Ransom War

How Cyber Crime Became a Threat to National Security
Door Max Smeets
New York (Oxford University Press) 2025
256 blz.
ISBN 9781911723912
€ 29,-

Een langlopende discussie in het cyberdomain is of cyberspace-operaties een strategisch effect kunnen hebben. Menig wetenschapper geeft aan dat effecten in cyberspace niet het niveau van een fysieke aanval of dreiging kunnen halen, laat staan een nucleaire – zij spreken van de 'myth of cyberwar'.[1] Aan de andere kant geven onderzoekers aan dat acties in cyberspace een militaire actor kunnen tegenwerken (*counterforce*) maar ook een strategisch effect kunnen hebben door het waarden- en normenstelsel van een maatschappij te ondermijnen (*countervalue*).[2] Max Smeets hoort bij de laatste categorie en zijn meest recente boek *Ransom War* laat zien dat *ransomware*-operaties in cyberspace wel degelijk de vitale belangen van een staat kunnen raken.

Even een stapje terug. In de afgelopen 20 jaar ging de discussie over het strategische effect van operaties via cyberspace vooral over de vraag of er een cyberoorlog plaats kon vinden,[3] of dat met cybermiddelen een opponent afgeschrikt kon worden (*deterrence*).[4] De meest voorkomende (kwaadwillende) activiteiten in cyberspace waren echter aanvallen die een website platleggen (DDoS), die de startpagina van een website verandert (*defacement*), of acties die data 'gijzelen' (ransomware). Dit waren veelal niet meer dan hinderlijke acties. In de laatste jaren is, met name, ransomware in hoge mate geprofessionaliseerd. Dit heeft te maken met de ontwikkeling van software en de afhankelijkheid van het internet, maar ook met de mogelijkheid om (anoniem) via bitcoins betaald te krijgen. Tot slot is er ook de mogelijkheid ransomware te koppelen aan andere technieken, zoals het lekken van de gegijzelde data of het wissen van de data (wiperware),[5] wat Smeets *double* of zelfs *triple extortion* noemt.

Een ransomware-operatie is dus een schadelijke cyberaanval waarbij hackers de controle over vitale bestanden en systemen krijgen en vervolgens losgeld eisen van de eigenaar ervan. Een thema dat actueler is dan op het eerste gezicht lijkt. In de Russisch-Oekraïense oorlog heeft Oekraïne besloten alle overheidsdata over te hevelen van lokale computers naar de cloud, zoals Microsoft Azure. Microsoft biedt dit soort diensten aan in de vorm van SaaS (*Software as a Service*). Naast de oorlog in Oekraïne heeft de zogeheten Contigroep – een berucht ransomwarehackerscollectief – in 2022 de overheidsdata van Costa Rica gegijzeld, waarna dat land Conti de oorlog verklaarde. Het zijn voorbeelden als deze waarmee Smeets aangeeft dat ransomware niet langer een 'hinderlijke digitale actie' is, maar te zien is als een operatie die de vitale belangen van een staat raakt, ofwel ransom war.

Ransom War illustreert dat operaties in cyberspace fundamenteel anders zijn dan in het fysieke domein. Ten eerste vinden acties plaats die in het fysieke domein onbestaanbaar zijn (gijzelen van data) en ten tweede geeft het aan dat niet-statelijke actoren strategische effecten genereren. Naast deze aspecten is de meerwaarde van Smeets' boek dat hij een theoretisch raamwerk creëert om de ransom war acties te duiden en te analyseren. Smeets gebruikt hierbij de opkomst en ondergang van de Contigroep als illustratie, gebruikmakend van data die door de Oekraïner Danylo zijn gelekt via @ContiLeaks. Interessant is dat Smeets Conti niet als een groep

