Landen aansprakelijk stellen voor cyberaanvallen nog lastig

JURGEN TIEKSTRA

ONDERZOEK

WWW.RUG.NL/STAFF/E.V.MOYAKINE

Evgeni Moyakine onderzoekt of landen aansprakelijk kunnen worden gesteld voor cyberaanvallen door hackersgroepen. Volgens hem stelt het internationaal recht te hoge eisen aan de bewijslast. Digitale aanvallen zijn in de oorlog in Oekraïne al strijdwapens.

Het was een aantal maanden nadat het Maleisische passagiersvliegtuig MH17 boven het oosten van Oekraïne was neergeschoten, dat Evgeni Moyakine aan de Universiteit van Tilburg promoveerde op een onderwerp in het internationaal recht.

Die tragedie in de zomer van 2014, die 298 mensen het leven kostte, raakte hem diep. Want aan boord van het toestel zat ook Willem Witteveen, hoogleraar op de rechtenfaculteit in Tilburg, met diens vrouw en dochter. ‘Enige tijd voor hij overleed had ik hem nog gesproken’, vertelt de huidige universitair docent IT-recht en Cyberveiligheid. ‘Het was vreselijk, ik kon het niet begrijpen. Ik studeerde internationaal recht en werkte aan mijn promotieonderzoek naar de aansprakelijkheid van staten, dus ik dacht: hoe kunnen we zorgen dat landen zoals Rusland, wanneer dit soort incidenten gebeurt, aansprakelijk gesteld kunnen worden? Dat dit was gebeurd, maakte dat voor mij zelfs persoonlijker.’ En persoonlijk was het al, omdat Moyakine geboren is in, zoals hij het verwoordt, ‘de voormalige Sovjet-Unie’.

‘Onderhandelen met cybercriminelen, moet je dat wel doen?’

Eind 2014 promoveerde hij op een onderzoek naar de internationaalrechtelijke aansprakelijkheid van een land als de Verenigde Staten voor de schendingen van mensenrechten en internationaal humanitair recht door private militaire bedrijven. Berucht voorbeeld is de wetteloosheid in Irak en Afghanistan van het Amerikaanse bedrijf Blackwater.

Cyber Operations

Moyakine richt zich nog steeds op die aansprakelijkheid van landen, maar nu in verband met Cyber Operations (CO's). Oftewel digitale aanvallen door private groepen die niet zelden banden hebben met landsregeringen. Die cyberaanvallen gebeuren overigens niet alleen door landen buiten het Westen. Beroemd voorbeeld is de Stuxnet-computerworm waarmee in 2009 een uraniumverrijkingsfabriek in Iran schade werd toegebracht. Het publieke geheim is dat Israël en de VS betrokken waren,en waarschijnlijk zelfs een Nederlandse AIVD'er. Dit Stuxnet-virus schond het internationaal recht, maar gestraft werd niemand. Het is moeilijk bewijsbaar wie achter zo'n digitale aanval schuilt.

Maar eerst: hoe kwetsbaar is een land als Nederland voor cyberaanvallen? 'Het antwoord kan kort en bondig zijn: héél erg kwetsbaar', reageert Moyakine. 'Nederland is een van de meest gedigitaliseerde economisch ontwikkelde landen ter wereld, met een geavanceerde technische infrastructuur. Ik vertel mijn studenten altijd dat volgens onderzoek elke 40 seconden ergens in de wereld een cyberaanval plaatsvindt: DDoS-aanvallen (Distributed Denial of Service), ransomware en andere soorten malware. Het cybersecuritybedrijf Kaspersky heeft een website waarop je live ziet waar in de wereld ze worden gedetecteerd.'

Ransomware

'Waarschijnlijk is ransomware nu een van de grootste bedreigingen. Daarmee worden verschillende organisaties geraakt: de voetbalbond KNVB onlangs, en ook de NWO (de Nederlandse Organisatie voor Wetenschappelijk Onderzoek, red). Interessant was dat de minister van Onderwijs zei: de overheid onderhandelt niet met cybercriminelen. Dat is een belangrijke ethische vraag die ik aan mijn studenten stel. Moet je dat wel doen? Als private of publieke organisatie verwerk je vaak persoonsgegevens. Daar kunnen ook bijvoorbeeld gezondheidsdata tussen zitten, denk aan ziekenhuizen. Als je het losgeld niet betaalt, kunnen ze op straat komen te liggen.'

