalatie uit te lokken. Het recht van gewapend conflict is volgens het internationaal recht enkel van toepassing indien een cyberaanval effectief schade veroorzaakt "met gevolgen die vergelijkbaar zijn met een gewapende aanval tijdens een internationaal conflict". Onder tegenmaatregelen kunnen alle reacties gezien worden die in normale omstandigheden illegaal zouden zijn, maar toch worden toegestaan als reactie op een internationaal onrechtmatige handeling van een andere staat. Uiteindelijk heeft de NAVO geen effectieve tegenmaatregel genomen na deze cyberaanvallen (Pernik, 2018). Dit incident toont nogmaals aan dat het ontbreken van krachtige en voorspelbare reacties op cyberaanvallen door de NAVO, de internationale veiligheid en stabiliteit in het cyberdomein vermindert.

3.5. Samenvatting

Als intergouvernementele militaire alliantie wordt de NAVO steeds meer blootgesteld aan verschillende dreigingen in *cyberspace* die komen vanuit natiestaten. Deze cyberdreigingen werden ingedeeld in verschillende categorieën: malware door middel van DdoS-aanvallen, cyberterrorisme, cyberspionage en cyberoorlogsvoering. Het is cruciaal voor de NAVO om de ontwikkeling van de cybercapaciteit van de vijandige natiestaten in de gaten te houden. China, Rusland, Iran en Noord-Korea breidden hun

cybermacht de afgelopen jaren aanzienlijk uit. Enkelen van hen hebben reeds talrijke cyberoperaties uitgevoerd, waarbij de NAVO direct of indirect in betrokken werd. De voornoemde cyberincidenten lieten dan ook zien dat bij verschillende cyberaanvallen vergelijkbare methoden kunnen worden ingezet, en dat voor het eerst unieke tactieken werden toegepast om een succesvolle cyberoperatie uit te voeren vaak in combinatie met conventionele tactieken (Canbolat & Sezgin, 2016).

Dit hoofdstuk geeft een antwoord op de tweede en derde onderzoeksvraag. Uit deze verschillende cases kan er worden besloten dat de reactie van de NAVO louter defensief bleef, waarbij het bondgenootschap hun cybercapaciteit extra ging beschermen en haar beleid verder aanpaste. Toch bleef een doeltreffende vergelding ten opzichte van de vijandelijke natiestaat uit. Op deze manier kwamen de aanvallende actoren er over het algemeen 'makkelijk' mee weg, en bovendien moedigde het hen aan om hun capaciteit in *cyberspace* te versterken. In tegenstelling tot de offensieve cyberaanval van de VS op Iran waarbij het doel wel werd bereikt (Milevski, 2011).

Het lijkt alsof de NAVO als organisatie een zwakke positie heeft in het conflict door achteraf enkel haar beleid aan te passen en niet offensief terug te slaan. De Russische aanvallen op Estland, Georgië en Oekraïne gaven het land een strategisch voordeel door de landen ook in het cyberdomein aan te vallen. Hoewel in deze cases een van de NAVO-lidstaten of kandidaat-lidstaten, werd getroffen, sloeg de NAVO nooit terug als organisatie onder de vorm van collectieve zelfverdediging. Hierdoor kan gesteld worden dat een louter defensieve houding een strategisch nadeel lijkt te geven aan de NAVO, en bovendien schrikt het de tegenstanders niet voldoende af om terug toe te slaan. Bijgevolg gaat het volgende hoofdstuk dieper in op de huidige cyberstrategie van de NAVO, en wordt er nagegaan waarom het bondgenootschap terughoudend is ten opzichte van een (collectieve) offensieve cybercapaciteit.

4. De cyberstrategie van de NAVO: ‘een veerkrachtige cyberdefensie’

Zowel de NAVO als organisatie, als haar bondgenoten nemen voortdurend maatregelen om de defensie te versterken en haar veerkracht te vergroten. Ze ontwikkelen hun capaciteiten door onder andere partnerschappen aan te gaan met andere landen, internationale organisaties, het bedrijfsleven en de academische wereld. Er is reeds veel vooruitgang geboekt, maar de uitdagingen waar het bondgenootschap mee te maken heeft vergen constante inspanningen (Brent, 2019). Onze samenleving is gebaat bij een op normen gebaseerde voorspelbare en veilige *cyberspace*, omdat de impact van een cyberaanval op een bondgenoot zeer schadelijk kan zijn. Gezien het centrale belang van *cyberspace* voor de moderne manier van oorlogsvoering, lijkt het absoluut noodzakelijk dat het bondgenootschap op dit gebied even slagvaardig is als in de lucht, op zee, te land en in de ruimte. Het blijft echter van belang dat de NAVO nagaat hoe het meer kan doen, aangezien de cyberdreigingen alleen maar ernstiger worden. Daarom zal dit hoofdstuk dieper ingaan op de huidige NAVO-strategie in *cyberspace*, en waarom deze tot nu toe voornamelijk defensief is.

4.1. Defensieve cybercapaciteit van de NAVO

De NAVO heeft een louter defensief mandaat in *cyberspace*, wat inhoudt dat het bondgenootschap vooral inzet op verdedigen. Cyberverdediging is het vermogen om de levering en het beheer van diensten in een operationeel communicatie- en informatiesysteem te beveiligen tegen mogelijke, dreigende en reële kwaadaardige acties die zich bevinden in *cyberspace* (SHAPE Public Affairs Office, 2020).

Defensieve cyberoperaties zijn verdedigende acties om de vrijheid van handelen in *cyberspace* te garanderen aan de bondgenoten. Om een doeltreffende cyberdefensie te behouden is vertrouwen tussen de bondgenoten een essentiële factor, want hoewel technologie een cruciaal onderdeel is van het domein, wordt dit nog steeds beheerd door mensen. De NAVO probeert het vertrouwen te behouden en te versterken door middel van collectieve operaties en trainingsoefeningen in *cyberspace*. Ook is het in bezit van een professioneel netwerk van experten.

4.1.1. NATO CCD COE

In 2004 kwam Estland, toen nog maar pas een nieuwe NAVO-bondgenoot, met het idee om een centrum voor cyberdefensie op te richten (CCDCOE, About Us, 2021). Drie jaar later werd Estland zelf het slachtoffer van een resem politiek gemotiveerde cyberaanvallen. Hierdoor toonde het land aan dat cyberdreigingen reëel zijn en dat ze collectief moeten worden bestreden. In 2008 richtte Estland, in samenwerking met zes andere bondgenoten, het door de NAVO geaccrediteerde Cooperative Cyber Defence Centre of Excellence (CCDCOE) op in Tallinn. Dit centrum beschikt vandaag over civiele en militaire experts uit 25 gelijkgestemde landen en houdt zich bezig met onderzoek, opleiding en oefeningen. Enkele van de voornaamste ontwikkelingen die de CCDCOE heeft gerealiseerd zijn de creatie van het Tallinn Manual, Locked Shields en CyCon. Hieronder wordt kort beschreven wat ze inhouden.

Het Tallinn Manual

Het Tallinn Manual is een academische, niet-bindende studie dat de internationale rechtsnormen in *cyberspace* bevat. In 2013 kwam de eerste editie uit (CCDCOE, 2021). Dit handboek probeert een stand van zaken van het internationaal recht weer te geven, terwijl het een eerder ‘beleids- en politiek neutraal’ project blijft, want de rechtsregels worden vertegenwoordigd door de standpunten van deskundigen. Het vormt een aanvulling op het wetenschappelijk debat over cyberaanvallen, die nu onder de drempel van gewapende aanvallen en gewapend conflict vallen.

In 2017 brachten auteurs en gerenommeerde rechtsgeleerden van over heel de wereld een tweede versie uit onder leiding van professor Michael N. Schmitt: het Tallinn Manual 2.0. Dit is de meest uitgebreide gids voor juristen en beleidsadviseurs over het internationale recht die van toepassing is op cyberoperaties. Ondanks het project met succes is afgesloten blijft het onderzoek doorgaan. Zo bevat het handboek bestaand recht dat werd geherformuleerd, alsook vraagstukken die verder worden bestudeerd, onder meer over soevereiniteit, zorgvuldigheid en attributie. Het verschil ten opzichte van de eerste editie is dat deze versie veel uitgebreider is (Liu, 2017, p. 390). Het bevat namelijk regels voor de toepassing van gespecialiseerde internationale rechtsstelsels op cyberoperaties, met inbegrip van het internationaal recht inzake mensenrechten, het zeerecht en het ruimterecht (p.391).

Echter valt het wel nog te bezien in welke mate het handboek invloed zal hebben op de actoren waarop het in de eerste plaats betrekking heeft: de staten (Eichensehr, 2014, p. 587). Voor regeringen die reeds uitgebreide verrichtingen hebben verricht, biedt het Tallinn Manual wellicht geen nieuwe aanknopingspunten. Toch kan de ervaring van de auteurs en de ruime werkingssfeer van het handboek de regeringen ertoe aanzetten om het handboek te raadplegen als hulpmiddel naast hun nationaal recht. Het lijkt wel een grotere uitdaging of deskundigen uit niet-NAVO-lidstaten het inhoudelijk eens zullen zijn met het handboek en erop zullen vertrouwen. Alle opstellers, technische deskundigen en waarnemers komen uit de Verenigde Staten, West-Europa of Australië (Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare, 2013, pp. x-xii). Ook de *peers* komen uit deze regio's. Bovendien werden enkel nationale militaire handleidingen uit Canada, Duitsland, het Verenigd Koninkrijk en de Verenigde Staten als referentiemateriaal gebruikt, waardoor het handboek een bepaald westers wereldbeeld heeft met betrekking tot de wetten van gewapend conflict (p.8). Hierdoor heerst de vraag of de handleidingen van niet-NAVO-lidstaten overeenkomen met of afwijken van de standpunten die worden weergegeven in het Tallinn Manual (Eichensehr, 2014, p. 588).

