Maersk, the shipping giant, has suffered millions of dollars in damage due to the NonPetya ransomware attack http://zd.net/2DV9fgP by @SecurityCharlie

ZDNet @ZDNet

6 Cyberaanval op Maersk

Menno van Duin, Jimmy Maan

6.1 Inleiding

Op 27 juni 2017 kwam in de haven van Rotterdam van het ene op het andere moment het vrachtverkeer bij APM Terminals tot stilstand. Bij het Deense bedrijf – dat onderdeel is van scheepvaart- en transportgigant Maersk – bleken de computers te zijn vergrendeld door de *malware* NotPetya (zie kader). Al snel bleek dat niet alleen APM Terminals, maar ook andere bedrijven slachtoffer waren van deze cyberaanval. Het stilvallen van de terminals leidde tot grote problemen: vrachtschepen konden niet worden gelost, lagen dagenlang stil of moesten uitwijken naar andere havens. De financiële schade voor alleen al APM Terminals liep op tot enkele honderden miljoenen euro's.[1] Het Havenbedrijf Rotterdam moest alle zeilen bijzetten om het uitwijkende vrachtverkeer in goede banen te leiden. Het Nationaal Cyber Security Centrum (NCSC) werd ingeschakeld om de effecten van deze aanval op de vitale infrastructuur te bewaken. Ondertussen werd wereldwijd met man en macht getracht de aard en omvang van deze cyberaanval te inventariseren.

De invloed die cyberaanvallen kunnen hebben op het functioneren van een maatschappij maakt dat uit deze casus waardevolle lessen kunnen worden geleerd. Cyberaanvallen behoren tot een van de belangrijkste (on)veiligheidsproblemen van dit moment.[2] Er is bijna geen krant

1 In het jaarverslag van het moederbedrijf A.P. Møller-Mærsk wordt gesproken van een geschatte schade tussen de 250 en 300 miljoen dollar. Wereldwijd wordt de schade door Cyberreason.com geschat op zeker 1,2 miljard dollar.

2 Zie hierover bijvoorbeeld MT.nl, 15 oktober 2018. Management: Technologie: Cybersecurity: 'Alleen met open deuren kunnen we de cyberwereld redden'. Op 5 novem-

open te slaan of een journaaluitzending te volgen of er wordt wel in een item een link met dit onderwerp gelegd (Russische spionage, hackers, diefstal of afpersing via internet e.v.).

Voor dit hoofdstuk is gebruikgemaakt van mediaberichtgeving en openbare publicaties van betrokken partijen. Ook zijn blogs verwerkt van analisten die zich de eerste dagen hebben gestort op het ontrafelen van de *malware* NotPetya.

6.2 Feitenrelaas

In de ochtend van 27 juni 2017 beginnen bij verschillende bedrijven en overheidsinstellingen in Oekraïne computersystemen vast te lopen. Computers worden automatisch vergrendeld en gebruikers krijgen een melding dat zij driehonderd dollar aan bitcoins moeten overmaken om weer toegang te krijgen tot hun bestanden. Door heel het land worden verstoringen gemeld, zowel bij ziekenhuizen als bij elektriciteitscentrales en telecomproviders. Ook de metro en het vliegveld van Kiev ondervinden hinder van de cyberaanval. Voor even komt in Oekraïne het maatschappelijke leven tot stilstand.

Al snel verspreidt de cyberaanval zich naar andere landen, waaronder Denemarken, Frankrijk, het Verenigd Koninkrijk en de Verenigde Staten.[3] Ook het Nederlandse TNT Express ondervindt problemen (NCTV, 2018).

Zowel overheidsinstanties als private beveiligingsbedrijven (Kaspersky, Eset, Symantec en Talos) starten een onderzoek naar de bron en aard van de besmetting. Via blogs publiceren onderzoekers hun bevindingen en na analyse van de code van de *malware* wordt duidelijk dat wat eerst een aanval van *ransomware* leek te zijn, een aanval van meer destructieve aard is die de naam NotPetya meekrijgt.

ber 2018 ontleend aan https://www.mt.nl/management/technologie/cybersecurity/alleen-met-open-deuren-kunnen-we-de-cyberwereld-redden/561111.

