Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2018–2019

33 694 Internationale Veiligheidsstrategie

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 47 **BRIEF VAN DE MINISTER VAN BUITENLANDSE ZAKEN**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 5 juli 2019

In het Plenair Debat Spionage door Rusland van 20 december 2018 (Handelingen II 2018/19, nr. 39, item 33) is een uiteenzetting van de toepassing van de desbetreffende onderdelen van bestaand internationaal recht op het digitale domein toegezegd. Daarnaast is in de motie van de leden Verhoeven en Bruins Slot (Kamerstuk 33 694, nr. 35) verzocht om een weergave van initiatieven ten behoeve van het bestendigen van de internationale rechtsorde in het digitale domein. Doel van deze brief is uw Kamer mede namens de Ministers van Defensie, Justitie en Veiligheid en Binnenlandse Zaken en Koninkrijksrelaties te informeren over bovenstaande punten. In de bijlage wordt op de belangrijkste volkenrechtelijke aspecten ingegaan.

Bestendigen van de internationale rechtsorde in het digitale domein

Het kabinet wil een leidende rol spelen bij het toepassen en versterken van een internationaal normatief kader voor de regulering van cyberoperaties tussen staten. Het recent door de EU bekrachtigd NL initiatief van een cybersanctieregime is een voorbeeld van de NL inzet. Het bestaande internationaal recht is daarbij het uitgangspunt. Nederland heeft immers belang bij een goed functionerende internationale rechtsorde die zorgt voor een mate van voorspelbaarheid, stabiliteit en conflictpreventie.

Zoals uiteengezet in het Cyber Security Beeld Nederland 2019[1] en de jaarverslagen van de Inlichtingen- en Veiligheidsdiensten,[2] neemt de digitale dreiging vanuit statelijke actoren toe en is er onvoldoende overeenstemming over de internationale normen en waarden die gelden in het digitale domein. Recente gebeurtenissen zoals de verstoring van de

[1] Cyber Security Beeld Nederland 2019 (Kamerstuk 26 643, nr. 614).

[2] Openbaar jaarverslag 2019 van de Algemene Inlichtingen en Veiligheidsdienst (AIVD) (Kamerstuk 30 977, nr. 154) en Openbaar jaarverslag 2018 van de Militaire Inlichtingen en Veiligheidsdienst (MIVD) (Kamerstuk 29 924, nr. 184).

kst-33694-47
ISSN 0921 - 7371
's-Gravenhage 2019

cyberoperatie van de Russische militaire inlichtingendienst GRU, gericht tegen de Organisatie voor het Verbod op Chemische Wapens (OPCW) op 13 april 2018, zijn een manifestatie van een veel bredere geopolitieke trend. De status quo wordt in toenemende mate bedreigd door statelijke actoren die kwetsbaarheden die digitalisering met zich mee brengt uitbuiten.

Teneinde specifiek op het cyberdomein toegesneden handvatten te bieden, zet het kabinet daarnaast in op internationale afspraken over vrijwillige, niet-bindende-gedragsnormen voor staten en de ontwikkeling van een stelsel van vertrouwenwekkende maatregelen. Daarbij zijn de consensusrapporten van de UN Group of Governmental Experts 2010, 2013 en 2015[3] leidend. Nederland draagt zo bij aan de ontwikkeling van een internationale veiligheidsarchitectuur voor het cyberdomein.

Het kabinet acht betrokkenheid vanuit het bedrijfsleven, kennisinstellingen, de technische gemeenschap en maatschappelijk middenveld in deze van groot belang. Complementair aan de bestaande interstatelijke processen heeft het kabinet daarom onder meer de Global Commission on the Stability of Cyberspace (GCSC) ondersteund. De GCSC werkt aan een raamwerk voor stabiliteit in cyberspace. Het eindrapport zal in november gereed zijn.

Nederland tracht in aanloop naar onderhandelingen in een tweetal VN fora[4] door middel van consultaties over de toepassing van het internationaal recht in het digitale domein het interstatelijke draagvlak voor het open, vrije en veilige internet te vergroten. Zo heeft het kabinet onlangs internationale consultaties georganiseerd met een groot aantal staten over de toepassing van het internationaal recht in het digitale domein.

Daarnaast zet het kabinet in op capaciteitsopbouw om het internationale draagvlak voor een open, vrij en veilig internet, waar het bestaande internationaal recht wordt gerespecteerd en geïmplementeerd, te verbreden. Middels het in 2015 door Nederland gelanceerde Global Forum on Cyber Expertise (GFCE) zijn strategische capaciteitsopbouw activiteiten ontplooid. Toepassing van internationaal recht op het digitale domein is een van de thema's waar het GFCE zich op richt. Aan de hand van de Tallinn Manual 2.0[5] worden wereldwijde capaciteitsopbouwprojecten uitgevoerd.

In beide VN-processen zal desalniettemin actief weerstand moeten worden geboden tegen pogingen de toepassing van internationaal recht in cyberspace en eerder in VN overeengekomen principes en gedragsnormen ter discussie te stellen. Er is immers sprake van een steeds scherpere tegenstelling tussen enerzijds de multistakeholder-georiënteerde landen waaronder Nederland, die pleiten voor bescherming van de openheid, vrijheid en integriteit van het internet, en anderzijds staatsgeoriënteerde landen die pleiten voor controle en inperking van datgene dat over het internet wordt verspreid. Daarbij is de inzet van het netwerk van Nederlandse diplomatieke vertegenwoordigingen, dat op het terrein van cyberexpertise wordt versterkt, van groot belang.

---

[3] UNGGE Consensus rapport 2009/2010, A/65/201, 2012/2013, A/68/98*, 2014/2015, A/70/174.

[4] NL zal in 2019 opnieuw zitting te nemen in de *United Nations Group of Governmental Experts (UNGGE)* van start. Daarnaast zal Nederland ook deelnemen aan de Open Ended Working Group over internationale cybersecurity vraagstukken die is opgericht n.a.v. een Russische resolutie in de Algemene Vergadering van de Verenigde Naties.

[5] NL ondersteunt een meer inclusieve en gedetailleerde discussie over de toepassing van internationaal recht op cyberoperaties a.d.h.v. «Tallinn Manual 2.0 on the international law applicable to cyberoperations».