Locked Shields

Locked Shields is de grootste en meest complexe internationale cyberverdedigingsoefening ter wereld (NATO CCD COE, 2018). Het doel van deze oefening is om zowel civiele als militaire cyberbeveiligingsexperts te trainen in het verdedigen van netwerken en vitale diensten onder intense cyberaanvallen. De omvang en reikwijdte van het fictieve netwerk is de afgelopen jaren aanzienlijk toegenomen. De focus van de oefening ligt voornamelijk in het verdedigen van gespecialiseerde en militaire IT-systemen naast de reguliere systemen. Dit betekent dat fictieve aanvallers, voorgesteld als het Red Team, meer unieke en geraffineerde aanvallen kunnen plegen, om zo de uitdagingen die er zijn langs juridische, media- en forensische zijde aan te pakken. Tijdens deze oefeningen wordt er gebruik gemaakt van de meest moderne en gesofisticeerde technologieën, om de efficiëntie van de cyberverdediging op een zo accuraat mogelijke manier te testen. Ook niet-lidstaten van de NAVO kunnen deelnemen aan deze oefening. In april 2021 scoorde het cyberbeveiligingsteam van Zweden het hoogst op de oefening om haar netwerk te beveiligen (Kangur, 2021). Het lijkt merkwaardig dat een niet-lidstaat van de NAVO het best voorbereid is om zich te verdedigen in het cyberdomein, wat betekent dat de bondgenoten nog steeds veel werk voor de boeg hebben.

CyCon

'CyCon' is de jaarlijkse internationale conferentie over cyberconflicten (CCDCOE, 2021). Deze wordt al sinds 2008 gehouden en trekt deskundigen uit het cyberdomein van over heel de wereld aan. Tijdens deze conferentie geven experts hun visie op nieuwe uitdagingen, en wat ze verwachten dat de toekomst in *cyberspace* zal beïnvloeden. Wat ook uniek is, is de 360° visie op het cyberdomein. Dit houdt in dat deskundigen met verschillende achtergronden aanwezig zijn, onder andere uit de rechten, technologie en politiek. Deze worden samengebracht om de nieuwste trends en uitdagingen te bespreken, en welke invloed deze zullen hebben op overheden en wetten die ermee samenhangen. Deze conferentie biedt een unieke kans voor deze experts en academici om samen te komen en relevantie kwesties te bespreken.

4.1.2. De rol van Artikel 5

Tijdens de *Wales Summit* (2014) besloten de geallieerden om cyberdefensie toe te voegen aan de kernonderdelen van de collectieve defensie. Hierbij verklaarden ze dat een cyberaanval kan leiden tot het inroepen van de collectieve defensieclausule (Artikel 5) van het Noord-Atlantisch Verdrag (Brent, 2019). Dit artikel houdt in dat indien er een gewapende aanval plaatsvindt tegen een of meerdere geallieerde partijen in Europa of Noord-Amerika, wordt het als een aanval tegen hen allen beschouwd. Bijgevolg mogen andere bondgenoten de aangevallen lidstaat gaan bijstaan, in de uitoefening van individuele of collectieve zelfverdediging erkend in Artikel 51 van het VN-Handvest (NATO, 2011). Concreet betekent dit dat de NAVO elke vorm van agressie tegen bondgenoten zal afschrikken en verdedigen, of deze nu in de fysieke of in de virtuele wereld plaatsvindt.

Gebruik

Na de tragische gebeurtenissen op 11 september 2001 in New York, kwam de Noord-Atlantische Raad, het hoogste besluitvormingsorgaan van de NAVO, tot de consensus dat deze terroristische aanslagen onder het Artikel 5 van het Verdrag van Washington vielen (Gorka, 2006). Dit was een mijlpaal voor de alliantie, want het was de eerste keer dat Artikel 5 van kracht ging. De Verenigde Staten konden, in overeenstemming met hun rechten en plichten uit het VN-Handvest, zelfstandig acties ondernemen, maar werden hierbij gesteund door de NAVO-lidstaten. Op verzoek van de VS werd er tussen oktober 2001 en mei 2002 een anti-terreuroperatie, *Eagle Assist*, uitgevoerd waarbij zeven NAVO-radarvliegtuigen de VS bijstonden met patrouilleren boven hun luchtruim.

In het cyberdomein

Sinds de terreuraanslagen van 9/11 is het Artikel 5 niet meer in werking getreden (NATO, 2021). Dit betekent dus dat een collectieve reactie op een cyberaanval nog niet heeft plaatsgevonden. Na analyse van het Tallinn Manual 2.0 lijkt het niet duidelijk op welke manier het Artikel 5 zou toegepast worden in *cyberspace* (Schmitt, 2017, pp. 1-563). Deze bevinding geeft een antwoord op de vierde vraag uit dit onderzoek.

.

Sommige auteurs vinden de rol van Artikel 5 achterhaald. Volgens beleidsanalist Stephen Jackson (2016) brengt de gedateerdheid van het artikel verschillende uitdagingen met zich mee. Elk internationaal verdrag is een product van zijn historische en technologische context, en dat geldt ook voor het Noord-Atlantisch Verdrag uit 1949. Net na de Tweede Wereldoorlog en bij de oprichting van de Sovjet-Unie probeerden de NAVO-bondgenoten gezamenlijk de Sovjet-agressie tegen het Westen te bestrijden. Na het uiteenvallen van de Sovjet-Unie en de *Global War on Terror* hield de NAVO zich bezig met het bestrijden van niet-statelijke actoren op NAVO-grondgebied, terwijl de operaties ook werden uitgebreid naar regio's zoals het Midden-Oosten (NATO, 2021). Tot op heden blijft de NAVO steunen op het Artikel 5 als middel om alle vormen van gewapende aanvallen te vergelden. Toch mag hier niet worden onderschat dat cyberaanvallen een nieuw en uniek obstakel vormen voor het bondgenootschap (Jackson, 2016).

4.2. Offensieve cybercapaciteit van de NAVO

4.2.1. Soeverein offensief mechanisme

Hoewel er in deze masterproef reeds verschillende keren werd aangehaald dat de NAVO voornamelijk steunt op een defensief mandaat tijdens cyberconflicten, bleek uit een gastcollege met cyberexpert Timmie Bonneu dat het bondgenootschap onlangs een offensief mechanisme uitgedacht (Bonneu, 2021). Dit mechanisme is zeer recent en tijdens verder opzoekingswerk is er gebleken dat er tot nu toe amper iets over geschreven is.

Gebruik

Het nieuwe offensieve mechanisme is gebaseerd op de soevereiniteit van de bondgenoten, en houdt in dat een lidstaat steun kan vragen aan een bondgenoot met een geavanceerdere cybercapaciteit bij het uitvoeren van een offensieve cyberaanval. Net zoals te land, in de lucht of ter zee kunnen NAVO-lidstaten in *cyberspace* collectief optreden, via het bondgenootschap, of individueel als soevereine staten. Toch worden de staten niet belet

om samen te werken wanneer ze onafhankelijk van het bondgenootschap optreden. De NAVO kan op deze manier een beroep doen op een offensieve cybercapaciteit, al zal het wel altijd op initiatief van de lidstaten zijn (Freedberg, 2018). Volgens Freedberg (2018) moet het dus als volgt worden geïnterpreteerd: een NAVO-commandant kan, handelend in zijn of haar alliantie-hoedanigheid, geen enkele lidstaat *bevelen* een offensieve cyberoperatie uit te voeren. Echter beschikt de commandant wel over de mogelijkheid om een offensieve cyberoperatie *voor te stellen*, waarbij een of meerdere lidstaten deze *vrijwillig* kan uitvoeren. Hierbij gaat ook Artikel 3 van het Noord-Atlantisch Handvest van kracht dat stelt dat de partijen, ieder voor zich en gezamenlijk, hun individueel en collectief vermogen om een gewapende aanval te weerstaan kunnen handhaven en ontwikkelen door voortdurend en op doelmatige wijze zichzelf te versterken en elkander hulp te verlenen (NAVO, 2011).

Uitdagingen

Hoe dit concreet in zijn werk zal gaan is nog niet duidelijk, en het zal waarschijnlijk zeer complex zijn. Binnen de NAVO zelf heersen er nog veel twijfels over de effectiviteit van dit mechanisme. Tijdens de *CyCon*-bijeenkomst van november 2019 in de Verenigde Staten, uitte senior-adviseur nationale veiligheidswetgeving voor de *Army Cyber Command* David Bailey zijn zorgen over het mechanisme (Pomerleau, 2019). Vooral het feit dat de offensieve cyberaanvallen niet onder het commando en controle van een feitelijke NAVO-commandant vallen, maar onder die van het land dat zijn bijdrage levert is een twistpunt. Volgens Bailey zal het zeer moeilijk worden om op deze manier een hetzelfde niveau van coördinatie te bereiken dat momenteel van kracht is bij militaire operaties. Tijdens dezelfde bijeenkomst wees ook Massimiliano Signoretti van het CCD COE naar de extra complicaties en wrijvingen die dit mechanisme met zich kan meebrengen. Hij vreest dat er problemen zullen ontstaan tussen de bondgenoten omtrent het vertrouwen in een soevereine commandant, die zelf niet over de cybercapaciteiten beschikt, maar deze wel moet goedkeuren en inzetten. Bovendien zouden er ook problemen kunnen ontstaan met het handhaven van de vertrouwelijkheid van de natie die hun vermogen aan die commandant levert (Pomerleau, 2019).