3 Emerce.nl, 29 juni 2017. Nieuws: Nederland op vier na grootste slachtoffer Petya. Op 5 november 2018 ontleend aan https://www.emerce.nl/nieuws/nederland-vier-na-grootste-slachtoffer-petya.

NotPetya: geen *ransomware*, maar *wiperware*
NotPetya (ook bekend onder de namen Nyetya, ExPetr of New Petya) is een *malware* voor Windowssystemen. In tegenstelling tot de verspreiding van de meeste andere *malware*, waarbij een handeling van het slachtoffer (bijvoorbeeld het openen van een geïnfecteerde bijlage) het virus toegang geeft tot het systeem, vindt de verspreiding van NotPetya zelfstandig plaats via interne netwerken van bedrijven.
NotPetya vertoonde aanvankelijk overeenkomsten met Petya, een virus dat in de categorie *ransomware* valt. Bij *ransomware* worden computers of bestanden vergrendeld en krijgen gebruikers pas weer toegang, nadat zij geld hebben overgemaakt aan de verspreider van het virus. Om opsporing te bemoeilijken wordt hierbij doorgaans gebruikgemaakt van cryptovaluta, zoals bitcoins.
Bij NotPetya kregen slachtoffers een soortgelijke melding. NotPetya bleek echter geen *ransomware*, maar *wiperware* te zijn. Data op de geïnfecteerde systemen werd niet vergrendeld, maar onherstelbaar beschadigd. Ook bleken geïnfecteerde computers een willekeurig gegenereerde 'unieke code' te krijgen waardoor ontgrendeling niet kon plaatsvinden. Kaspersky Labs gaf aan dit nieuwe virus de naam NotPetya, vanwege de uiterlijke overeenkomsten met het in 2016 opgedoken Petya.[4]

De cyberaanval is te herleiden tot software updates van het Oekraïense boekhoudprogramma M.E.Doc.[5] Onderzoekers van het beveiligingsbedrijf Talos reizen af naar Oekraïne om M.E.Doc te assisteren in het analyseren van hun systemen en om te achterhalen op welke wijze bij het bedrijf is binnengedrongen.[6] Gaandeweg blijkt dat hackers zich op ingenieuze wijze al maandenlang toegang hebben weten te verschaffen tot de systemen van Intellect Service, het moederbedrijf van M.E.Doc. Dit is een softwareontwikkelaar van onder andere het boekhoudsysteem M.E.Doc, dat veelvuldig wordt gebruikt om gegevens uit te wisselen met de Oekraïense belastingdienst. Door de malware te verstoppen in het updateproces van software kwam NotPetya ongemerkt de netwerken binnen van bedrijven die gebruikmaakten van deze software. Gedurende enkele maanden zijn updates uitgebracht met een *backdoor,* een door hackers aangebrachte wijziging van de M.E.Doc

4 Kaspersky.com, 27 juni 2017. Blog: New Petya/NotPetya/ExPetr ransomware outbreak. Op 5 november 2018 ontleend aan https://www.kaspersky.com/blog/new-ransomware-epidemics/17314/.
5 Zie voor de beschrijving van deze casus bijvoorbeeld NCTV, 2018, p. 15.
6 TalosIntelligence.com, 5 juli 2017. Blog: The MeDoc Connection. Op 5 november 2018 ontleend aan https://blog.talosintelligence.com/2017/07/the-medoc-connection.html?m=1.

software, waardoor zij op 27 juni NotPetya konden verspreiden onder klanten van deze softwareleverancier.

Ook de computersystemen van Maersk raken via deze weg besmet.[7] Rond 13.15 uur op 27 juni 2017 bereikt NotPetya via het interne netwerk van Maersk de systemen van APM Terminals in de Rotterdamse haven. Kranen van APM Terminals, die normaal gesproken goed zijn voor een derde van de goederenoverslag in de Rotterdamse haven, komen als gevolg van de cyberaanval tot stilstand. Terwijl het virus zich bij verschillende bedrijven over de hele wereld verspreidt, blijft binnen de Rotterdamse haven de schade beperkt tot de bedrijven van Maersk.