Diplomatieke en politieke respons op cyberincidenten

Terwijl de internationale discussie over de toepassing en de reikwijdte van het internationaal recht in het digitale domein voortduurt, blijven sommige landen schadelijke activiteiten ontplooien. Diplomatiek optreden tegen ongewenste statelijke cyberoperaties, bij voorkeur internationaal gecoördineerd of in coalitieverband met gelijkgezinde landen, kan een effectief middel zijn ter bestendiging van de internationale rechtsorde en (inter)nationale veiligheidsbelangen. Het kabinet zet dientengevolge ook in op een versterking van de capaciteit om diplomatiek en politiek te kunnen reageren op ondermijnende cyberoperaties. De internationale respons na de verstoorde cyberoperatie bij de OPCW is hier een treffend voorbeeld van. Om gecoördineerd op te kunnen treden, is inzet van het postennet essentieel. Bij het bepalen van responsopties staat een zorgvuldige en integrale afweging van de Nederlandse (veiligheids)belangen centraal.

Om de internationale samenwerking ook in Europees-verband verder te structuren, is op Nederlands initiatief een EU cyberdiplomatie *toolbox*[6] tot stand gekomen. Hiermee kunnen verschillende instrumenten van het Gemeenschappelijk Buitenlands en Veiligheidsbeleid worden aangewend om degenen die ondermijnende cyberactiviteiten ontplooien ter verantwoording te roepen. Als onderdeel daarvan is op Nederlands initiatief 17 mei jl. in een EU cyber sanctieregime[7] ingesteld waarmee het mogelijk wordt om tegoeden te bevriezen en inreisverboden op te leggen.

Ook voor het NAVO-bondgenootschap is het van belang zich te kunnen verweren tegen het volledige spectrum aan vijandige cyberoperaties. Dit betreft niet alleen cyberoperaties die beschouwd kunnen worden als een gewapende aanval, maar ook operaties die onderdeel zijn van een hybride campagne onder de drempel van een gewapend conflict. Hiervoor blijft het kabinet zich in bondgenootschappelijk verband sterk maken.

Tot slot

In de bijlage worden de belangrijkste internationaalrechtelijke regels die gelden in het digitale domein uiteengezet. Tevens wordt toegelicht hoe het kabinet de toepassing van deze regels interpreteert. Waar relevant, is aangegeven welke kwesties nog onderwerp van internationale discussie zijn en welke nadere uitwerking vereisen. Hierbij wordt ingegaan op verplichtingen van staten in het cyberdomein, attributie van cyberoperaties en responsopties bij ongewenst cyberoptreden door een andere staat.

Het kabinet zet ondertussen onverwijld in op de reeds in de Geïntegreerde Buitenland en Veiligheidsstrategie en de Nederlandse Cyber Security Agenda ingezette aanpak. Daarbij geniet i) de versterking van het diplomatiek responskader in EU- en NAVO verband en met gelijkgezinde landen en ii) verbreding van draagvlak voor een open, vrij en veilig internet, waar het bestaande internationaal recht van toepassing is en nageleefd wordt, prioriteit. Medio 2020 zal het kabinet uw Kamer inlichten over de voortgang.

De Minister van Buitenlandse Zaken,
S.A. Blok

---

[6] Doc. 9916/17 Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities.

[7] Doc. 7299/19 Council Decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

Bijlage: **Internationaal recht in het digitale domein (cyberspace)**

Algemeen

In deze bijlage wordt ingegaan op een aantal belangrijke internationaalrechtelijke verplichtingen van staten in het cyberdomein. Een schending van (een van) deze verplichtingen die toerekenbaar is aan een staat levert een internationaalrechtelijke onrechtmatige daad van die staat op, tenzij sprake is van een internationaalrechtelijk erkende rechtvaardigingsgrond.[8] Zoals het kabinet meerdere malen heeft aangegeven en consequent uitdraagt, is het internationaal recht van toepassing op het cyberdomein. Dit wordt ook internationaal erkend.[9] Dit neemt niet weg dat nog veel vragen bestaan over hoe het internationaal recht precies moet worden toegepast in het cyberdomein, wat komt door de bijzondere kenmerken van de digitale wereld ten opzichte van de fysieke wereld. Digitale gegevens verplaatsen zich doorgaans snel en zijn daardoor vaak lastig te lokaliseren, kunnen in enkele seconden naar een ander land worden verplaatst, of zijn verspreid over meerdere landen opgeslagen. Daarnaast hebben ongewenste activiteiten in het cyberdomein lang niet altijd (meteen) fysiek effect, terwijl de effecten ervan wel ernstig kunnen zijn. Het is nog niet geheel duidelijk hoe deze en andere bijzondere kenmerken moeten worden meegenomen bij de toepassing van het internationaal recht. Het kabinet stimuleert de internationale discussie over het verduidelijken van de toepassing van het internationaal recht op het cyberdomein. Duidelijkheid en overeenstemming daarover is van belang voor de internationale rechtsorde.
Het formuleren van de antwoorden op de openstaande vragen is een continu proces, waarbij het kabinet nauw afstemt met gelijkgezinde partners en initiatieven neemt om de discussie verder te helpen, zoals de internationale consultaties over internationaal recht in het cyberdomein die Nederland eind mei in Den Haag heeft georganiseerd.
In deze bijlage wordt nader ingegaan op een aantal belangrijke internationaalrechtelijke regels die gelden in het cyberdomein. Ook wordt toegelicht hoe het kabinet tegen de toepassing van deze regels aankijkt. Waar relevant zal worden aangegeven welke kwesties nog onderwerp van internationale discussie zijn en nadere uitwerking vereisen. De volgende indeling wordt aangehouden: verplichtingen van staten in het cyberdomein, attributie van cyberoperaties en responsopties bij ongewenst cyberoptreden door een andere staat. Het kabinet gaat uit van de primaire bronnen van internationaal recht zoals vermeld in artikel 38 van het Statuut van het Internationaal Gerechtshof, dat onder meer verwijst naar verdragen, gewoonterecht en algemene rechtsbeginselen als bronnen van internationaal recht.

Verplichtingen van staten

Respect voor soevereiniteit

Het beginsel van soevereiniteit, oftewel het beginsel dat staten gelijkwaardig en onafhankelijk zijn en binnen de grenzen van hun grondgebied het hoogste gezag hebben, is een van de fundamentele beginselen van

---

[8] De aansprakelijkheid van staten en rechtvaardigingsgronden onder het internationaal recht zijn onder meer verwoord in de *Articles on the Responsibility of States for Internationally Wrongful Acts*, die is opgenomen in resolutie A/56/589 van de Algemene Vergadering van de Verenigde Naties. Het commentaar op de ARSIWA is opgenomen in het *Yearbook of the International Law Commission*, 2001, vol. II, Part Two.