4.2.2. Waarom een offensieve cybercapaciteit zo'n moeilijke kwestie is

In het General Report van de Parlementaire Vergadering van de NAVO (2019) stelt Artikel 37 uitdrukkelijk dat offensieve cybereffecten niet onder bevel en controle van de NAVO staan, maar onder controle van de bijdragende bondgenoot. Dit is vergelijkbaar met de wijze waarop nationale speciale troepen worden ingezet bij NAVO-operaties.

Volgens de permanente vertegenwoordiger van België bij de NAVO, Philippe Van Gyseghem, zijn de redenen hiervoor zeer simpel (2021). Eerst en vooral is het beschikken over een offensieve cybercapaciteit zeer duur. Er moet geïnvesteerd worden in expertise en doeltreffende technieken en technologieën. De NAVO heeft slechts een beperkt budget, waardoor het momenteel niet mogelijk is om onder de naam van de organisatie te investeren in een offensieve cybercapaciteit (Slayton, 2016, p. 107). Ook is de NAVO een orgaan dat beslissingen neemt in consensus. Dit betekent dat alle dertig bondgenoten het ermee eens moeten zijn. Ieder land heeft een stem en alle landen moeten akkoord gaan, er is dus geen sprake van een meerderheidsquotum (Van Gyseghem, 2021). Dit geldt ook bij het bepalen of het bondgenootschap een militaire operatie zal voeren.

Ten tweede zijn alle bondgenoten van de NAVO verbonden aan zowel het internationaal recht, als hun eigen nationaal recht. Deze laatste kan bepaalde soevereine regels bevatten die stellen dat de betrokkenheid bij een offensieve cyberaanval als strafbaar wordt beschouwd. De bondgenoten zijn inherent verbonden aan de overtuiging dat zowel het internationaal als nationaal recht moet worden gerespecteerd. Ook het humanitair recht belet de NAVO-bondgenoten om offensief te werk te gaan, omdat het bijna onmogelijk is om geen schade toe te brengen aan de burgers, wat dus in strijd is met het humanitair recht. De NAVO kan niet in het wilde weg gaan aanvallen, dit is niet mogelijk in een wereld zonder oorlog. Hierdoor is het zeer moeilijk om vandaag de dag een offensieve aanval te doen op Rusland. Mocht de NAVO een offensieve cyberaanval plegen waardoor de kritieke infrastructuur van de aangevallen staat wordt beschadigd, dan zullen hier ongetwijfeld burgerslachtoffers onder lijden. Van Gyseghem stelt wel dat indien er sprake is van een internationaal gewapend conflict, het discours omtrent een offensieve cyberaanval anders zou zijn.

Ten derde is het momenteel een enorme uitdaging om te achterhalen welke actor de cyberaanval heeft gepleegd (Limnéll & Salonius-Pasternak, 2016). Om collectief te kunnen reageren moet de attributie met 100% zekerheid gebeuren. Het gebeurt vaak dat vijandige regeringen cyberoperaties gaan uitbesteden aan niet-statelijke actoren, waardoor de attributie aan een natiestaat zeer moeilijk wordt.

Tot slot beaamde Van Gyseghem ook dat het consensusmodel en het gebrek aan een offensieve cybercapaciteit in het nadeel van de NAVO speelt. Toch nuanceert hij dat er op die manier belet wordt dat de NAVO zich in een avontuur stort waarbij een enkele

bondgenoot omwille van zijn eigenbelang een collectieve cyberaanval wil lanceren, en het bondgenootschap zich zo in een onverantwoordelijke militaire operatie stort.

4.3. Besluit

Het lijkt dat het cyberdomein de afgelopen twee decennia enorm aan aandacht heeft gewonnen binnen de NAVO. Met de mechanismes van het CCD COE hebben er zich zowel op het vlak van beleid als strategie verschillende veranderingen voorgedaan. Doordat deze strategie grotendeels bestaat uit defensieve mechanismes is het wel niet duidelijk op welke manier de NAVO als collectieve organisatie zou optreden in een internationaal gewapend conflict dat zich afspeelt in het cyberdomein.

Tijdens het uitwerken van dit onderzoek stel ik mij zelf ook vragen bij de effectiviteit van het soevereine mechanisme zoals hierboven beschreven. Met dertig bondgenoten en slechts een half dozijn lidstaten die beschikken over een offensieve cybercapaciteit lijkt het zeer moeilijk om dit mechanisme op een doeltreffende manier te laten werken. Wat indien een lidstaat getroffen wordt door een cyberaanval van een vijandige natiestaat met enorme schade tot gevolg, en deze wil terugslaan met een offensieve cyberoperatie, maar vindt geen bondgenoot die haar hierin wil steunen? En wat moet er verstaan worden onder de collectiviteit van Artikel 5 in *cyberspace*, want met louter soevereine zelfverdediging in plaats van collectieve zelfverdediging lijkt dit mechanisme toch volledig achterhaald? Nog maar te zwijgen over het feit dat de NAVO als organisatie geen inspraak heeft in dit soevereine mechanisme? Mocht er zich een cyberoorlog voordoen lijkt het mij onmogelijk voor de NAVO om deze succesvol te kunnen bestrijden door louter te steunen op het beveiligen en beschermen van haar kritieke infrastructuur.

Vanwege deze bevindingen wordt in het volgende hoofdstuk geargumenteerd waarom de NAVO wel over een collectieve offensieve cybercapaciteit moet beschikken, ondanks de obstakels waar het bondgenootschap momenteel mee te maken heeft.

5. Tijd voor een collectieve offensieve cybercapaciteit

5.1. Evaluatie en motivering

Uit de vorige hoofdstukken is gebleken dat de NAVO in het verleden heeft geworsteld met het uitbouwen van een alomvattende strategie die de bondgenoten voldoende voorbereidt om cyberaanvallen af te schrikken, zich ertegen te verdedigen en deze te vergelden. Ondanks de belangrijk stappen die het bondgenootschap reeds heeft gezet, is de NAVO nog lang niet klaar om cyberdreigingen met de 'snelheid van relevantie' te bestrijden (Arts, 2018). De garanties van individuele leden om hun cybercapaciteiten namens het bondgenootschap in te zetten, zoals eerder vermeld, proberen die leemte in de strategie op te vullen.

Na het analyseren van de NAVO haar huidige cyberstrategie lijkt het onmogelijk dat de NAVO als organisatie een cyberoorlog kan bestrijden. Alles hangt af van een handvol lidstaten die beschikken over een offensieve cybercapaciteit. Indien zij tijdens een internationaal gewapend cyberconflict hun offensieve cybercapaciteiten niet willen inzetten maakt het bondgenootschap geen schijn van kans. Zonder een welomschreven beleidsovereenkomst tussen de bondgenoten, en een onduidelijke soevereine commandostructuur kan de offensieve tegenaanval met dit soevereine mechanisme resulteren in een conventioneel conflict.

In dit hoofdstuk worden enkele argumenten opgesomd waarom het noodzakelijk is dat de NAVO een collectieve offensieve cybercapaciteit in haar cyberstrategie opneemt. Omwille van deze redenen zou de NAVO haar strategisch nadeel wegwerken bij een internationaal gewapend conflict in het cyberdomein.

5.1.1. Geloofwaardige vergelding

Een doeltreffende cyberstrategie betekent dat vijandige natiestaten worden afgeschrikt om een aanval te plegen tegen een NAVO-bondgenoot. Offensieve cybercapaciteiten houden in dat de actor doelbewust netwerken of systemen van de tegenstander binnendringt met de bedoeling deze te verstoren, te beschadigen of te vernietigen. Indien een militaire macht zoals de NAVO geen offensieve cybercapaciteiten in haar arsenaal heeft, kan het dan wel op een geloofwaardige wijze beweren dat het over geavanceerde capaciteiten beschikt (Lewis J. A., 2015)? Het inzetten van deze offensieve cybercapaciteit is grotendeels bedoeld om dwingende politieke druk uit te oefenen op

doelwitten in plaats van hen te vernietigen of te ontwrichten. Bovendien dragen offensieve cybercapaciteiten bij tot het gebruik van geweld voor defensieve doeleinden, aangezien het ook een preventieve aanvalsmogelijkheid kan aanbieden (Smeets & Lin, 2018, p. 58).