Hoewel individuele bedrijven in het Rotterdamse havengebied (op dat moment) geen meldplicht hebben voor cyberaanvallen, heeft deze cyberaanval een dermate grote verstoring van het vrachtverkeer tot gevolg dat APM Terminals zich genoodzaakt ziet het Rotterdamse Havenbedrijf in te lichten. Een uur nadat NotPetya de Rotterdamse haven heeft bereikt, krijgt de havenmeester een telefoontje van een medewerker van APM Terminals. Omdat het Rotterdamse havengebied is aangewezen als vitaal onderdeel van de Nederlandse infrastructuur, en de havenmeester als 'port cyber resilience officer' daarom een meldplicht heeft voor ernstige ICT-incidenten, stelt deze het NCSC direct op de hoogte. Op 28 juni voorziet het Havenbedrijf bedrijven van gedetailleerde informatie over de cyberaanval en van een handelingsperspectief voor grootschalige cyberaanvallen. Onder meer wordt geadviseerd updates te installeren, zodat de kwetsbaarheid tegen aanvallen wordt beperkt.[8]

Voor APM Terminal en bedrijven die van de goederenoverslag afhankelijk zijn, is de schade van de cyberaanval groot. Omdat de infrastructuur van de terminal op de Tweede Maasvlakte volledig geautomatiseerd is, kunnen schepen niet meer worden geladen of gelost. Ook de wat oudere terminal op de Eerste Maasvlakte ligt stil. Schepen moeten uit-

7 Drie van de negen bedrijfsonderdelen van Maersk werden geraakt: APM Terminals, Maersk Line en Damco. Zie Maersk Q2 2017 interim rapport. Op 5 november 2018 ontleend aan http://files.shareholder.com/downloads/ABEA-3GG91Y/5003725988x0x954063/4803DE66-B269-4730-8A92-C0D59BD7EE28/Presentation_Q2_2017.pdf.

8 FERM-Rotterdam.nl, 28 juni 2017. Nieuws en agenda: Handelingsperspectief grootschalige ransomware-aanval. Op 5 november 2018 ontleend aan https://ferm-rotterdam.nl/nl/nieuws/handelingsperspectief-grootschalige-ransomware-aanval.

wijken naar andere terminals en havens; het vrachtverkeer kan dagenlang niet bij de twee terminals van APM terecht. Slechts een deel van de activiteiten kan handmatig worden overgenomen, maar de kranen blijven stilstaan.[9]

De EternalBlue exploit

Voor de verspreiding en werking van NotPetya werd misbruik gemaakt van (onder andere) de EternalBlue exploit. Deze exploit is een (bijna met zekerheid) door de *National Security Agency* (NSA) van de Verenigde Staten ontdekte kwetsbaarheid in Windows computers, die het mogelijk maakt toegang te verkrijgen tot deze systemen (NCTV, 2018). Een hackersgroep genaamd 'Shadow Brokers' heeft de exploit weten te ontvreemden van de NSA en deze vervolgens op 14 april 2017 vrijgegeven.[10] Na ontdekking van de diefstal heeft Microsoft al in maart 2017 updates uitgebracht om de kwetsbaarheid te verhelpen, maar veel gebruikers hebben deze updates niet geïnstalleerd. Al snel werd deze exploit misbruikt voor de aanval met de ransomware WannaCry op 12 mei 2017.
Na de NotPetya cyberaanval op 27 juni 2017 wezen de Verenigde Staten, het Verenigd Koninkrijk en de Deense overheid met een beschuldigende vinger naar het Russische leger. Verspreiding van NotPetya zou onderdeel zijn van de schaduwoorlog tussen Rusland en Oekraïne, het land dat het zwaarst werd getroffen door deze cyberaanval.[11] Digitale aanvallen vormen een belangrijk middel om geopolitieke belangen te beschermen, maar soms zijn ook vooral economische belangen (bedrijfsspionage) in het geding.