[9] Zie onder meer de rapporten van de *Group of Governmental Experts on Developments in the field of information and telecommunications in the context of international securit*y uit 2013 en 2015, te vinden via https://www.un.org/disarmament/ict-security/; de EU cybersecurity strategy, 2017, en in NATO summit declarations in 2014, 2016 en 2018.

het internationaal recht.[10] Internationaalrechtelijke regels als het geweldsverbod, het non-interventiebeginsel en het recht op zelfverdediging vloeien hieruit voort. Deze regels zullen hierna in meer detail worden besproken.
Volgens sommige landen en juristen vormt het soevereiniteitsbeginsel niet een zelfstandige regel van internationaal recht die los staat van de daarvan afgeleide regels. Nederland deelt deze visie niet en is van mening dat respect voor de soevereiniteit van andere landen een op zichzelf staande verplichting is, waarvan de schending een zelfstandige internationaalrechtelijk onrechtmatige daad kan opleveren. Dit standpunt vindt onder meer steun in de rechtspraak van het Internationaal Gerechtshof, dat in de *Nicaragua* zaak oordeelde dat de Verenigde Staten in strijd had gehandeld met de gewoonterechtelijke verplichting niet de soevereiniteit van een andere staat te schenden.[11] Hieronder wordt nader in gegaan op de betekenis van deze verplichting.
Soevereiniteit houdt in de eerste plaats in dat staten exclusieve rechtsmacht hebben over zaken, personen en activiteiten binnen hun grondgebied, met inachtneming van hun internationaalrechtelijke verplichtingen, zoals verplichtingen met betrekking tot privileges en immuniteiten of verplichtingen voortvloeiend uit mensenrechtenverdragen. Dit is het interne aspect van soevereiniteit. In de tweede plaats houdt soevereiniteit in dat staten vrij en onafhankelijk zijn in het bepalen van hun buitenlands beleid, bij het aangaan van internationale verplichtingen en betrekkingen en het ontplooien van activiteiten buiten hun grenzen, zolang zij zich houden aan de regels van het internationaal recht. Dit is het externe aspect van soevereiniteit.
Beide aspecten gelden onverkort in het cyberdomein. Staten hebben exclusief gezag over de materiële, personele (menselijke) en immateriële (logische of software) aspecten van het cyberdomein binnen hun territorium. Zij mogen binnen hun grondgebied bijvoorbeeld regels stellen over technische specificaties van mobiele netwerken, de weerbaarheid tegen cyberaanvallen en *cybersecurity* reguleren, maatregelen treffen om cybercriminaliteit te bestrijden of handhavend optreden om de vertrouwelijkheid van persoonsgegevens te beschermen. Daarnaast mogen zij zelfstandig buitenlands cyberbeleid voeren en verdragsverplichtingen op het gebied van cyber aangaan. De beslissing van Nederland om zich aan te sluiten bij het Cybercrimeverdrag van de Raad van Europa is bijvoorbeeld een uitoefening van de Nederlandse soevereiniteit.
Op staten rust de verplichting de soevereiniteit van andere staten te respecteren en zich te onthouden van activiteiten die inbreuk maken op de soevereiniteit van andere landen. Ook mogen landen geen cyberoperaties uitvoeren die de soevereiniteit van een ander land schenden. Hierbij moet worden aangetekend dat de precieze grenzen van wat wel mag en wat niet mag nog niet volledig zijn uitgekristalliseerd. Dit heeft het maken met de sterk territoriale en fysieke connotatie van het traditionele begrip soevereiniteit. Het beginsel is van oudsher gericht op het beschermen van het gezag over *zaken en personen binnen de eigen landsgrenzen*. In het cyberdomein is de notie van territorialiteit of fysieke tastbaarheid vaak minder duidelijk. Zo is het mogelijk dat één cyberoperatie opgebouwd is uit verschillende componenten of acties die vanuit verschillende landen worden geïnitieerd of die via verschillende landen lopen, op een manier die niet altijd kan worden getraceerd. Daarnaast zijn er verschillende mogelijkheden om de geografische herkomst van activiteiten in het

---

[10] *Island of Palmas arbitral award of 1928:* «Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State.»
[11] *Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America)*, International Court of Justice (ICJ), 27 juni 1986, par. 15 en 292.

cyberdomein te maskeren. Bovendien worden gegevens tegenwoordig vaak via een *cloud* systeem op verschillende, wisselende en niet altijd kenbare locaties opgeslagen. Lang niet altijd kan dus worden vastgesteld of een cyberoperatie een grensoverschrijdend element heeft en daarmee de soevereiniteit van een land schendt. En zelfs als de herkomst of route van een cyberoperatie kan worden vastgesteld, geldt dat dit soort operaties niet altijd tot (direct) fysiek tastbare gevolgen leidt.
Ook in het kader van de rechtshandhaving, een onderdeel van de interne soevereiniteit van staten, is de wijze waarop het beginsel van soevereiniteit moet worden toegepast, internationaal nog niet volledig uitgekristalliseerd. Inmiddels lijkt een gedeelde opsporingspraktijk op Europees en internationaal niveau zich te ontwikkelen. Voor de opsporing relevante gegevens staan steeds vaker over de grens, bijvoorbeeld in de cloud, in hoofdzakelijk private datacenters opgeslagen. Ook voor het plegen van strafbare feiten op, of met gebruik van, het internet is de locatie van gegevens, waaronder kwaadaardige software of code, en van fysieke infrastructuur vaak nauwelijks relevant. Bovendien zijn locatie en identiteit op het internet goed te verbergen en is steeds meer communicatie versleuteld. Bij de digitale opsporing van strafbare feiten, waaronder cybercriminaliteit, kan – zelfs als sprake is van een puur nationale zaak, met een verdachte en slachtoffer binnen één staat – daarom al snel sprake zijn van buiten Nederland opgeslagen gegevens, vooral bij het vorderen van gegevens van online dienstenaanbieders of hostingproviders, de netwerkzoeking en het (heimelijk) op afstand binnendringen van een geautomatiseerd werk. Bij grensoverschrijdende toepassing van opsporingsbevoegdheden is traditioneel sprake van een schending van de soevereiniteit van het andere land, tenzij dat land expliciet toestemming heeft verleend (al dan niet via een verdrag). Over de vragen wanneer er sprake is van grensoverschrijdende toepassing van onderzoeksbevoegdheden en wanneer dit zonder verdragsrechtelijke basis toelaatbaar is, wordt verschillend gedacht. In het digitale domein wordt ook in de praktijk niet door elk land hetzelfde omgegaan met soevereiniteit bij de opsporing van strafbare feiten. Nederland levert een actieve bijdrage aan internationale gesprekken over mogelijkheden om de opsporing effectiever te maken, waarbij in het bijzonder aandacht is voor de juiste waarborgen.
In algemene zin onderschrijft het kabinet stelregel 4 die is voorgesteld door de samenstellers van de Tallinn manual 2.0 voor het vaststellen van de grenzen van soevereiniteit in het cyberdomein.[12] Volgens deze regel is sprake van een schending van de soevereiniteit als 1) inbreuk wordt gemaakt op de territoriale integriteit van de andere staat; of dat 2) sprake is van verstoring van of miskennen van de uitoefening van inherente overheidsfuncties van de andere staat. De precieze invulling van deze factoren is nog onderwerp van discussie.