5.1.2. Instandhouding van het bondgenootschap

Er zijn enkele belangrijke kwesties die de NAVO moet aanpakken om een realistische en doeltreffende militaire cybermacht te worden. Eerst en vooral moet het bondgenootschap erkennen dat het verdedigen van haar netwerk zoals ze nu doet, niet gelijk is aan een collectieve verdediging in *cyberspace*. Uit dit literatuuronderzoek is gebleken dat het bondgenootschap niet als 'alliantie' optreedt in het cyberdomein. Met behulp van het defensieve mandaat houdt de NAVO zich grotendeels bezig met het beveiligen van haar netwerk. Hoewel er tijdens de Warschau Summit in 2016 werd beslist dat het cyberdomein onder de collectieve zelfverdediging van de NAVO valt, is er gebleken dat deze reactie toch niet zo gezamenlijk is als vooropgesteld. Er is geen collectief model dat stelt hoe de NAVO zal terugslaan in een cyberoorlog. Indien de vijand over een geavanceerde en gesofisticeerde cybercapaciteit beschikt en slachtoffers of kritieke schade aanricht aan de NAVO-bondgenoot, dan zal het louter beschermen van het netwerk onvoldoende zijn.

De NAVO heeft geen gezamenlijke vergeldingscapaciteit, en als de keuze om offensief op te treden bij de soevereine bondgenoten zelf ligt dan is het gegeven van 'collectieve verdediging', en dus ook de rol van Artikel 5, verwaarloosbaar. Aan de hand van deze interpretatie stelt deze masterproef dat het vermogen van de NAVO als organisatie in *cyberspace*, onvoldoende is om een cyberaanval, laat staan een cyberoorlog, te bestrijden. De NAVO als organisatie voert tot op heden geen strijd in het vijfde domein, het louter verdedigt en beschermt. Dit is een persoonlijke mening gebaseerd op het literatuuronderzoek, en zou waarschijnlijk door academici en deskundigen uit het cyberdomein in perspectief moeten geplaatst worden.

5.1.3. Een noodzaak bij cyberoorlogsvoering

Cybertechnieken kunnen worden ingezet tijdens een conventioneel conflict. Ze zullen volgens James A. Lewis zelfs essentieel zijn voor de soort gevechtsoperaties die NAVO-strijdkrachten in de toekomst kunnen uitvoeren (2015). Geen moderne luchtmacht zou de strijd aangaan zonder hulp van elektronische oorlogsvoering (EW). Indien cybertechnieken en EW zouden samensmelten tot één activiteit, zullen luchtoperaties

ondersteuning nodig hebben uit het cyberdomein. Dit geldt ook voor operaties van de speciale strijdkrachten, wat betekent dat het cyberdomein de slagvelden van de toekomst zullen vormgeven.

De potentiële vijanden van de NAVO gaan zelf nieuwe geavanceerde manieren creëren waarin ze gebruikmaken van offensieve cyberoperaties, wat eerder als hybride oorlogsvoering werd benoemd (Aaronson, 2011). Landen die traditioneel al door de NAVO in het oog werden gehouden zoals China en Rusland, maar ook nieuwe cybermachten zoals Iran en Noord-Korea, of proxies en niet-statelijke actoren zijn constant bezig met het verbeteren van hun (offensieve) technieken in *cyberspace.* Deze vijandige natiestaten proberen steeds meer de militaire macht van de Verenigde Staten en de rest van de alliantie te omzeilen door onconventionele technieken te gebruiken om hun doelen te bereiken. Het is deze nieuwe vorm van oorlogsvoering die een uitdaging zal vormen voor de NAVO om doeltreffende tegenmaatregelen te nemen (NATO, 2020). Om deze redenen zal de NAVO moeten nadenken aan de uitbouw van haar cybercapaciteit, die meer is dan louter defensief en beschermend.

Ook lijkt het niet waarschijnlijk dat zelfs met het soevereine collectieve mechanisme, de NAVO erin zal slagen om militaire operaties in het cyberdomein te doen slagen. De grens wordt hierbij vervaagd of de NAVO als alliantie achter de aanval zit, of de aanval vanuit een of meerdere bondgenoten op zelfstandige basis komt. Indien de aangevallen staat vergelding wil voor de daad en terugslaat op een specifieke NAVO-bondgenoot kan dit conflict escaleren en enorm veel schade toebrengen aan de lidstaat, terwijl de NAVO als organisatie schrik opwekt bij vijandige natiestaten waardoor ze minder snel de neiging zouden hebben om aan te vallen.

5.2. Offensieve cyberinstrumenten

Over welke soorten wapens een offensieve cybercapaciteit van de NAVO precies moet beschikken zal niet verder worden uitgewerkt in deze masterproef. Zoals eerder vermeld blijft dit onderzoek volledig politiekwetenschappelijk, en wordt er niet ingegaan op het technische aspect. Ook is het niet de bedoeling om gedetailleerde beleidsopties voor te stellen, noch een gedetailleerde beschrijving te geven van wat de NAVO-troepen precies moeten doen tijdens een specifieke offensieve cyberoperatie. In de plaats worden er twee offensieve instrumenten voorgesteld die de NAVO in haar beleid kan hanteren, namelijk *compellence, swaggering en retaliation*. Dit zijn drie strategische doelstellingen van

militaire macht die ruim 40 jaar geleden werden ontwikkeld door Robert J. Art (1980), en hieronder worden er gekeken op welke manier ze zouden kunnen fungeren binnen de NAVO.

5.2.1. *Compellence*

Compellence of dwang is een term afkomstig van Thomas Schelling en wordt vaak gebruikt in de internationale betrekkingen (Shelling, 1966). Het dwingend gebruik van militair geweld heeft twee doelstellingen. Enerzijds kan het een activiteit van een tegenstander stopzetten, anderzijds kan het een tegenstander dwingen om iets te doen wat hij nog niet gedaan heeft.

Omwille van verschillende redenen zou het gebruik van dwang een strategisch voordeel kunnen opleveren voor de NAVO voor of tijdens een cyberincident. Eerst en vooral hoeft de impact van dwang op de vijandige natiestaat niet noodzakelijk publiek gemaakt worden (Smeets & Lin, 2018, p. 58). Ook kan de gedwongen natiestaat ontkennen dat het getroffen wordt door een offensieve cyberaanval. Stel dat een virus de computersystemen in een luchthaven voor enkele dagen verstoort, met enorme financiële verliezen tot gevolg, dan kunnen deze worden toegeschreven aan een algemene storing in het systeem. In werkelijkheid werd de vijandige natiestaat getroffen door een offensieve cyberaanval van de NAVO, maar dit hoeft niet publiek gemaakt worden. Vanwege deze redenen lijdt de gedwongen actor achteraf geen reputatieschade in het internationale toneel, en kan een eventuele escalatie van het conflict vermeden worden (Smeets, 2017).

Bovendien kunnen offensieve cybercapaciteiten bijdragen tot de naleving van internationale normen. De tegenstander weet dat indien hij zich terugtrekt, de oude situatie hersteld kan worden, want vijandige natiestaten hebben niet altijd het vermogen om het incident te laten escaleren tot een werkelijke oorlog. Een simpele karakterisering van een cybersituatie kan zijn dat de dwingende staat dreigt met: “Elke dag je mij blijft aanvallen, zal ik gegevens over ‘X’ van je kritieke computersysteem beschadigen.” Op deze manier wijzigt de stimulering voor de aanvallende staat en is het mogelijk dat het de dwingende eis naleeft uit vrees voor mogelijke beschadiging van zijn data.

Een ander voorbeeld van *compellence* is dat de NAVO een vijandelijke cyberstaat gaat dwingen zijn gedrag of beleid te veranderen, door haar overheid vooraf op de hoogte te brengen van de offensieve cyberaanval met een bericht (Smeets & Lin, 2018, p. 65). In dit bericht stelt de NAVO haar eisen en brengt ze de vijandige staat op de hoogte van een

kwetsbaarheid in haar systeem die ze nog niet had ontdekt (*een zero-day exploit*). Deze kwetsbaarheid is een *'burning vulnerability'* en kan het probleem aanpakken. De vijandige staat kan op deze manier worden afgeschrokken door de cybercapaciteiten van de NAVO. Op die manier kan de staat een oordeel maken over de schade die het land zal lijden indien het zich blijft verzetten tegen de eisen van de NAVO.

5.2.2. *Swaggering*

In principe behoort *swaggering* tot een restcategorie van een offensieve cyberstrategie (Smeets & Lin, 2018, p. 66). De doelstellingen voor *swaggering* zijn diffuus en niet gericht op het weerhouden van een andere staat om aan te vallen of het afweren van aanvallen.

Swaggering heeft betrekking tot een vreedzaam gebruik van geweld en kan op verschillende manieren worden uitgedrukt (Art, 1980). De NAVO kan *swaggering* gebruiken om haar militaire macht tijdens militaire oefeningen of internationale demonstraties te tonen, en zo de internationale omgeving afschrikken. Ook het aankopen van prestigieuze wapens behoort tot deze soort. In bezit zijn van een arsenaal van cyberwapens kan de vastberadenheid en bekwaamheid van een staat aantonen.

Toch blijkt deze offensieve cybercapaciteit het minst efficiënt (Smeets, 2017). Cybercapaciteiten zijn grotendeels immaterieel waardoor het moeilijk is om er publiekelijk mee te paraderen. Ook het tijdelijke karakter van *cyberspace* is een probleem voor *swaggering*. Indien de NAVO haar cybercapaciteiten onthult, wordt de kans vergroot dat vijandelijke natiestaten de kans grijpen om meer te weten te komen over de kwetsbaarheid van de cyberwapens.