1 Erik Gartzke, 'The Myth of Cyberwar. Bringing War in Cyberspace Back down to Earth' (2013) 38 *International Security* 41.
2 Richard Harknett en Max Smeets, 'Cyber Campaigns and Strategic Outcomes' (2020) 45 *Journal of Strategic Studies* 4.
3 Thomas Rid, 'Cyber War Will Not Take Place' (2012) 35 *Journal of Strategic Studies* 5 versus John Stone, 'Cyber War Will Take Place!' (2013) 36 *Journal of Strategic Studies* 101.
4 Michael Fischerkeller en Richard Harknett, 'Deterrence Is Not a Credible Strategy for Cyberspace' (2017) 61 *Orbis* 381.
5 Kraesten Arnold en Sander van Dorst, 'Wiperware. Een nieuw cyberwapen voor de militaire toolbox?' *Militaire Spectator* 192 (2023) (11) 512.

pizza-etende hackers benadert, maar door de lens van een professioneel bedrijf met alle voor- en nadelen van dien – zoals gebrekkige solvabiliteit en managementskills.

Smeets geeft aan dat de karakteristieken van niet-statelijke ransom war-actoren anders zijn dan het handelen van statelijke actoren in cyberspace – veelal *cyber commands* en inlichtingendiensten. Hoewel de technieken om toegang te krijgen (*access*) en die positie uit te buiten (*exploit*) soortgelijk zijn, selecteren ransom wargroepen andere *targets*. Zij richten zich op doelwitten waar een groot maatschappelijk belang aan zit zoals ziekenhuizen, of socialeverzekeringsbanken. Data die daarbij verkregen wordt mag niet op straat komen te liggen, waardoor de neiging om losgeld te betalen groot is. De grootste uitdaging voor ransom wargroepen is dat zij kampen met de *ransomware trust paradox* – ze moeten betrouwbaar overkomen op degene van wie ze de data hebben gegijzeld, zo niet dan lopen ze het losgeld mis.

Smeets analyseert ransom wargroepen – primair de Contigroep – aan de hand van het MOB-model. De M staat voor de modus operandi van de groep, die veel uitgebreider is dan de werkwijze van 'reguliere' hackers (statelijk of crimineel) omdat er naast de reconnaissance, access en exploits ook nog aspecten als onderhandelen met de gegijzelde, customer services en financiële dienstverlening bijkomen. De O gaat over de organisatiegraad van de groep, die eerder overeenkomt met een bedrijf dan met een hackerscollectief, denk aan een investeringsplan en diversificatie van taken. De B staat voor de *branding* ofwel: hoe zet je jezelf in de markt? Ransom wargroepen als Conti bieden geen SaaS, maar een RaaS (Ransomware as a Service) aan, ze hebben een eigen website met zelfs een soort 'klanttevredenheidsrubriek' – een verklaring van het slachtoffer dat de data na betaling weer beschikbaar kwam.

De meerwaarde van het MOB-model is dat dit tevens de sleutel biedt hoe tegen deze ransomware groepen op te treden, namelijk door ze als bedrijf te zien. De perceptie moet zijn het verstoren van de markt; financiële forensische opsporing in plaats van het oppakken van criminelen; pro-actief delen van compromitterende kennis over deze groepen in plaats van dit zien als 'geheime staatsinlichtingen'; en vooral het ondermijnen van de reputatie van de ransomwaregroepen.

Geruststellend is wellicht dat de hoogte van het losgeld gekoppeld is aan de BigMac index van *The Economist*. Dus 'there is honour among thieves' en zelfs Conti had een soort van ethisch protocol, wat niet voor iedere beroepsgroep te zeggen is. ■

Bgen prof. dr. B.J.M. Pijpers, NLDA

Schrijft u een gastcolumn in de *Militaire Spectator*?

De redactie van de *Militaire Spectator* biedt lezers de mogelijkheid een gastcolumn te schrijven van maximaal duizend woorden. Het thema is vrij, maar moet passen in de formule van het tijdschrift. Een gastcolumn bevat een relevante boodschap voor de lezers, een gefundeerde eigen mening en juiste en verifieerbare feiten in een logisch opgebouwd betoog.
U kunt uw gastcolumn sturen naar de bureauredactie (zie colofon) of aanbieden via de website. De redactie wacht uw bijdrage met belangstelling af.

De hoofdredacteur