Verbod op interventie

Met de ontwikkeling van geavanceerde digitale technologieën hebben staten meer mogelijkheden gekregen om invloed uit te oefenen op ontwikkelingen buiten hun eigen grenzen en zich te mengen in de aangelegenheden van andere staten. Het pogen verkiezingsuitslagen te beïnvloeden via sociale media is hier een voorbeeld van. Het internationaal recht stelt grenzen aan dit soort activiteiten met het verbod op interventie, dat voortvloeit uit het soevereiniteitsbeginsel. Net als dit beginsel is het verbod alleen van toepassing tussen staten.
Interventie wordt gedefinieerd als inmenging in de interne of externe aangelegenheden van een andere staat met het oog op het uitoefenen van

[12] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, een handboek voor de toepassing van het internationaal recht in het cyberdomein, opgesteld door een aantal internationaalrechtelijke experts, in samenspraak met overheidsjuristen.

dwang op die staat. Het gaat hierbij om aangelegenheden waarover staten volgens het soevereiniteitsbeginsel zelf de zeggenschap hebben. Nationale verkiezingen zijn bijvoorbeeld een interne aangelegenheid. Voorbeelden van externe aangelegenheden zijn de erkenning van staten en lidmaatschap van een internationale organisatie.
Wanneer sprake is van het uitoefenen van dwang, en dus ongeoorloofde interventie, is nog niet volledig uitgekristalliseerd in het internationaal recht. Het gaat om het bewegen van een staat tot het doen of laten van iets wat die staat normaliter niet vrijwillig zou doen. Het doel moet zijn om een verandering teweeg te brengen in het handelen van de staat die het doelwit is. Hoewel er geen eenduidige definitie van het dwangelement is, kan worden gesteld dat het gebruik van geweld altijd zal voldoen aan het element van een afdwingbaar effect. Geweldgebruik tegen een andere staat is altijd een vorm van interventie.

Verbod op geweldgebruik

Artikel 2(4) van het VN-Handvest bevat het verbod op het dreigen met of het gebruiken van geweld en luidt als volgt: «In hun internationale betrekkingen onthouden alle Leden zich van bedreiging met of het gebruik van geweld tegen de territoriale integriteit of de politieke onafhankelijkheid van een staat.» Dit verbod is van toepassing op elke vorm van geweldgebruik, ongeacht het wapen of middel dat hiervoor wordt ingezet.[13]
Het geweldverbod is nagenoeg absoluut. Er zijn slechts drie situaties waarbij het gebruik van geweld of het dreigen ermee niet in strijd is met internationaal recht. Dit is het geval bij zelfverdediging tegen een gewapende aanval (artikel 51 VN Handvest) en bepaalde acties ter implementatie van een resolutie van de VN Veiligheidsraad onder hoofdstuk 7 van het Handvest.[14] Daarnaast is geweldgebruik geen schending van het geweldverbod wanneer het plaatsvindt met instemming van de staat op wiens grondgebied geweld wordt gebruikt.
Bij de toepassing van dit verbod in het cyberdomein komt de vraag op of en wanneer bij cyberoperaties sprake is van het uitoefenen van geweld, aangezien geen gebruik wordt gemaakt van wapens in de gebruikelijke (fysieke) zin van het woord. Het kabinet is van mening dat cyberoperaties onder het geweldverbod kunnen vallen, namelijk wanneer de effecten van een cyberoperatie vergelijkbaar zijn met die van een conventionele geweldshandeling die onder het geweldverbod valt. Met andere woorden: de effecten van een operatie zijn bepalend, niet de manier waarop die effecten worden bereikt. Dit standpunt vindt steun in de rechtspraak van het Internationaal Gerechtshof, dat heeft vastgesteld dat gekeken moet worden naar de omvang en effecten van een operatie bij het oordeel of sprake is van een gewapende aanval in de context van het recht op zelfverdediging (zie hieronder). Er is geen reden aan te nemen dat dezelfde benadering niet zou moeten worden gevolgd bij het beoordelen of er sprake is van geweldgebruik in de zin van artikel 2(4) VN-Handvest. Een cyberoperatie zou daarom in ieder geval worden gekwalificeerd als geweldgebruik wanneer de omvang en effecten hetzelfde niveau bereiken als geweldgebruik bij niet cybergerelateerde operaties.
Een duidelijke definitie van geweldgebruik is niet voorhanden in het internationaal recht. Het kabinet onderschrijft het algemeen geaccepteerde standpunt dat per geval moet worden bekeken of sprake is van zodanige «omvang en effecten» dat sprake is van een schending van het

---

[13] *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion,* International Court of Justice (ICJ), 8 juli 1996, par. 39.

[14] Gebruik van geweld is niet hetzelfde als een gewapende aanval in het internationaal recht. Laatstgenoemde term is van belang in het kader van het recht op zelfverdediging. Dit wordt op pagina 9 verder besproken.

geweldverbod. In een advies over Digitale Oorlogvoering (2011) schreven de Adviesraad Internationale Vraagstukken en de Commissie van Advies inzake Volkenrechtelijke Vraagstukken dat *«de gebruikelijke uitleg van deze bepaling is dat alle vormen van gewapend geweld onder het verbod vallen, maar dat puur economische, diplomatieke en politieke druk of dwang niet vallen onder wat in artikel 2 lid 4 wordt verstaan onder geweld. Het beëindigen van de handelsrelaties of het bevriezen van tegoeden kan bijvoorbeeld zeer nadelig zijn voor de staat die het betreft, maar wordt tot nu toe niet beschouwd als vorm van geweld in de zin van het verbod uit het Handvest. Gewapend geweld met een feitelijk of mogelijk fysiek effect op de staat die het doelwit is, valt wel onder het verbod.»*[15] In de visie van het kabinet kan op dit moment niet worden uitgesloten dat een operatie met zeer ernstige financiële of economische gevolgen als geweldgebruik kan worden gekwalificeerd.
Bij het beoordelen van de omvang en effecten van een cyberoperatie moet naar zowel kwalitatieve als kwantitatieve factoren worden gekeken. In de Tallinn Manual 2.0 wordt een aantal factoren genoemd die hierbij een rol zouden kunnen spelen, waaronder de ernst van de gevolgen van de cyberoperatie, de ingrijpendheid ervan en de vraag of de operatie een militair karakter heeft of wordt uitgevoerd door een staat.[16] Dit zijn geen bindende juridische voorwaarden. Het gaat om factoren die een indicatie zouden kunnen geven dat een cyberoperatie kan worden gekwalificeerd als geweldgebruik, die het kabinet onderschrijft. Hierbij moet worden opgemerkt dat een cyberoperatie die onder de drempel blijft van geweldgebruik eventueel wel kan worden gekwalificeerd als een verboden interventie of een soevereiniteitsschending.