Na negen dagen zijn beide containerterminals weer deels operationeel. Hiervoor heeft Maersk in een ongekend tempo de volledige IT-infrastructuur herbouwd, waarbij 4000 servers, 45.000 pc's en 2500 applicaties opnieuw moesten worden geïnstalleerd.[12] De schade

9 Logistiek.nl, 30 juni 2017. Nieuws: APM heeft weer 1 terminal open na cyberaanval. Op 5 november 2018 ontleend aan https://www.logistiek.nl/supply-chain/nieuws/2017/06/apm-heeft-weer-1-terminal-open-101157047.

10 MicrosoftSecure, 16 juni 2017. Analysis of the Shadow Brokers release and mitigation with Windows 10 virtualization-based security. Op 5 november 2018 ontleend aan https://cloudblogs.microsoft.com/microsoftsecure/2017/06/16/analysis-of-the-shadow-brokers-release-and-mitigation-with-windows-10-virtualization-based-security/.

11 Wired.com, 15 februari 2018. Security: The White House blames Russia for NotPetya, the 'most costly cyberattack in history'. Op 5 november 2018 ontleend aan https://www.wired.com/story/white-house-russia-notpetya-attribution/.

12 'Maersk moest complete IT-systeem vernieuwen na cyberaanval', *Het Financieele dagblad*, 27 januari 2018.

lijkt hoofdzakelijk financieel; bij de cyberaanval zouden geen klantgegevens zijn buitgemaakt. Maersk voorzitter Hagemann Snabe heeft naderhand kenbaar gemaakt dat dankzij de overschakeling naar handmatige administratie, de omvang van het vrachtverkeer bij ATM Terminals met slechts 20 procent is gedaald.[13] In het jaarverslag wordt de financiële schade van de cyberaanval alsnog geschat op 250 tot 300 miljoen dollar.

6.3 Een rol voor de overheid?

Het is evident dat bij deze cyberaanval eerst en vooral Maersk (APM Terminals) actie moest ondernemen. Het bedrijf was getroffen door een aanval met gijzelsoftware, vanwege een rechtstreekse link met Oekraine, waar deze problemen waren ontstaan. Omdat Maersk de computer- en informatieveiligheid kennelijk niet voldoende op orde had, moest het bedrijf zelf aan de bak (computers aanpassen en software vervangen) om weer operationeel te kunnen worden. Toch is daarmee niet het hele verhaal verteld. Op verschillende manieren waren ook overheden betrokken en de vraag is of in de toekomst, bij een vergelijkbare casus, de rol van de overheid wellicht zelfs groter zal (moeten) zijn.

Een direct betrokken partij was het Rotterdamse Havenbedrijf. De havenmeester was sedert enkele maanden tevens 'port cyber resilience officer' en heeft zich in die hoedanigheid vanaf de melding van APM Terminals intensief met de casus beziggehouden. Mede naar aanleiding van het incident is bij het Havenbedrijf een officieel meldpunt voor cyberaanvallen ingesteld.[14] Bedrijven in de Rotterdamse haven hebben sinds 11 juni 2018 de verplichting een al dan niet opzettelijke verstoring van hun digitale infrastructuur bij het Havenbedrijf te melden. Doel hiervan is om bij te dragen aan de veiligheid en continuïteit van de haven tijdens en na IT-verstoringen. De gedachte daarbij is dat een tij-

13 TheRegister.co.uk, 25 januari 2018. Security: IT 'heroes' saved Maersk from NotPetya with ten-day reinstallation bliz. Op 5 november 2018 ontleend aan https://www.theregister.co.uk/2018/01/25/after_notpetya_maersk_replaced_everything/.

14 *Beleidsdocument Haven Cyber Meldpunt*. Op 5 november 2018 ontleend aan https://www.portofrotterdam.com/sites/default/files/beleidsdocument_haven_cybermeldpunt.pdf?token=vGqaPtgo.

dige melding het Havenbedrijf in de gelegenheid stelt passende maatregelen te nemen en aan relevante partijen een handelingsperspectief te bieden. Juist deze casus liet immers zien hoe een cyberincident ook doorwerkte in de 'gewone wereld' en er in de Rotterdamse haven bijna een verkeersinfarct ontstond.