5.2.3. *Retaliation*

Met een uitgebouwde offensieve cybercapaciteit zou de NAVO er ook voor kunnen kiezen om in plaats van te dreigen, effectief terug te slaan met een grootschalige cyberaanval indien een van haar lidstaten het slachtoffer wordt van een grootschalige cyberaanval. Bij voorkeur zou een tegenaanval, bijvoorbeeld het lamleggen van bepaalde kritieke infrastructuur zoals het netwerk van haar overheid, een duidelijk signaal zijn dat cyberaanvallen door tegenaanvallen in *cyberspace* worden beantwoord (Van der Meer, 2018). Op deze manier moet er voorkomen worden dat er een escalatiecyclus op gang gebracht wordt die uitmondt in een resem van cyberaanvallen.

Het is wel de bedoeling dat de tegenaanval proportioneel is in verhouding met de cyberaanval door de vijandige natiestaat. Het mag niet teveel schade, laat staat daadwerkelijke burgerslachtoffers, veroorzaken om een doeltreffend effect te verkrijgen. De tegenaanval moet enkel de bedoeling hebben om de vijandige staat af te schrikken, en te tonen dat het zelf ook getroffen kan worden. Een offensieve tegenreactie brengt wel de nodige risico's met zich mee. Zo is er altijd een kans dat de vijandige staat repressailles neemt tegen de tegenaanval, vooral als het de ontkenning van de oorspronkelijke cyberaanval wil versterken. De NAVO moet dus zeker rekening houden met het feit dat escalatie in principe meer problemen kan veroorzaken dan oplossen.

Ook is er het risico dat de internationale gemeenschap deze tegenaanval zal veroordelen indien er een gebrek is aan bewijs voor de toerekening van de oorspronkelijk cyberaanval. Dit kan bijvoorbeeld gebeuren indien de NAVO niet het concrete bewijs kan leveren ter bescherming van de gebruikte inlichtingenmethoden. Tot slot mag er ook niet over het hoofd worden gezien dat ook *collateral damage* tot internationale veroordeling kan leiden. Tot op heden zijn er nog geen voorbeelden van publieke vergelding van een cyberaanval door een tegencyberaanval, maar ze zullen waarschijnlijk al hebben plaatsgevonden zonder dat ze openbaar werden gemaakt (Green & al., 2015).

6. Conclusie en vervolgonderzoek

Deze masterproef ving aan met de hypothese of de huidige cyberstrategie van de NAVO over het vermogen beschikt om een cyberoorlog te voeren indien een of meerdere lidstaten betrokken raken in een internationaal gewapend cyberconflict. Door te verdiepen in een uitgebreide hoeveelheid aan boeken, tijdschriften, papers, blogs, video's, en het volgen van verschillende lezingen met betrekking tot dit onderwerp, kunnen volgende conclusies worden getrokken.

Dreigingen in *cyberspace* mogen in de toekomst niet onderschat worden door de NAVO-lidstaten. Hun aandeel zal tijdens militaire operaties sterk toenemen (Stimpson, 2015). Hoewel het momenteel nog een surrealistische gedachte lijkt dat een oorlog zich volledig op het web zal afspelen, moet er toch rekening gehouden worden met deze mogelijkheid. Gesofisticeerde cyberaanvallen kunnen namelijk onvoorziene schade toebrengen aan de kritieke infrastructuur van een staat. Hierdoor is het van belang dat de NAVO haar netwerk en bondgenoten kan beschermen indien er zich een cyberoorlog zou voordoen, alsook dat ze een tegenaanval kan voeren tegen de vijandige natiesta(a)t(en).

Momenteel beschikt de NAVO louter over een defensieve cybercapaciteit ter beveiliging van haar kritieke infrastructuur. Na het analyseren van verschillende cyberincidenten is gebleken dat de NAVO vooral passief reageerde op de aanvallen door haar cyberbeleid aan te scherpen en extra defensieve instrumenten te hanteren in haar strategie, zoals het Tallinn Manual, de cyberverdedigingsoefening *Locked Shields*, en het houden van een jaarlijkse conferentie omtrent cyberconflicten. Bij de besproken cyberincidenten bleef een doeltreffende vergelding of represailles ten opzichte van de aanvallende staat uit. Hierdoor kan geconcludeerd worden dat de vijandige staat niet op voldoende wijze werd afgeschrikt om haar cyberwapenarsenaal af te bouwen. Integendeel, het niet gestraft worden door het westerse bondgenootschap kan juist een drijfveer zijn voor vijandige actoren om hun cybercapaciteiten verder uit te breiden (Rid, 2021).

Ook werd het probleem omtrent de rol van Artikel 5 in het cyberdomein aan het licht gebracht. Cyberdefensie behoort sinds 2014 tot de kernonderdelen van de collectieve defensie van het bondgenootschap, maar tot op heden is het niet duidelijk hoe het mechanisme concreet in zijn werk zou gaan indien een NAVO-bondgenoot betrokken raakt in een cyberoorlog. In principe zou het bondgenootschap kunnen instemmen om deze lidstaat bij te staan en in de tegenaanval te gaan zoals het deed tijdens de *Global*

War on Terror van de Verenigde Staten, al lijkt het niet duidelijk hoe de NAVO dat van plan is zonder een offensieve cybercapaciteit ter beschikking te hebben. Wel wordt er binnen de NAVO sinds kort het debat gevoerd omtrent een soevereine offensieve cybercapaciteit waarbij lidstaten die zelf beschikken over een offensieve cybercapaciteit ervoor kunnen kiezen om de getroffen bondgenoot bij te staan tijdens een cyberconflict (Bonneu, 2021). Omwille van de complexiteit en heersende onduidelijkheid werd besloten dat dit soevereine mechanisme allesbehalve doeltreffend lijkt mocht er zich plots een cyberoorlog voordoen. Vanwege deze bevindingen antwoordt deze masterproef negatief op de hypothese of de NAVO momenteel beschikt over het vermogen om een succesvolle cyberoorlog te voeren.

Hierdoor werden enkele argumenten gemotiveerd die pleiten voor de uitbouw van een collectieve offensieve cybercapaciteit door het bondgenootschap, ondanks de huidige obstakels. Allereerst zou het de geloofwaardigheid van het bondgenootschap ten goede komen, en op deze manier vijandige natiestaten afschrikken om cyberaanvallen te plegen tegen NAVO-bondgenoten. Ook zou het de bondgenoten dichter bij elkaar brengen, omdat deze weten dat ze op het bondgenootschap kunnen rekenen indien ze betrokken raken in een cyberincident. Bovendien zou het Artikel 5 een effectieve rol krijgen in het cyberdomein, omdat dit collectieve verdedigingsmiddel de basis vormt voor het bondgenootschap. Tot slot kan er tijdens een effectief cyberconflict niet om een tegenaanval heen indien het bondgenootschap wil terugslaan. De NAVO moet ook over vergeldende instrumenten beschikken in plaats van louter beschermende, want als het bondgenootschap zelf getroffen wordt door een cyberaanval met een onvoorziene impact, en het beschikt niet over middelen om terug te slaan, heeft het bondgenootschap de strijd op voorhand al verloren.

Toch moet er nog eens duidelijk benadrukt worden dat dit literatuuronderzoek voornamelijk gebaseerd is op een analytische en beschrijvende benadering. Het is een louter politiekwetenschappelijk onderzoek, die bij het concluderen van haar bevindingen geen gebruik heeft gemaakt van de juridische en technische consequenties, die het uitbouwen van een collectieve offensieve cybercapaciteit met zich meebrengen. Daarnaast botste het onderzoek op verschillende hiaten in de literatuur omtrent dit onderwerp. Het is merkwaardig dat er tot nu toe amper geschreven werd omtrent de rol van Artikel 5 in het cyberdomein. Het is niet duidelijk of dit bewust werd gedaan, omdat het bondgenootschap haar strategie liever niet publiek maakt omtrent dit artikel, of omdat experten en politici niet overeenkomen over de inhoud van het artikel in het cyberdomein.

Ook bestaan er nog veel hiaten omtrent het soevereine offensieve mechanisme van de NAVO in *cyberspace*. Het is dankzij de gastcolleges van meneer Bonneu en meneer Van Gyseghem dat dit mechanisme in dit onderzoek verwerkt kon worden. Daarnaast is onderzoek in het cyberdomein sowieso een moeilijke opgave, omdat cyberoperaties in de meeste gevallen geheim en geclassificeerd zijn. Er is nog veel mogelijkheid binnen dit onderwerp om adequaat vervolgonderzoek te doen en eventueel andere domeinen te betrekken.

Deze masterproef hoopt met behulp van dit onderzoek het publiek debat te openen tussen experten, academici en politici omtrent het uitbouwen van een collectieve offensieve cybercapaciteit binnen de NAVO.

V. Bibliografie

Aaronson, M. (2011). NATO Countering the Hybrid Threat. *Prism*, 111-124.

Albahar, M. (2017). Cyber Attacks and Terrorism: A Twenty-First Century Conundrum. *Science And Engineering Ethics*, 995.

Alexander, D. C. (2014). *Cyber Threats Against the North Atlantic Treaty Organization (NATO) and Selected Responses.* Istanbul: Istanbul Gelişim Üniversitesi Sosyal Bilimler Dergisi.

Andress, J., & Steve, W. (2013). Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners. In J. Andress, & W. Steve, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners.* Waltham: Elsevier.