'De KNVB heeft naar verluidt één miljoen euro betaald. De Universiteit van Maastricht heeft in 2019 ook betaald: 200.000 euro in bitcoin. Maar uiteindelijk wist de politie dat geld weer terug te krijgen. En doordat de bitcoin in waarde was gestegen, kreeg de universiteit zelfs 300.000 euro extra terug. Ze hebben er dus zelfs geld mee verdiend. Dat hebben ze geïnvesteerd in een fonds voor noodlijdende studenten.'

De beruchtste ransomware is LockBit. Begin mei bleek hiervan verdacht wordt: de Rus Dmitry Khoroshev. Het probleem is: Rusland levert geen ingezetenen uit, en heeft waarschijnlijk zelf geen last van de afpersingen. 'LockBit valt het eigen land niet lastig', legt Moyakine uit. 'Het gaat zelfs zo ver dat je niet wordt aangevallen als Russisch in je taalinstellingen staat. Het instellen van Russisch is dus een van de beschermingsmaatregelen die je kunt treffen maar de vraag is natuurlijk hoe lang deze maatregel effectief blijft.'

FOTO JAN WILLEM VAN VLIET

Evgeni Moyakine werkt sinds 2015 aan de RUG en sinds 2018 als universitair docent IT-recht en cyberveiligheid in het Rölinggebouw in het centrum van Groningen. Ook is hij *research fellow* aan de Universiteit van Milaan. In 2010 kreeg hij een promotiebeurs van de NWO, bedoeld voor talentvolle buitenlandse studenten. Een van zijn favoriete boeken is *De meester en Margarita* uit 1967, van de Russische schrijver Michail Boelgakov.

Fysieke schade

Het gebeurt zelden dat een cyberaanval fysieke schade achterlaat, terwijl in Nederland al jaren de vrees rondgaat dat cruciale infrastructuur als sluizen en bruggen doelwit worden. 'In Nederland hebben zich gelukkig nog geen ontwrichtende digitale aanvallen voorgedaan', bevestigt Moyakine, 'maar in Oekraïne in 2022 wel toen de Russen elektriciteitsnetwerken uitschakelden, waardoor mensen zonder stroom en warmte kwamen te zitten. Stel dat zoiets in de winter gebeurt, dan kunnen mensen doodgaan. Het ging om hackers die vermoedelijk samenwerkten met de Russische overheid.'

'Het is verre van makkelijk om landen aansprakelijk te stellen', vertelt Moyakine. 'Niet alleen omdat het heel moeilijk is voldoende bewijs te verzamelen, maar ook omdat we in het internationale recht theorieën hebben die ontzettend verouderd zijn. Je wilt ten eerste een schuldige kunnen aanwijzen. Dus wie is de persoon die de aanval heeft uitgevoerd? Daarna wil je de banden met staten blootleggen. We hebben het Internationaal Gerechtshof in Den Haag, dat er onder andere voor kan zorgen dat een schadevergoeding moet worden uitbetaald. Maar ook wordt het dan mogelijk dat aangevallen staten zich kunnen verdedigen en tegenmaatregelen nemen.'

Staatscontrole

Moyakine vindt de bewijsdrempel nu nog te hoog. 'Stel dat een private entiteit of persoon wordt aangestuurd door een staat. Om die aansprakelijk te kunnen stellen, zegt het Internationaal Gerechtshof dat die aansturing 'effectief' moet zijn. Dat betekent dat de staat in elk stadium van een cyberoperatie voldoende controle uitoefende en ervoor kon zorgen dat de operatie stopte of doorging. Aan de andere kant heeft het Joegoslavië Tribunaal gezegd dat de controle ook '*overall*' kan zijn. Dat betekent dat een staat een bepaalde rol heeft bij onder andere het opzetten van de operatie, het financieren, het trainen van de mensen, en het verstrekken van virussen.'

'Dat is al een veel lagere drempel voor het constateren van staatscontrole. Maar gezien de ontwikkelingen die plaatsvinden, vind ik dat er nog een controletest moet worden ontwikkeld. Te denken valt aan het concept 'working in tandem' bedacht door de jurist Collin Allan. Dat betekent dat als een staat en een groep hackers samenwerken en cyberoperaties tegelijk met andere operaties worden uitgevoerd, je al kunt zeggen dat de aansprakelijkheid van de staat niet uitgesloten is. Wij als juristen kunnen bijdragen aan deze discussie. Wellicht dat overheidsjuristen onze stukken lezen en denken: ja, misschien is er wel wat te zeggen voor deze theorie.'