Consequenties van een nieuw type oorlogsvoering

Prins, Corien

Published in:
Nederlands Juristenblad

Publication date:
2019

Consequenties van een nieuw type oorlogsvoering

30 Digitalisering heeft ons veel gebracht, maar kent ook schaduwzijden. Al langer benutten kwaadwillende partijen de technologie in hun voordeel. Oplichting, spionage, gijzeling met behulp van zgn. ransomware en het platleggen van systemen: het behoort tot de realiteit van de digitale wereld. Met name de anonimiteit die het internet biedt, maakt het aantrekkelijk voor criminelen en staten om langs digitale weg twijfel te zaaien of ernstige schade aan te richten.

Met ontwikkelingen als kunstmatige intelligentie lijkt digitalisering zich te ontwikkelen tot wat het 'perfecte wapen' wordt genoemd.[1] Veel cyberwapens zijn relatief goedkoop. Ze zijn inzetbaar voor een variëteit aan doeleinden. En het benutten ervan valt vervolgens redelijk eenvoudig te ontkennen. Maar belangrijker wellicht nog is dat het nieuwe wapentuig de (geopolitieke) orde verandert. De machtsbalans verschuift, nu ook kleinere landen zich op het mondiale strijdtoneel kunnen begeven. Zonder dat ze daartoe een grootschalige militaire confrontatie aan moeten gaan of feitelijk het grondgebied van een andere staat dienen te betreden. Kortom, op relatief eenvoudige wijze valt grote slagkracht te ontwikkelen. Illustratief zijn twee cyberaanvallen in 2017 – NotPetya en WannaCry – waarbij bedrijven en organisaties in meer dan honderd landen werden geraakt, met miljarden dollars aan schade tot gevolg.

Ook ons land begeeft zich kennelijk op dit nieuwe strijdtoneel. Volkskrant-journalist Modderkolk beschreef in zijn recente boek *Het is oorlog, maar niemand die het ziet*, dat Nederland de helpende hand bood bij de hack op het Iraanse nucleaire programma. Die aanval werd al in 2010 bekend, maar dat ons land een cruciale rol speelde is nieuw. De actie roept talloze vragen op. Niet alleen die naar de wenselijkheid van Nederlandse betrokkenheid. Problematisch is dat internationale regels over wat met behulp van digitale middelen is toegestaan en wat een proportionele respons is, ontbreken. Ook zijn er vragen hoe een cyberaanval te kwalificeren. Er wordt immers geen gebruik gemaakt van wapens in de klassieke – fysieke – zin van het woord.

Alhoewel in EU- en VN-verband wordt gesproken over het verduidelijken en versterken van een internationaal normatief kader, is de voortgang traag. Veel staten zijn terughoudend in de bijdrage aan de ontwikkeling van specifieke internationale gedragsregels en houden de eigen activiteiten in cyberspace vaak geheim. Nederland is een actief pleitbezorger van de zgn. Tallinn Manual. De Manual biedt een normatief kader voor onder meer de volkenrechtelijke vraag wanneer een cyberaanval als een 'armed attack' geldt en wanneer slechts als 'use of force'.[2]

Vlak voor het zomerreces informeerde Minister van Buitenlandse Zaken, Blok, het parlement over het Nederlands standpunt inzake de kwalificatie van cyberaanvallen.[3] Volgens het kabinet moet per geval 'worden bekeken of sprake is van zodanige "omvang en effecten" dat sprake is van een schending van het geweldverbod.' Ook cyberoperaties kunnen in principe onder dit verbod vallen, aldus het kabinet, 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. (...) 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.' Onder verwijzing naar het advies over Digitale Oorlogvoering (2011) van de Adviesraad Internationale Vraagstukken en de Commissie van Advies inzake Volkenrechtelijke Vraagstukken merkt het kabinet verder op dat op dit moment niet valt uit te sluiten dat een operatie met zeer ernstige financiële of economische gevolgen als geweldgebruik is te kwalificeren. Dat de schade kan oplopen tonen de genoemde NotPetya- en WannaCry-aanvallen. De meest gunstige schatting van het totaal schadebedrag voor beide aanvallen is een luttele 15 miljard dollar.

Juist omdat de financiële of economische gevolgen ook burgers en bedrijven zwaar kunnen treffen, is een belangrijke vraag of er voor de schade dekking is. Valt deze schade te verzekeren? De schadeclaims als gevolg van NotPetya- en WannaCry waren voor enkele grote verzekeraars aanleiding om de dekking van hun verzekeringen verder te beperken. Zij voelden zich daarin gesteund door de Amerikaanse toeschrijving van de aanval aan Rusland. Schade als gevolg van gewapende conflicten valt vanwege het te grote financiële risico lang niet overal te verzekeren.[4] Maar ging het bij NotPetya, WannaCry of de Nederlandse betrokkenheid bij de cyber-aanval in Iran om een oorlogshandeling of was het niet meer dan fysieke sabotage? Duidelijk is in ieder geval dat cyberaanvallen zich niet zo eenvoudig in een helder kader laten onderbrengen. Maar ondertussen lijken verzekeraars cyberaanvallen meer en meer als gewapend conflict aan te merken. Met als problematisch gevolg dat er geen compensatiemechanismen voor bedrijven en andere slachtoffers zijn.[5] Een aantal van de getroffen bedrijven heeft de stap naar de rechter gezet. Daarmee ziet het ernaar uit dat waar staten nog niet in staat zijn meer helderheid te bieden, het nu aan de rechter is om knopen door te hakken. Ondertussen zijn het bedrijven, organisaties en burgers die zonder compensatie met de feitelijke schade en andere gevolgen van de nieuwe oorlogsvoering achterblijven.

Corien Prins

1. Sanger, D.A. (2018), *The perfect weapon. War sabotage and fear in the cyber age*, New York; Crown.
2. Zie: Eric Talbot Jensen, 'The Tallinn Manual 2.0: Highlights and Insights', *Georgetown Journal of International Law*, Vol. 48 (2017).
3. *Kamerstukken II* 2018/19, 33694, nr. 47.
4. www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html
5. Zie in meer detail het WRR-rapport *Voorbereiden op Digitale Ontwrichting*, 2019.