Arimatsu, L. (2012). A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations. *Cyber Conflict (CYCON) 4th International Conference* (pp. 1-19). Tallinn: NATO CCDCOE.

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar Is Coming! *Comparative Strategy*, 141-165.

Art, R. J. (1980). To What Ends Military Power. *International Security*, 3-35.

Arts, S. (2018). *Offense as the New Defense: New Life for NATO's Cyber Policy.* Washington D.C.: The German Marshall Fund of the United States.

Baezner, M., & Robin, P. (2018, Oktober 1). *Cyber and Information Warfare in the Ukrainian Conflict*. Retrieved April 2021, from Center for Security Studies: https://www.researchgate.net/publication/322364443_Cyber_and_Information_warfare_in_the_Ukrainian_conflict

Bicakci, S. (2014). NATO's Emerging Threat Perception: Cyber Security in the 21st Century. *Uluslararasi Iliskiler*, 101-130.

Bonneu, T. (2021, Maart 24). Gastcollege ADIV in het vak 'Nationale Veiligheids in een Hedendaags Perspectief'. (E. Platteau, Interviewer)

Brennan, D. (2018, Augustus 8). *U.S. Expects Iranian Cyber Attacks in Retaliation to New Sanctions, Experts Say*. Retrieved April 2021, from Newsweek: https://www.newsweek.com/us-expects-iranian-cyber-attacks-retaliation-new-sanctions-experts-say-1062977

Brenner, S. W. (2007). At light speed: attribution and response to cybercrime/terrorism/warfare. *Journal of Criminal Law and Criminology*, 379-475.

Brent, L. (2019, Februari 12). *NATO's role in cyberspace*. Retrieved April 2021, from NATO Review: https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html

Bugajski, J. (2019, April 30). *China's Eurasian Ambitions*. Retrieved April 2021, from CEPA: https://cepa.org/chinas-eurasian-ambitions/

Canbolat, M., & Sezgin, E. (2016). *Is NATO Ready for a Cyber War?* Monterey, California: Naval Postgraduate School.

Caso, J. S. (2014). The rules of engagement for cyber-warfare and the Tallinn Manual: A case study. *The 4th Annual IEEE International Conference on Cyber Technology in Automation, Control and Intelligent* (pp. 252-257). Hong Kong: IEEE.

Caton, J. L. (2016, Juni 1). *NATO Cyberspace Capability: a strategic and operational evolution*. Retrieved Maart 2021, from Strategic Studies Institute, US Army War College: http://www.jstor.com/stable/resrep11524

CCDCOE. (2021). *About Us*. Retrieved April 2021, from CCDCOE: https://ccdcoe.org/about-us/

CCDCOE. (2021). *CyCon*. Retrieved April 2021, from CCDCOE: https://ccdcoe.org/cycon/

CCDCOE. (2021). *The Tallinn Manual Process*. Retrieved April 2021, from CCDCOE: https://ccdcoe.org/research/tallinn-manual/

Clausewitz, C. (1976). On War. In C. Clausewitz, *On War* (p. 32). New York: Oxford University Press.

Croft, A., & Apps, P. (2014, Maart 16). *NATO websites hit in cyber attack linked to Crimea tension*. Retrieved Maart 2021, from Reuters: https://www.reuters.com/article/us-ukraine-nato-idUSBREA2E0T320140316

Danning, D. E. (1999, December 10). *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*. Retrieved April 2021, from Nautilus Institute for Security and Sustainability: https://nautilus.org/global-problem-solving/activism-hacktivism-and-cyberterrorism-the-internet-as-a-tool-for-influencing-foreign-policy-2/

Davis, S. (2019). *NATO in the Cyber Age: Strenghtening Security & Defence, Stabilising Deterrence.* United States: NATO Parliamentary Assembly.

Dennekamp, G.-J. (2020, Maart 7). *Hoe de strijd tussen Rusland en Oekraïne leidde tot het neerhalen van MH17*. Retrieved April 2021, from NOS:

https://nos.nl/nieuwsuur/collectie/13835/artikel/2326188-hoe-de-strijd-tussen-rusland-en-oekraine-leidde-tot-het-neerhalen-van-mh17

Dominik, H. (2019). Cyber Espionage and Cyber Defense. In C. Reuter, *Information Technology for Peace and Security: IT Applications and Infrastructures in Conflicts, Crises, War, and Peace* (pp. 84-86). Wiesbaden: Springer Vieweg.

Dowse, A., & Dov Bachmann, S.-D. (2019, Juni 18). *Explainer: what is 'hybrid warfare' and what is meant by the 'grey zone'?* Retrieved Maart 2021 , from The Conversation: https://theconversation.com/explainer-what-is-hybrid-warfare-and-what-is-meant-by-the-grey-zone-118841

Eichensehr, K. E. (2014). Reviewed Work(s): Tallinn Manual on the International Law Applicable to Cyber Warfare. *The American Journal of International Law*, 585-589.

Fitton, O. (2016). Cyber Operations and Gray Zones: Challenges for NATO. *Connections: The Quarterly Journal*, 109-119.

Ford, C. A. (2010, Oktober). *The Trouble with Cyber Arms Control*. Retrieved April 2021, from The New Atlantis: https://www.thenewatlantis.com/publications/the-trouble-with-cyber-arms-control

Freedberg, S. J. (2018, November 16). *NATO To 'Integrate' Offensive Cyber By Members*. Retrieved April 2021, from Breaking Defense: https://breakingdefense.com/2018/11/nato-will-integrate-offensive-cyber-by-member-states/

Fruhlinger, J. (2020, September 4). *What is phishing? How this cyber attack works and how to prevent it.* Retrieved April 2021, from CSO Online: https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html

Galeotti, M. (2018, Maart 5). *I'm Sorry for Creating the 'Gerasimov Doctrine'*. Retrieved Maart 2021, from Foreign Policy: https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/

Gasparr, R. (2008, Maart 9). *The Israeli 'E-tack' on Syria – Part I*. Retrieved Maart 2021, from Air Force Technology: https://www.airforce-technology.com/features/feature1625/

Gazula, M. B. (2017). *Cyber Warfare Conflict Analysis and Case Studies.* Cambridge: Massachusetts Institute of Technology.

Geers, K., Kindlund, D., Moran, N., & Rachwald, R. (2013). *World War C: understanding nation-state motives behind today's advanced cyber attacks*. Retrieved Maart 2021, from Fire Eye: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/fireeye-wwc-report.pdf

Goel, S. (2011). Cyberwarfare: connecting the dots in cyber intelligence. *Communications of the ACM*, 132-140.

Gorka, S. L. (2006). *Het inroepen van Artikel 5 in zijn historische context*. Retrieved Maart 2021, from NAVO Kroniek: https://www.nato.int/docu/review/2006/issue2/dutch/art1.html

Green, J. A., & al., e. (2015). Cyber Warfare: a multisciplinary analysis. In J. A. Green, *Cyber Warfare: a multidisciplinary analysis* (pp. 61-73). New York: Routledge.

Greenberg, A. (2018, Augustus 27). *NotPetya: How a Russian malware created the world's worst cyberattack ever*. Retrieved April 2021, from Business Standard: https://www.business-standard.com/article/technology/notpetya-how-a-russian-malware-created-the-world-s-worst-cyberattack-ever-118082700261_1.html

Gulf International Forum. (2020, Juli 28). *A New Age of Cyber Conflict for Iran? Increasing Capabilities and Incentives*. Retrieved April 2021, from Gulf International Forum: https://gulfif.org/a-new-age-of-cyber-conflict-for-iran-increasing-capabilities-and-incentives/

Hasanov, A. H., Iskandarov, K. I., & Sadiyev, S. S. (2019). The evolution of NATO's cyber security policy and future prospects. *Journal of Defense Resources Management*, 94-106.

Hasanov, A. H., Iskandarov, K. I., & Sadiyev, S. S. (2019). The Evolution of NATO's Cyber Security Policy and Future Prospects. *Journal of Defense Resources Management*, 94-106.

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security*, 51.

Hoffman, W. (2019). Is Cyber Strategy Possible? *The Washington Quarterly*, 131-152.

Holcomb, F. (2020, December 4). *Countering Russian and Chinese Cyber-Aggression*. Retrieved April 2021, from CEPA: https://cepa.org/countering-russia-and-chinese-cyber-aggression/

Hollis, D. (2011, Januari 6). *Cyberwar Case Study: Georgia 2008*. Retrieved April 2021, from Small Wars Journal: https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf

Hughes, R. (2009). *Towards a Global Regime for Cyber Warfare.* London, Chatham House: Cyber Security Project.

Inkster, N. (2016). China's Cyber Power. In N. Inkster, *China's Cyber Power* (pp. 9-11). London: Routledge.

Innvolve. (2017, Mei 14). *Ransomware WannaCry – Alles wat u moet weten*. Retrieved from Innvolve: https://innvolve.nl/ransomware-wannacry/

Intsights. (2020). *Dark Side of China: The Evolution of a Global Cyber Power.* New York: Intsights.