Andere relevante overheidspartijen waren het NCSC, de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). In het Cybersecuritybeeld Nederland 2018 van de NCTV wordt uitgebreid ingegaan op deze casus (NCTV, 2018). Daarnaast worden andere kwetsbaarheden van de Nederlandse samenleving beschouwd. In het rapport wordt aan de hand van zes aspecten uiteengezet waarom cybersecurity (steeds meer) een probleem is en wordt:

- Cyberaanvallen zijn snel profijtelijk en kennen een lage pakkans (lastige attributie).
- Er bestaat een laagdrempelige toegankelijkheid van aanvalsmiddelen.
- Veel digitale producten zijn gewoon onveilig (geen updates meer door leveranciers; veiligheid geen economische drijfveer voor producenten).
- Er zijn belangentegenstellingen (bijv. gebruiksgemak versus security).
- De toenemende complexiteit en connectiviteit van systemen zet de weerbaarheid van de digitale infrastructuur onder druk.
- Er is sprake van afhankelijkheid van een beperkt aantal buitenlandse producenten (die mogelijk door autoriteiten van het land waar ze gevestigd zijn, worden aangezet tot spionage).

De Maersk-casus past in een reeks van gebeurtenissen die zich de afgelopen jaren voordeden en gezamenlijk leidden tot een grotere betrokkenheid van de (rijks)overheid. Nederland blijkt een populair doelwit van cyberaanvallen. Op de ranglijst van meest aangevallen landen stond ons land in 2017 op de tweede plaats, achter de VS.[15] Onderstaand geven we een willekeurig overzicht van enkele cyberaanvallen in de afgelopen jaren.[16]

15 Bron: https://www.securitymanagement.nl/nederland-populaire-plek-cybercrime/.

16 Met dank aan Jana Domrose en Vina Wijkhuijs voor het aanleveren van dit overzicht.

Een willekeurig overzicht van cyberaanvallen in Nederland

Op 2 september 2011 bleek dat er in juli van dat jaar een digitale inbraak had plaatsgevonden bij het bedrijf DigiNotar. Dit bedrijf verzorgde beveiligingscertificaten die een veilig en betrouwbaar internetverkeer met (onder andere) overheidsinstellingen dienden te garanderen. Als gevolg van de digitale inbraak waren beveiligingscertificaten uitgegeven die door hackers waren vervalst, hetgeen betekende dat bezoekers van overheidssites niet de garantie hadden op de desbetreffende overheidssite terecht te komen. De kans was groot dat zij naar een malafide website werden doorgeleid.

In augustus 2012 werden verschillende gemeenten en instellingen getroffen door het virus Dorifel, dat op netwerkschijven actief naar Microsoft Officedocumenten zocht, deze onleesbaar maakte en besmette voor verdere verspreiding. Het virus verspreidde zich via systemen die eerder geïnfecteerd waren geraakt met het Citadel/Zeus-virus, dat bekendstaat als een 'banking trojan' en is gemaakt om bank- en inloggegevens te stelen.

Op 5 april 2013 werd ING getroffen door een DDoS-aanval, waardoor het mobiel en internetbankieren bij deze bank en ook betalingen via iDeal bij andere banken enige tijd niet mogelijk was. In diezelfde maand raakte als gevolg van een DDoS-aanval de website van de Nederlandse Spoorwegen voor enige tijd onbereikbaar en was ook DigiD tijdelijk niet of moeilijk te gebruiken. In augustus 2013 werd de openbaar vervoerssite '9292.nl' door een DDoS-aanval geraakt. Rond diezelfde tijd maakte Yahoo bekend slachtoffer te zijn geworden van een cyberaanval, waarbij namen, e-mailadressen, telefoonnummers, geboortedata en onversleutelde beveiligingsvragen van drie miljard Yahoo-accounts waren gestolen.