Zorgvuldigheidsbeginsel

Het zorgvuldigheidsbeginsel houdt in dat van staten verwacht wordt dat zij bij het uitoefenen van hun soevereiniteit rekening houden met de rechten van andere staten. Het beginsel is onder meer verwoord door het Internationaal Gerechtshof in de *Corfu Channel*[17] zaak, waar het oordeelde dat staten de plicht hebben op te treden wanneer zij kennis krijgen of hebben van het gebruik van hun grondgebied op een manier die de rechten van een derde staat schaadt. Hierbij moet worden aangetekend dat niet alle landen van mening zijn dat het zorgvuldigheidsbeginsel een op zichzelf staande verplichting onder het internationaal recht is. Nederland beschouwt het zorgvuldigheidsbeginsel wel als een op zichzelf staande verplichting, waarvan de schending een internationaal onrechtmatige daad kan opleveren.
In de cybercontext betekent het zorgvuldigheidsbeginsel dat staten moeten optreden tegen:
– cyberactiviteiten die worden uitgevoerd door personen op hun grondgebied of waarbij gebruik wordt gemaakt van zaken of netwerken op hun grondgebied of waar zij anderszins controle over hebben;
– die inbreuk maken op een recht van een andere staat; en
– waarvan zij op de hoogte zijn of zouden moeten zijn.[18]

---

[15] Digitale Oorlogvoering, No 77, AIV/ No 22, CAVV December 2011, p. 19.
[16] Tallinn Manual 2.0, Rule 69.
[17] *Corfu Channel Case; Assessment of Compensation (United Kingdom v. Albania)*, International Court of Justice (ICJ), 9 april 1949, par. 22.
[18] *Corfu Channel Case; Assessment of Compensation (United Kingdom v. Albania)*, International Court of Justice (ICJ), 9 april 1949, par. 44. Het Internationaal Gerechtshof concludeerde dat aan de *constructive knowledge standard* van het zorgvuldigheidsbeginsel (in internationaalrechtelijke zin) ook is voldaan wanneer een staat had moeten weten dat de activiteit plaatsvond op zijn grondgebied. Concreet betekent dit dat een staat verplicht is om alles wat redelijkerwijs mogelijk is te ondernemen. Wanneer in de cybercontext aan dit vereiste zal worden voldaan is momenteel nog onderwerp van discussie.

Hierbij moet een staat maatregelen nemen die in de gegeven omstandigheden van een redelijk handelende staat verwacht mogen worden. Niet van belang is of de desbetreffende cyberactiviteit wordt uitgevoerd door een statelijke of een niet-statelijke actor en waar deze actor zich bevindt. Als dus bijvoorbeeld een cyberaanval wordt uitgevoerd tegen Nederland waarbij gebruik wordt gemaakt van servers in een ander land, kan Nederland op grond van het zorgvuldigheidsbeginsel het andere land verzoeken om de servers uit te schakelen, ongeacht of vaststaat dat er een staat achter de cyberaanval zit.
Algemeen wordt aangenomen dat het zorgvuldigheidsbeginsel slechts van toepassing is als sprake is van voldoende ernstige negatieve gevolgen voor de staat op wiens recht(en) inbreuk wordt gemaakt. De precieze drempel hangt af van de specifieke omstandigheden van het geval. Wel is duidelijk dat niet per se sprake hoeft te zijn van fysieke schade.

Verplichtingen in een gewapend conflict – humanitair oorlogsrecht

Het humanitair oorlogsrecht (HOR) is van toepassing op optreden in het kader van een gewapend conflict. Dit geldt ook voor cyberoperaties die worden uitgevoerd in het kader van een gewapend conflict. Voorwaarde voor de toepassing van dit speciale rechtsgebied is dus de aanwezigheid van een (niet-internationaal of internationaal) gewapend conflict. In 2011 heeft het kabinet al aangegeven dat *«de toepassing van de regels van het humanitair oorlogsrecht (jus in bello) op vijandelijkheden in het digitale domein «technisch gezien haalbaar en juridisch gezien ook een vereiste» is.»*[19]
Belangrijk onderdeel van het HOR is het internationaal recht inzake neutraliteit. Neutraliteit houdt in dat staten die niet betrokken zijn bij het gewapend conflict zich onthouden van elke actie waaruit betrokkenheid bij, of het bevoordelen van een van de partijen in het conflict zou kunnen worden afgeleid. In de relaties met de strijdende partijen is de neutrale staat gehouden hen gelijk te behandelen om zo zijn neutraliteit te handhaven. Zo mag een staat niet de toegang tot zijn IT-systemen ontzeggen aan de ene partij bij het conflict en niet aan de andere partij. Het kabinet benadrukte in de kabinetsreactie op voornoemd AIV/CAVV-advies reeds dat *«Nederland kan bij een gewapend conflict van andere partijen zijn neutraliteit beschermen door het verhinderen van het gebruik door deze partijen van infrastructuur en systemen (bijv. botnets) op Nederlands grondgebied. Hierbij is permanente waakzaamheid geboden. Een goede inlichtingenpositie en een permanente scanfunctie zijn hierbij noodzakelijk.»*[20]
Het HOR bevat verder specifieke regels inzake aanvallen gericht op personen of objecten, die onverkort gelden voor cyberoperaties die worden ingezet in de context van een gewapend conflict.[21] Bij het plannen en uitvoeren van dit soort operaties dient te worden gehandeld in overeenstemming met bijvoorbeeld de beginselen van onderscheid en proportionaliteit, alsook de verplichting tot het treffen van voorzorgsmaatregelen.

---

[19] Digitale Oorlogvoering, No 77, AIV/ No 22, CAVV December 2011, p. 23; Kabinetsreactie op het AIV/CAVV-advies Digitale Oorlogvoering, 17 januari 2012.
[20] Digitale Oorlogvoering, No 77, AIV/ No 22, CAVV December 2011, p. 26.
[21] Aanvullend Protocol bij de Verdragen van Genève van 12 augustus 1949, betreffende [...] van internationale gewapende conflicten (Protocol I), Bern, 08 juni 977, artikel 49; Tallinn Manual 2.0, Rule 92. Het voert te ver om in deze brief in te gaan op de technische discussie over het onderscheid tussen cyberoperatie en cyberaanval in de context van een gewapend conflict.