Jackson, S. (2016, Augustus 16). *NATO Article 5 and Cyber Warfare: NATO's Ambiguous and Outdated Procedure for Determining When Cyber Aggression Qualifies as an Armed Attack.* Retrieved April 2021, from Center for Infrastructure Protection and Homeland Security: https://cip.gmu.edu/2016/08/16/nato-article-5-cyber-warfare-natos-ambiguous-outdated-procedure-determining-cyber-aggression-qualifies-armed-attack/

Ji Young, K., Kyoung Gon, Kim, & Jong In, Lim. (2019). The All-Purpose Sword: North Korea's Cyber Operations and Strategies. *2019 11th International Conference on Cyber Conflict: Silent Battle* (pp. 1-20). Tallinn: NATO CCD COE.

Joubert, V. (2012). *Five years after Estonia's cyber attacks: lessons learned for NATO.* Rome: NATO Defense College.

Jun, J. (2018). *Hybrid and Transnational Threats.* Brussel: Friends of Europe.

Juncker, J.-C. (2017, September 13). *President Jean Claude Juncker's State of the Union Address 2017*. Retrieved Maart 2021, from European Commission: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_17_3165

Kangur, C. (2021). *Sweden Scored Highest at the Cyber Defence Exercise Locked Shields 2021*. Retrieved April 2021, from CCD COE: https://ccdcoe.org/news/2021/sweden-scored-highest-at-the-cyber-defence-exercise-locked-shields-2021/

Kaplan, F. (2016). In *Dark Territory: The Secret History of Cyber War* (pp. 28-32). New York: Simon & Schuster.

Kaska, K., Beckvard, H., & Minarik, T. (2019). *Huawei, 5G and China as a Security Threat.* Tallinn: CCDCOE.

Kaspersky. (2017, Juni 27). *New Petya / NotPetya / ExPetr ransomware outbreak*. Retrieved April 2021, from Kaspersky: https://www.kaspersky.com/blog/new-ransomware-epidemics/17314/

Kelsey, J. T. (2008). *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare.* Retrieved Maart 2021, from Michigan Law Review: https://repository.law.umich.edu/mlr/vol106/iss7/6

Korns, S. W., & Kastenberg, J. E. (2008). Georgia's cyber left hook. *Parameters*, 60-67.

Kuehl, D. T. (2009). From Cyberspace to Cyberpower: Defining the Problem. In F. Kramer, S. Starr, & L. Wentz, *Cyberpower and National Security* (pp. 24-42). Nebraska: University of Nebraska Press.

Kukkola, J. (2018). Russian Cyber Power and Structural Asymmetry. *GAME PLAYER Facing the structural transformation of cyberspace* (pp. 19-35). Washington DC: International Conference on Cyber Warfare and Security (ICCWS).

Langner, R. (2011, Maart 29). *Cracking Stuxnet, a 21st-century cyber weapon*. Retrieved April 2021, from YouTube: https://www.youtube.com/watch?v=CS01Hmjv1pQ&ab_channel=TED

Lasiello, E. (2015). Are Cyber Weapons Effective Military Tools? *Military and Strategic Affairs/The Institute for National Security Studies*, 23-40. Retrieved from http://works.bepress.com/emilio_iasiello/4/

Lewis, J. A. (2002, November 1). *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. Retrieved April 2021, from Center For Strategic and International Studies: https://www.csis.org/analysis/assessing-risks-cyber-terrorism-cyber-war-and-other-cyber-threats

Lewis, J. A. (2015). The Role of Offensive Cyber Operations in NATO's Collective Defence. *The Tallinn Papers*, 2.

Lewis, J. A. (2019, Juni 25). *Iran and Cyber Power*. Retrieved April 2021, from Center for Strategic and International Studies: https://www.csis.org/analysis/iran-and-cyber-power

Libicki, M. (2014). Why Cyber War Will Not and Should Not Have Its Grand Strategist . In M. Libicki, *Why Cyber War Will Not and Should Not Have Its Grand Strategist* (pp. 23-40). Maxwell: Air University Press.

Limnéll, J., & Salonius-Pasternak, C. (2016). *Challenge for NATO – Cyber Article 5.* Stockholm: Center for Asymmetric Threat Studies.

Lindsay, J. (2021, Januari 22). The SolarWinds Hack And The Future Of Cyber Espionage. (CNBC, Interviewer)

Liu, I. Y. (2017). The due diligence doctrine under Tallinn Manual 2.0. *Elsevier*, 390-391.

Machiels, M. (2019, November 1). *Active Cyber Defence and NATO - NATOs innovative offensive strategy towards Russia and China*. Retrieved Februari 2021, from Atlantic Forum: https://atlantic-forum.com/content/active-cyber-defence-and-nato-natos-innovative-offensive-strategy-towards-russia-and-china

Medvedev, S. A. (2015). *Offense-defense theory analysis of Russian cyber capability.* Monterey: Naval Postgraduate School.

Mena, J. (2003). Investigative Data Mining for Security and Criminal Detection. In J. Mena, *Investigative Data Mining for Security and Criminal Detection* (p. 270). Burlington: Elsevier Science.

Milevski, L. (2011). Stuxnet and strategy: a special operation in cyberspace? *Joint Forces Quarterly*, 64-69.

Milnetzky, A. (2012). Defending America against Chinese cyber espionage through the use of active defenses. *Cardozo Journal of International & Comparative Law*, 536.

Minárik, T. (2016, Juli). *NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit.* Retrieved 2021 Februari, from NATO CCDCOE: https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/

Minarik, T. (2017, Juli 2). *NotPetya and WannaCry Call for a Joint Response from International Community*. Retrieved April 2021, from CCDCOE: https://ccdcoe.org/news/2017/notpetya-and-wannacry-call-for-a-joint-response-from-international-community/

Monaghan, S. (2019). Countering Hybrid Warfare: So What for the Future Joint Force? *Prism*, 88.

Mudrinich, E. M. (2012). Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem. *Air Force Law Review*, 168-205.

NASCIO. (2007, April 18). *Insider Security Threats: State CIOs Take Action Now!* Retrieved April 2021, from NASCIO: https://www.nascio.org/resource-center/resources/insider-security-threats-state-cios-take-action-now/?__cf_chl_captcha_tk__=8735dc054c09f634ca6194cef52507967ef145b2-

1617905239-0-ASyB4kru_R586JFR81AFS0oYXQwG3W8pO_0t0uB5ihHNFjRX6a76kFkK2uvVPNfixizrlUz7Y-vLs

National Cyber Security Centre. (2018, Februari 14). *Russian military 'almost certainly' responsible for destructive 2017 cyber attack*. Retrieved 2021 April, from National Cyber Security Center: https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack

NATO. (1999, Juli 15). *NATO's role in relation to the conflict in Kosovo*. Retrieved April 2021, from NATO's Role in Kosovo: https://www.nato.int/kosovo/history.htm

NATO. (2002, November 21). *Prague Summit Declaration: issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Prague, Czech Republic*. Retrieved Maart 2021, from North Atlantic Treaty Organization: https://www.nato.int/cps/en/natohq/official_texts_19552.htm

NATO. (2011, Maart 14). *Het Noord-Atlantisch Verdrag*. Retrieved April 2021, from NATO: https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=nl

NATO. (2016, Juli). *NATO's support to Ukraine*. Retrieved April 2021, from NATO: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-nato-ukraine-support-eng.pdf

NATO. (2020, November 25). *NATO 2030: United for a New Era.* Retrieved April 2021, from NATO: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf

NATO. (2021, Februari 8). *Collective defence - Article 5*. Retrieved Februari 2021, from NATO: https://www.nato.int/cps/en/natohq/topics_110496.htm

NATO. (2021, April 12). *Cyber defence*. Retrieved April 2021, from NATO: https://www.nato.int/cps/en/natohq/topics_78170.htm

NATO CCD COE. (2018, Januari 15). *At the Forefront of Cyber Defence: NATO CCDCOE*. Retrieved April 2021, from YouTube: https://www.youtube.com/watch?v=aHvcfX-WcSw&ab_channel=natoccdcoe

NAVO. (2011, Maart 14). *Het Noord-Atlantisch Verdrag*. Retrieved April 2021, from NATO: https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=nl

Net Politics. (2021, Maart 15). *The Iran-Russia Cyber Agreement and U.S. Strategy in the Middle East*. Retrieved April 2021, from Council on Foreign Relations: https://www.cfr.org/blog/iran-russia-cyber-agreement-and-us-strategy-middle-east

Nye, J. S. (2010, Mei). *Cyber Power*. Retrieved Maart 2021, from Belfer Center for Science and International Affairs: https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf

Ong, W. (2018). The rise of hybrid actors in the Asia-Pacific. *The Pacific Review*, 746-767.

Ottis, R. (2018). *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective.* Tallinn: CCDCOE.