In augustus 2015 was internetprovider Ziggo doelwit van een DDoS-aanval. Ziggo-gebruikers konden daardoor enkele dagen niet of moeilijk gebruikmaken van internet. In diezelfde maand kreeg ook de website Politie.nl een DDoS-aanval te verduren, waardoor het voor burgers niet mogelijk was om via internet aangifte te doen.

In juni 2016 bleek dat Chinese hackers het computernetwerk waren binnengedrongen van het Nederlands-Duitse bedrijf Rheinmetall Defence. Het bedrijf, gevestigd in Ede, is gespecialiseerd in defensietechnologie en leverde onder andere materialen voor pantservoertuigen.

In september 2017 kwam het CBS met een rapport waaruit bleek dat ruim twintig procent van de bedrijven met minstens tien werknemers in 2016 te maken had gehad met de gevolgen van cyberaanvallen.[17] Aanvallen van buitenaf bleken vooral voor te komen in de financiële

17 Zie: https://www.cbs.nl/nl-nl/nieuws/2017/39/een-op-vijf-bedrijven-slachtoffer-van-cyberaanval.

sector en bij energiebedrijven.[18] Niet-opzettelijke incidenten (zoals uitval van ICT-diensten door storingen in de hard- of software) kwamen echter vaker voor dan aanvallen van buitenaf.

Hoewel dat de ernst van cybercrime lijkt te relativeren, doet zich wel nog een andere ontwikkeling voor. Naast de wereldwijde cyberaanvallen NotPetya en WannaCry (in mei 2017), die onder de noemer *computer focused crime* kunnen worden geschaard, was in 2017 sprake van (mogelijke) Russische beïnvloeding van de Amerikaanse verkiezingen en pogingen tot beïnvloeding van verkiezingen in Frankrijk, Duitsland en het Verenigd Koninkrijk. Deze beïnvloeding en ook de inzet van nepnieuws kunnen als meer traditionele delicten worden beschouwd die met computers worden gepleegd, ook wel *computer assisted crime* geheten (Furnell, 2002; Van Erp et al., 2013). Juist ook deze vorm van cybercriminaliteit beschouwt het NCSC als zorgwekkend.

Eind 2017 kwam minister Ollengren in zeer korte tijd met verschillende brieven over Rusland, nepnieuws en de Nederlandse Tweede Kamerverkiezingen. Zo zond zij op 17 november 2017, naar aanleiding van een vraag van PvdA-fractieleider Asscher om concrete voorbeelden te noemen, een brief aan de Tweede Kamer waarin voorbeelden werden gegeven van Russisch nepnieuws in het kader van MH17 en beïnvloeding van Rusland van de Amerikaanse verkiezingen en pogingen daartoe bij verkiezingen in Frankrijk, het Spaanse referendum over de onafhankelijkheid van Catalonië en de verkiezingen in het Verenigd Koninkrijk.[19] Het is duidelijk dat juist nieuwe informatietechnologie en internet de verspreiding van desinformatie vergemakkelijken en dat dit proces schadelijk is voor de democratische rechtsorde. In het Cybersecuritybeeld Nederland 2017 (NCTV, 2017) wordt aangegeven dat digitale aanvallen en het verspreiden van nepnieuws bewuste pogingen zijn om democratische processen te beïnvloeden en daarmee een duidelijke bedreiging vormen voor de democratie. Op 26 januari 2018 kwam *de Volkskrant* met een uitgebreide analyse over hoe de AIVD de Verenigde Staten ondersteunde en bewijs leverde van Russische inmenging in de Amerikaanse verkiezingen. Een hacker van de AIVD zou zich al in 2014 hebben genesteld in het computernetwerk van een universiteits-

18 In de financiële sector leiden de aanvallen vaak tot uitval van ICT-systemen; energiebedrijven blijven na een aanval vooral met vernietigde of verminkte data zitten.