Mensenrechten

Mensenrechten vormen een belangrijk onderdeel van het internationaal recht en zijn onder meer vastgelegd in een aantal VN-verdragen en in het Europees Verdrag voor de Rechten van de Mens (EVRM). Hieronder vallen bijvoorbeeld het recht op leven, het verbod op foltering of onmenselijke of vernederende behandeling en het recht op een eerlijk proces.
Staten hebben de plicht om de mensenrechten van iedereen die zich binnen hun rechtsmacht bevindt, te respecteren en te beschermen. Dit houdt niet alleen de «negatieve» verplichting in om zich te onthouden van handelingen die mensenrechten schenden, maar ook de «positieve» verplichting om ervoor te zorgen dat mensen ook daadwerkelijk hun rechten kunnen uitoefenen en zich kunnen verdedigen tegen inbreuken door anderen. Zo is het niet voldoende dat de Nederlandse overheid zelf de privacy van haar burgers respecteert, maar moet zij ook maatregelen treffen om ervoor te zorgen dat bijvoorbeeld bedrijven de privacy van hun klanten respecteren.
De meeste mensenrechten zijn niet absoluut, wat betekent dat inperkingen ervan onder voorwaarden worden toegestaan. Zo mogen staten bijvoorbeeld haatzaaien of opruien tot geweld strafbaar stellen, al heeft dit implicaties voor de vrijheid van meningsuiting van bepaalde individuen. De toets om te beoordelen of een specifieke inperking geoorloofd is, verschilt per verdragsbepaling, maar houdt in de meeste gevallen in dat beoordeeld wordt of de inperking een legitiem doel dient, voorzien is bij wet en noodzakelijk en proportioneel is. Daarnaast is het voor een beperkt aantal mensenrechten mogelijk om de naleving ervan gedeeltelijk en gedurende een beperkte periode op te schorten in noodsituaties. Denk aan het instellen van een avondklok in geval van een oorlogssituatie.
Mensenrechten gelden in het cyberdomein evenzeer als in het fysieke domein. Er is geen verschil tussen online en offline rechten. Dit is onder meer erkend door de Algemene Vergadering van de Verenigde Naties.[22] Wel is duidelijk dat de voortschrijdende digitalisering en technologische ontwikkeling leiden tot nieuwe vragen en uitdagingen voor de toepassing van mensenrechten. Zo leiden de toegenomen mogelijkheden om gegevens te verzamelen, op te slaan en te verwerken bijvoorbeeld tot vragen in het kader van het recht op privacy. Op vergelijkbare wijze leiden de toegenomen mogelijkheden voor personen om zich te uiten via online platformen tot vragen in het kader van de vrijheid van meningsuiting. Niet kan worden uitgesloten dat voor een aantal van deze vraagstukken in de toekomst nadere (internationale) regelgeving nodig zal zijn. Vooralsnog is het kabinet echter van mening dat de bestaande mensenrechteninstrumenten voldoende ruimte bieden om effectieve bescherming van mensenrechten in het cyberdomein te garanderen.
Duidelijk is verder dat (toegang tot) het internet in toenemende mate van belang is voor de effectieve uitoefening van mensenrechten. Niet alleen voor mensenrechtenverdedigers en mensenrechten NGO's, die bijvoorbeeld via sociale media-aandacht kunnen vragen voor mensenrechtenschendingen en hun achterban kunnen mobiliseren, maar voor iedereen. Rechten als de vrijheid van meningsuiting en de vrijheid van vereniging en vergadering hebben bijvoorbeeld een nieuwe dimensie gekregen met de komst van sociale media, evenals het recht op onderwijs en gezondheid met de enorme toevloed aan informatie en trainingen die online te vinden zijn. Maar ook het recht op privé en familieleven, met de toegenomen mogelijkheden om digitaal te communiceren. Tegelijkertijd zijn de risico's op schendingen van mensenrechten online toegenomen. Te denken valt aan toegenomen surveillancemogelijkheden en desinformatie praktijken.

---

[22] Zie bijvoorbeeld *The Right to Privacy in the Digital Age*, GA Res. 68/167, para. 3, UN Doc. A/RES/68/167 (December 2013).

Het alsmaar toenemende belang van het internet voor mensenrechten onderstreept de noodzaak van een veilig, open en vrij internet. Hier zet het kabinet zich internationaal voor in.

Toerekening (attributie)

Voor de internationaalrechtelijke aansprakelijkheid van een andere staat voor een cyberoperatie, en daarmee de mogelijkheid om een door het internationaal recht toegestane tegenmaatregel in reactie op die operatie te kunnen treffen,[23] is het noodzakelijk dat de operatie kan worden toegerekend aan die staat. Aan de attributie van cyberoperaties ligt altijd een kabinetsbesluit ten grondslag. Daarbij gaat bijzondere aandacht uit naar de mate van beschikking over eigen informatie dan wel naar een zelfstandig oordeel over verkregen informatie.
In het cyberdomein kan onderscheid worden gemaakt tussen drie vormen van toerekening:

– Technische toerekening: een feitelijk en technisch onderzoek naar de mogelijke dader(s) achter de cyberoperatie en de mate van zekerheid waarmee dit kan worden vastgesteld.
– Politieke toerekening: een beleidsafweging waarbij wordt besloten om, al dan niet publiekelijk, politiek een specifieke cyberoperatie toe te rekenen aan een actor, zonder dat hier per se juridische gevolgen aan worden verbonden, zoals het nemen van tegenmaatregelen. Hierbij hoeft niet te worden toegerekend aan een staat: het kan ook gaan om een private actor.
– Juridische toerekening: de beslissing waarbij de benadeelde staat het handelen of nalaten door een specifieke staat toerekent aan die staat met het doel deze staat in juridische zin aansprakelijk te stellen voor het schenden van een internationaalrechtelijke verplichting.

Bij juridische toerekening moet onderscheid worden gemaakt tussen operaties uitgevoerd door of namens staten, en operaties van niet-statelijke actoren. Een handeling uitgevoerd door een staatsorgaan in zijn officiële hoedanigheid (bijvoorbeeld het NCSC) is altijd toerekenbaar aan de staat. Een handeling van een niet-statelijke actor is in beginsel niet toerekenbaar aan een staat. Dit is anders wanneer een staat effectieve controle uitoefent over die handeling, dan wel de handeling achteraf aanvaardt als zijn eigen handeling. Dit betekent dat de niet-statelijke actor (ook wel *proxy* genoemd) de operatie uitvoert op instructie van, of op aanwijzing of onder controle van de staat *(direction or control)*. De drempel voor het constateren van effectieve controle ligt hoog. Een financiële bijdrage aan de activiteiten van een niet-statelijke groep is bijvoorbeeld niet voldoende.
Voor toerekening is niet vereist dat het onderliggende bewijs wordt vrijgegeven. Bewijs wordt in juridische zin pas relevant als sprake is van een juridische procedure. Het kan voorkomen dat een staat die tegenmaatregelen neemt of een beroep doet op het inherente recht op zelfverdediging (zie hieronder) in reactie op een cyberoperatie, dit op den duur moet kunnen verantwoorden, bijvoorbeeld wanneer de kwestie aanhangig wordt gemaakt bij het Internationaal Gerechtshof. In een dergelijke situatie moet bewijs kunnen worden overhandigd dat het nemen van de tegenmaatregel of het beroep op zelfverdediging rechtvaardigt. Hierbij wordt zowel gedoeld op verkregen via reguliere kanalen alsook materiaal bestaande uit inlichtingen.
Het internationaal recht kent geen vaste standaard voor de bewijslast waaraan een staat moet voldoen bij (juridische) toerekening en het Internationaal Gerechtshof heeft tot nu toe verschillende bewijsstandaarden geaccepteerd. De CAVV en AIV merken ook terecht het volgende op: *«het internationaal recht kent geen harde regels voor de vereiste*