Parsons, E., & Bureau, H. (2019, April). *Understanding the Cyber Threat from North Korea*. Retrieved April 2021, from F-Secure: https://www.f-secure.com/en/consulting/our-thinking/understanding-the-cyber-threat-from-north-korea

Parsons, E., & Michael, G. (2019, April). *Understanding the Cyber Threat from Iran*. Retrieved April 2021, from F-Secure: https://www.f-secure.com/en/consulting/our-thinking/understanding-the-cyber-threat-from-iran

Parsons, E., & Michael, G. (2019, April). *Understanding the Cyber Threat from Iran*. Retrieved April 2021, from F-Secure: https://www.f-secure.com/en/consulting/our-thinking/understanding-the-cyber-threat-from-iran

Parsons, E., & Raff, M. (2019, Maart). *Understanding the Cyber Threat From Russia*. Retrieved April 2021, from F-Secure: https://www.f-secure.com/en/consulting/our-thinking/understanding-the-cyber-threat-from-russia

Pernik, P. (2018, Februari 23). *Responding to "the Most Destructive and Costly Cyberattack in History"*. Retrieved April 2021, from International Centre for Defence and Security: https://icds.ee/en/responding-to-the-most-destructive-and-costly-cyberattack-in-history/

Petters, J. (2020, Maart 29). *What is a Brute-Force Attack?* Retrieved April 2021, from Varonis: https://www.varonis.com/blog/brute-force-attack/

Pomerleau, M. (2019, November 20). *Here are the problems offensive cyber poses for NATO*. Retrieved April 2021, from Fifth Domain:

https://www.fifthdomain.com/international/2019/11/20/here-are-the-problems-offensive-cyber-poses-for-nato/

Raine, J. (2019, April 3). *War or peace? Understanding the grey zone*. Retrieved from International Institute for Strategic Studies: https://www.iiss.org/blogs/analysis/2019/04/understanding-the-grey-zone

Rhodes, R. (2012). In R. Rhodes, *The Making of The Atomic Bomb* (p. 586). Londen: Simon & Schuster.

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, 5-32.

Rid, T. (2021, Januari 2021). *CNBC: The SolarWinds Hack And The Future Of Cyber Espionage*. Retrieved Februari 2021, from YouTube: https://www.youtube.com/watch?v=jxTxGlE9X5s&ab_channel=CNBC

Rid, T., & McBurney, P. (2012, February 29). Cyber-Weapons. *The RUSI Journal*, pp. 6-13.

Riley, D. (2021, Februari 15). *Microsoft's Brad Smith labels SolarWinds hack 'largest, most sophisticated attack ever'*. Retrieved Februari 2021, from SiliconANGLE: https://siliconangle.com/2021/02/15/microsofts-brad-smith-labels-solarwinds-hack-largest-sophisticated-attack-ever/

Robinson, M., Janicke, H., Jones, K., & Maglaras, L. (2018). An Introduction To Cyber Peacekeeping. *Journal of Network and Computer Applications*, 70-87.

Robinson, M., Jones, K., & Janicke, H. (2014, Maart). Cyber warfare: Issues and challenges. *Computers & Security*, 70-94.

Robinson, M., Jones, K., & Janicke, H. (2015, Maart). Cyber warfare: Issues and challenges. *Computers & Security*, 70-94.

Rollins, J., & Wilson, C. (2007). *Terrorist Capabilities for Cyberattack: Overview and Policy Issues.* Washington DC: Congressional Research Service.

Rowe, N. (2010). The Ethics of Cyberwarfare. *Journal of Military Ethics*, 384-410.

Rowe, N. C. (2015). The Attribution of Cyber Warfare. In J. A. Green, *Cyber Warfare: a multidisciplinary analysis* (pp. 61-73). New York: Routledge.

Sanger, D. (2012). Confront and Conceal. In D. Sanger, *Confront and Conceal* (p. 190). New York: Random House.

Scarfone, K. (2021, Januari). *How to develop a cybersecurity strategy: Step-by-step guide*. Retrieved Maart 2021, from TechTarget: https://searchsecurity.techtarget.com/tip/How-to-develop-a-cybersecurity-strategy-Step-by-step-guide

Schmitt, M. N. (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. In M. N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge: Cambridge University Press.

Schmitt, M. N. (2017). (Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2017). In M. N. Schmitt, *(Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2017)* (pp. 1-563). Cambridge: Cambridge University Press.

Scott, R. D. (1999). Territorially Intrusive Intelligence Collection and International law. *A.F. L. Rev*, 46.

Senator John McCain. (2017, April 6). *National Geographic presents The Future of Cyberwarfare | Origins: The Journey of Humankind*. Retrieved Februari 2021, from YouTube: https://www.youtube.com/watch?v=L78r7YD-kNw&list=LL&index=7&ab_channel=NationalGeographic

SHAPE Public Affairs Office. (2020, December 2019). *NATO Cyber Defensive Capability As a Spearhead and Force Multiplier*. Retrieved April 2021, from SHAPE: https://shape.nato.int/news-archive/2020/nato-cyber-defensive-capability-as-a-spearhead-and-force-multiplier

Shea, J. (2017). How is NATO Meeting the Challenge of Cyberspace? *PRISM: The Fifth Domain*, 18-30.

Sheldon, J. B. (2011). Deciphering Cyberpower Strategic Purpose in Peace and War. *Strategic Studies Quarterly*, 95-112.

Sheldon, J. B. (2016). The Rise of Cyberpower. In J. Baylis, J. J. Wirtz, & C. S. Gray, *Strategy in the Contemporary World* (pp. 282-298). Oxford: Oxford University Press.

Shelling, T. C. (1966). Arms and influence. In T. C. Shelling, *Arms and influence* (pp. 69-91). Londen: Yale University Press.

Slayton, R. (2016). What Is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment. *International Security*, 107.

Smeets, M. (2017). A matter of time: On the transitory nature of cyberweapons. *Journal of Strategic Studies*, 6-32.

Smeets, M., & Lin, H. S. (2018). Offensive Cyber Capabilities: To What Ends? *2018 10th International Conference on Cyber Conflict* (p. 58). Tallinn: NATO CCD COE Publications.

Soare, S. R., & Burton, J. (2020). Smart Cities, Cyber Warfare and Social Disorder. In A. Ertan, K. Floyd, P. Pernik, & T. Stevens, *Cyber Threats and NATO 2030: Horizon Scanning and Analysis* (pp. 108-110). Tallinn: NATO CCDCOE Publications.

Soendergaard Larsen, M. (2021, Maart 15). *While North Korean Missiles Sit in Storage, Their Hackers Go Rampant*. Retrieved April 2021, from Foreign Policy: https://foreignpolicy.com/2021/03/15/north-korea-missiles-cyberattack-hacker-armies-crime/

Stimpson, M. (2015). Cyberwarfare Will Not Replace Conventional Warfare. *Canadian Forces College*, 22-23.

Stoker, D., & Whiteside, C. (2020, Januari 24). *Blurred Lines: Gray-Zone Conflict and Hybrid War—Two Failures of American Strategic Thinking.* Retrieved Maart 2021, from U.S. Naval War College: https://digital-commons.usnwc.edu/nwc-review/vol73/iss1/4/?utm_source=digital-commons.usnwc.edu%2Fnwc-review%2Fvol73%2Fiss1%2F4&utm_medium=PDF&utm_campaign=PDFCoverPages

The Cormorant's Nest. (2020, Juli 8). *Sir, nobody told you? Grey zones and hybrid warfare do not exist!* Retrieved Maart 2021, from Medium: https://medium.com/the-cormorants-nest/sir-nobody-told-you-grey-zones-and-hybrid-warfare-do-not-exist-366b55100c1d

Tikk, E., Kaska, Kadri, & Vihul, L. (2010). Some Recommendations for The Way Forward. In E. Tikk, Kaska, Kadri, & L. Vihul, *International Cyber Incidents: Legal Considerations* (p. 101). Tallinn, Estland: CCD COE Publications. Retrieved Maart 2021, from CCDCOE: https://ccdcoe.org/library/publications/international-cyber-incidents-legal-considerations/

Tsekov, I. (2017). *The Changing Balance of Power in the Age of Emerging Cyber Threats.* Sofia: Institute for Security and International Studies.

Välisluureamet. (2021). *International Security and Estonia 2021.* Tallinn: Estonian Foreign Intelligence Service.

Van der Meer, S. (2018). *State-level Responses to Massive Cyber-attacks: a policy toolbox.* Den Haag: Clingendael.

Van Gyseghem, P. (2021, April 21). Gastcollege NAVO in het vak 'Nationale Veiligheid in een Hedendaags Perspectief'. (E. Platteau, Interviewer)

Verton, D. (1999, April 4). *Serbs launch cyberattack on NATO*. Retrieved April 2021, from FCW: https://fcw.com/articles/1999/04/04/serbs-launch-cyberattack-on-nato.aspx

von Clausewitz, C. (1982). On War. In C. Von Clausewitz, *On War* (p. 101). Harmondsworth: Penguin Books.

Weisman, S. (2020, Juli 23). *What is a distributed denial of service attack (DDoS) and what can you do about them?* Retrieved April 2021, from Norton Life Lock: https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html

Whittaker, Z. (2019, April 19). *Mueller report sheds new light on how the Russians hacked the DNC and the Clinton campaign*. Retrieved April 2021, from TechCrunch: https://techcrunch.com/2019/04/18/mueller-clinton-arizona-hack/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAGz1kdzQ452KXUn8Y5vlVQQWRF-44wNbVtvqP_bOfn4eYrZxU6_sGVSknu4uXD9xFlzI8CilAbuIfQ3qV_xs--oodB6KmLOvmDXr5k0LTknO6R

Wortham, A. (2012). Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That Ma Hostile Intent That May Violate UN Char y Violate UN Charter Provisions Pr visions Prohibiting ohibiting the Threat or Use of Force? *Federal Communications Law Journal*, 643-655.

Zerzri, M. (2017). *The Threat of Cyber Terrorism and Recommendations for Countermeasures.* Bayern: Center for Applied Policy Research.