19 Brief van minister Ollengren d.d. 15 november 2017; TK 2017-2018, 26643, nr. 497.

gebouw naast het Rode Plein in Moskou en langs die weg veel informatie hebben kunnen vergaren. De hackers van de AIVD zouden toegang hebben gehad tot het computernetwerk van de beruchte Russische hackgroep *Cosy Bear* en ooggetuigen zijn geweest van allerlei activiteiten die van daaruit richting Verenigde Staten werden ondernomen. De AIVD heeft dit zelf echter nooit bevestigd.

6.4 Afrondend

Ten tijde van de Koude Oorlog kwam de dreiging uit het Oostblok en bestond de angst dat het Russische leger ons land zou binnenvallen. Cabaretier Wim Kan stelde in zijn beroemde Oudejaarsconferences van 1976 aan het publiek de vraag of zij dachten dat de Russen zouden komen. Waarop hij vervolgde: 'Weet u, ik denk wel dat ze zullen komen, maar een voor een.'[20] Daarmee verwees hij naar de komst van Russische dissidenten, die na – in toen nog communistisch Rusland – te zijn vrijgelaten, naar West-Europa kwamen. Nu, enkele decennia later, is er opnieuw angst voor de Russen, maar hoeft er zelfs geen Rus meer voor naar het Westen te komen.[21] De mogelijkheden om via internet en de moderne informatietechnologie het Westen te ontregelen en eventueel zelfs aan te vallen, zijn legio geworden. De Russen zijn er al![22]

De cyberaanval op Maersk was niet de enige 'cyberaanval' die zich in 2017 voordeed, en juist op onderhavig terrein is de scheidslijn tussen publiek en privaat steeds lastiger te maken. Aanvallen kunnen zowel op publieke als op private actoren zijn gericht en ook al zijn ze slechts gericht op een van beide, de gevolgen zullen al snel aan beide zijden merkbaar zijn. Daarnaast lijkt hier sprake van het gezegde van 'de keten is zo sterk als de zwakste schakel' en de gevolgen van een aanval zullen altijd wel ergens tot problemen leiden. In het voorkomen, voorbereiden

20 Zie voor het fragment: https://www.youtube.com/watch?v=9bvP8neRiW0.

21 Hoewel duidelijk is dat er in Nederland een aantal Russische 'spionnen' actief is (meer eufemistisch informatiemanagers genoemd).

22 Business Insider, 14 mei 2018. Politiek/Tech: De overheid stopt met antivirussoftware van het Russische Kaspersky Lab uit angst voor spionage. Op 5 november 2018 ontleend aan https://www.businessinsider.nl/overheid-stopt-met-antivirussoftware-van-het-russische-kaspersky-lab-vanwege-mogelijke-spionage/.

en reageren op een onverhoopte cyberaanval is daarom gezamenlijkheid geboden. Daarbij spelen uiteraard de hele grote ICT-bedrijven als Google, Facebook, Microsoft en Apple een grote rol. In de brieven aan de Tweede Kamer wordt gesproken over overleg tussen de overheid en deze instellingen over een toekomstige aanpak. Tegelijkertijd spelen deze multinationals vaak een dubbele rol. Zo was de cyberaanval met het WannaCry-virus mede het gevolg van verouderde of ondeugdelijke software van Microsoft en was vervolgens Microsoft ook weer een sleutelactor bij de oplossing. Daarmee, zo wordt in een mooi artikel in *NRC Handelsblad* gesteld,[23] verdienen deze 'luie en vadsige techreuzen' als geen ander aan deze cyberaanvallen, terwijl zij zelf veel te weinig investeren om de systemen veiliger te maken. Hoe onveiliger de software van Microsoft, hoe groter de vraag naar zijn beveiligingsdiensten om tegen cyberaanvallen te beschermen. Terwijl deze bedrijven kijken naar de overheid en hun inlichtingendiensten als zondebok aanwijzen, creëren zij zelf 'een secundaire markt voor cyberwapens'.[24]

23 'Cyberaanvallen: een gouden kans voor techreuzen om hun rijk te vergroten', *NRC Handelsblad*, 19 mei 2017.

24 Idem.