[23] Zie voor een bespreking van tegenmaatregelen pagina 8 van deze bijlage.

hoeveelheid bewijs, maar de praktijk en jurisprudentie vergen toch wel dat er, voordat een actie wordt uitgevoerd, een voldoende mate van zekerheid bestaat over de herkomst van de aanval en de identiteit van de aanvallers.»[24]
Het kabinet is van mening dat de bewijslast per situatie inderdaad verschilt, afhankelijk van de ernst van de handelingen die in strijd worden geacht met internationaal recht en de voorgenomen maatregelen hiertegen.

Responsopties voor staten

Het internationaal recht biedt staten verschillende opties om te reageren op gedragingen door een andere staat in het cyberdomein. Van welke opties in een concreet geval gebruik kan worden gemaakt, hangt af van de specifieke omstandigheden. Hieronder worden de belangrijkste responsopties vermeld en toegelicht.

Retorsie

Met retorsie wordt verwezen naar handelingen die weliswaar onvriendelijk zijn, maar niet in strijd met het internationaal recht. Deze optie is daarmee altijd beschikbaar voor staten die willen reageren op onwenselijk gedrag van een andere staat, omdat het gaat om de rechtmatige uitoefening van de bevoegdheden die zij als soevereine staat hebben. Staten zijn vrij om dit soort maatregelen te nemen zolang ze binnen de grenzen blijven van hun internationaalrechtelijke verplichtingen.
Een staat kan bijvoorbeeld in reactie op een cyberoperatie door een andere staat reageren door diplomaten tot «persona non grata» te verklaren, of economische of andersoortige maatregelen te treffen tegen de individuen of entiteiten die bij de operatie betrokken waren. Ook is het mogelijk dat een staat als retorsiemaatregel de toegang van de andere staat tot servers of andere digitale infrastructuur op zijn grondgebied beperkt of afsluit, behalve als beide landen bijvoorbeeld een verdrag over wederzijdse toegang tot digitale infrastructuur op elkaars grondgebied hebben gesloten.

Tegenmaatregelen (countermeasures)

Een staat mag onder bepaalde omstandigheden tegenmaatregelen nemen tegen een schending van een internationaalrechtelijke verplichting door een andere staat waarvan hij slachtoffer is (internationaal onrechtmatige daad).[25] Tegenmaatregelen zijn handelingen (of een nalaten) die normaliter een schending zouden opleveren van een internationaalrechtelijke verplichting maar die geoorloofd zijn omdat zij een reactie zijn op een eerdere schending van een internationaalrechtelijke verplichting door een andere staat. In het cyberdomein kan bijvoorbeeld gedacht worden aan het via een cyberoperatie uitschakelen van netwerken of systemen die door een ander land worden gebruikt bij een cyberaanval. Als handeling die normaliter in strijd zou zijn met het internationaal recht verschilt de tegenmaatregel van retorsie. Voor tegenmaatregelen gelden daarom strikte eisen, waaronder de eis dat de benadeelde staat de andere staat aansprakelijk stelt. Dit houdt in dat de benadeelde staat vaststelt dat sprake is van een schending van internationale verplichting die geldt tussen de benadeelde en de aansprakelijke staat, en dat de cyberoperatie kan worden toegerekend aan de aansprakelijke staat. Daarnaast moet de

[24] Digitale Oorlogvoering, No 77, AIV/ No 22, CAVV December 2011, p. 21.
[25] Zie voor een uitgebreidere uiteenzetting van het begrip tegenmaatregelen de brief van de Minister van Buitenlandse Zaken aan de Tweede Kamer hierover van 11 april 2013, Kamerstuk 32 500 V, nr. 166.

benadeelde staat in principe de andere staat op de hoogte stellen van het voornemen tegenmaatregelen te nemen. In het geval onmiddellijk handelen is vereist om de rechten van de benadeelde staat te handhaven en verdere schade te voorkomen, mag van notificatie worden afgezien. Verder moeten tegenmaatregelen onder meer tijdelijk en proportioneel zijn, mogen ze geen fundamentele mensenrechten schenden en mogen ze niet neerkomen op (dreigen met) geweldgebruik.

Noodzaak (necessity)

Noodzaak (*necessity*) is een rechtvaardigingsgrond die onder bepaalde strikte voorwaarden een rechtvaardiging biedt voor handelen dat anders als internationaal onrechtmatig zou worden bestempeld, zoals bijvoorbeeld het inzetten van offensieve cybermiddelen tegen een andere staat. Een staat kan een beroep doen op deze rechtvaardigingsgrond wanneer aan de volgende voorwaarden is voldaan:

– Er is sprake van een onmiddellijke en ernstige dreiging tegen een essentieel belang van de desbetreffende staat.
– Er is geen andere mogelijkheid om hiertegen op te treden dan het tijdelijk niet voldoen aan een of meer internationaalrechtelijke verplichtingen van de bedreigde staat.
– De tijdelijke niet-naleving maakt geen ernstige inbreuk op de essentiële belangen van een andere staat jegens welke de internationale verplichting bestaat of van de internationale gemeenschap en het internationaal recht staat een beroep op noodzaak voor deze specifieke verplichting toe.[26]
– De staat heeft niet zelf bijgedragen aan het ontstaan van de noodsituatie.

Noodzaak kan dus slechts in uitzonderlijke gevallen worden ingeroepen, wanneer niet alleen sprake is van (mogelijk) zeer ernstige gevolgen maar ook van een essentieel belang van het bedreigde land. Wat onder «essentieel belang» valt, zal zich moeten uitwijzen in de praktijk, maar zaken als het elektriciteitsnetwerk, de watervoorziening of het bancaire stelsel vallen er in de visie van het kabinet in ieder geval onder.
Voor wat betreft de zeer ernstige gevolgen die voor het vaststellen van een situatie van noodzaak vereist zijn, geldt dat de schade zich nog niet hoeft te hebben voorgedaan, maar wel onmiddellijk dreigend en objectief vast te stellen moet zijn. Wanneer schade als ernstig genoeg bestempeld kan worden om een beroep op noodzaak te rechtvaardigen, staat niet vast en zal per geval moeten worden vastgesteld. Het enkel hinderen of veroorzaken van ongemak is niet voldoende. De (dreigende) schade hoeft niet noodzakelijkerwijs fysiek te zijn: situaties waarbij het nagenoeg het gehele internet onbereikbaar wordt gemaakt of ernstige schokken worden veroorzaakt op de financiële markten, kunnen onder omstandigheden worden gekwalificeerd als situaties waarin een beroep op noodzaak mogelijk is. Verder geldt dat het voor het bestaan van een situatie van noodzaak niet nodig is dat wordt vastgesteld waar de schade precies vandaan komt of dat een andere staat er verantwoordelijk voor kan worden gesteld: de rechtvaardigingsgrond is er vooral op gericht om een staat de mogelijkheid te bieden de eigen belangen te beschermen en de schade te minimaliseren.
De handelingsmogelijkheden voor een staat die zich beroept op een situatie van noodzaak zijn beperkt. De rechtvaardigingsgrond kan alleen worden ingeroepen voor schendingen van internationaalrechtelijke verplichtingen waarbij er geen andere reële mogelijkheid is om op te treden tegen de (dreigende) schade en waarbij geen inbreuk wordt

[26] Voor sommige internationale verplichtingen wordt het inroepen van een rechtvaardigingsgrond voor het schenden ervan niet toegestaan. Het gaat om zogenaamde dwingende bepalingen van het internationaal recht, zoals het verbod op genocide.

gemaakt op de essentiële belangen van een andere staat of van de internationale gemeenschap als geheel.

Zelfverdediging

Een staat die het doelwit is van een cyberoperatie die gekwalificeerd kan worden als een gewapende aanval mag gebruik maken van het inherente recht tot zelfverdediging en geweld gebruiken om zichzelf te verdedigen.[27] Dit recht is neergelegd in artikel 51 van het VN-Handvest. Het komt dus neer op een rechtvaardiging van geweldgebruik dat normaliter wordt verboden door artikel 2(4) van het VN-Handvest.[28] Aan de uitoefening van het recht op zelfverdediging zijn daarom strenge voorwaarden verbonden. Een gewapende aanval is niet hetzelfde als geweldgebruik, zoals die term wordt gebruikt in artikel 2(4) van het VN-Handvest (zie hierboven). In de *Nicaragua*-zaak heeft het Internationaal Gerechtshof een gewapende aanval gekwalificeerd als de meest ernstige vorm van geweldgebruik. Hieruit volgt dat niet elke vorm van geweldgebruik een gewapende aanval is.
Voor de kwalificatie van een operatie als gewapende aanval moet worden gekeken naar de omvang en effecten van de aanval.[29] Het internationaal recht is niet eenduidig over de precieze omvang en effecten die een aanval moet hebben voordat sprake is van een gewapende aanval. Wel is duidelijk dat een gewapende aanval niet noodzakelijkerwijs wordt uitgevoerd met kinetische middelen. Deze opvatting is in overeenstemming met het advies van het Internationaal Gerechtshof over *Nucleaire Wapens,* waarin het Hof concludeerde dat het middel waarmee de aanval wordt uitgevoerd niet bepalend is voor de kwalificatie van een aanval als gewapende aanval. Het kabinet onderschrijft in dit verband de bevinding van de CAVV/AIV dat *«een digitale aanval die qua gevolgen (dodelijke slachtoffers, schade en vernietiging) vergelijkbaar is met een gewapende aanval kan een reactie met digitale middelen of met conventionele gewapende middelen rechtvaardigen.»* Er is dan ook geen reden waarom een digitale aanval op een computer- of informatiesysteem niet zou kunnen gelden als een gewapende aanval, indien de gevolgen ervan vergelijkbaar zijn met die van een aanval met conventionele of onconventionele wapens.
Op dit moment is er internationaal geen overeenstemming over het eventueel kwalificeren als gewapende aanval van een cyberaanval die geen dodelijke slachtoffers, fysieke schade of vernietiging veroorzaakt maar wel zeer ernstige niet-fysieke gevolgen teweegbrengt.
Het kabinet onderschrijft het standpunt van het Internationaal Gerechtshof dat heeft opgemerkt dat een gewapende aanval een grensoverschrijdend karakter moet hebben. Hierbij moet worden opgemerkt dat niet alle gewapende grensincidenten neer komen op een gewapende aanval in de zin van artikel 51 van het VN Handvest: dit hangt altijd af van de omvang en effecten van de desbetreffende incidenten.[30]
De bewijslast voor gerechtvaardigde zelfverdediging tegen een gewapende aanval ligt hoog. Het kabinet deelt de conclusie van de CAVV/AIV *«Geen enkele vorm van zelfverdediging mag worden uitgevoerd zonder voldoende bewijs omtrent de herkomst en bron van de aanval en zonder overtuigend bewijs dat een bepaalde staat of bepaalde staten of een georganiseerde groep verantwoordelijk is voor de uitvoering van of controle op de aanval.»*[31] Staten mogen daarom alleen gebruik

---

[27] Handvest van de Verenigde Naties, San Francisco, 26 juni 1945 Artikel 51.
[28] Het begrip verbod op geweldgebruik wordt hierboven uitgelegd, op pagina 3.
[29] *Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America),* International Court of Justice (ICJ), 27 juni 1986, par. 195.
[30] *Idem*.
[31] Digitale Oorlogvoering, No 77, AIV/ No 22, CAVV December 2011, p. 21.

maken van geweld ter zelfverdediging indien de herkomst van de aanval en de identiteit van de aanvallers met een voldoende mate van zekerheid kan worden vastgesteld. Het kan hierbij gaan om statelijke of niet-statelijke actoren.
Bij het uitoefenen van hun recht op zelfverdediging moeten staten zich daarnaast houden aan de voorwaarden van noodzakelijkheid en proportionaliteit. Het kabinet deelt in dit verband de bevindingen van CAVV en AIV op dit punt: *«het beroep op zelfverdediging is slechts gerechtvaardigd indien het afslaan van de aanval het doel is, de maatregelen niet uitgaan boven dat doel en er geen haalbare alternatieven zijn. Het vereiste van proportionaliteit sluit maatregelen uit die het gevaar van escalatie naar een grotere intensiteit met zich meebrengen en die niet strikt noodzakelijk zijn om de aanval af te slaan en aanvallen in de nabije toekomst te voorkomen.»*