ARTIKEL

Cyberterrorisme: veel woorden, maar weinig daden

André Hoogstrate en Sergei Boeke

Het fenomeen cyberterrorisme spreekt tot de verbeelding, maar lijkt vaker te worden beschreven door onderzoekers en journalisten dan door terroristische groeperingen te worden uitgevoerd.[1] Dit ondanks waarschuwingen van politici en beleidsmakers.

Zo waarschuwde de Amerikaanse Minister van Defensie Panetta in 2012 dat terroristische groepen computeraanvallen kunnen gebruiken om treinen te laten ontsporen, de watervoorziening te verstoren of de elektriciteitsvoorziening af te sluiten.

Er zijn duidelijke parallellen met het debat over cyberoorlog, dat eveneens plaats lijkt te vinden tussen de polen van *doomsday* en *dismissal*.[2] Voor het fenomeen cyberoorlog heeft het artikel uit 2012 van Thomas Rid, 'Cyber war will not take place', definities tegen het licht gehouden en een meer conceptuele vorm aan het debat gegeven.[3] De definitie die Rid van oorlog hanteert, is een zeer Clausewitziaanse (en dus geworteld in de negentiende eeuw), maar hij heeft wel *malicious* statelijke cyber-activiteiten nuttig onderverdeeld in spionage, sabotage en subversie.

Dit heeft tegenwicht geboden tegen de alarmisten die waarschuwen dat een *electronic Pearl Harbor* ons zal overkomen, waarbij dit voorbeeld vooral is gerelateerd aan staten en oorlog. De veel gebruikte metafoor en waarschuwing van een mogelijke 'digital *nine-eleven*' is daarentegen meer van toepassing op het debat over cyberterrorisme, en de vraag is ook hier hoe het debat beter conceptueel vorm kan krijgen.

De definitie van terrorisme (nog zonder het 'cyber' element) is gedurende enkele decennia onderwerp van verhit academisch en internationaal debat. Er is en zal geen consensus ontstaan over de exacte formulering, maar uiteindelijk is een duidelijk begrip van wat onder de noemer van terrorisme valt van groot belang, omdat het ook tot op zekere hoogte het beleidsantwoord van verschillende regeringen hierop bepaalt. Weinberg et al. hebben onderzocht welke kernelementen volgens academici in de definitie moeten terugkomen, en via een benadering van de laagste gemene deler leidt dit tot de volgende definitie:

> *"Terrorism is a politically motivated tactic involving the threat or use of force or violence in which the pursuit of publicity plays a significant role."*[4]

Net zoals het concept terrorisme lastig af te bakenen is, blijkt het voorzetsel 'cyber' eveneens verschillende betekenissen voor verschillende mensen te hebben. Dit leidt tot verschillende definities van 'cybersecurity', 'cyberspace' en 'cyberwar', waarbij men het zelfs ook nog niet eens is over de schrijfstijl (aan elkaar, met streepje of los). Wel is duidelijk dat het woord 'cyber' zowel binnen organisaties als bij de media neigt naar een hype, met alle gevolgen van dien voor percepties, begrippen en budgetten.

De combinatie van cyber met terrorisme is er derhalve één die verder onderzoek verdient. Dit artikel geeft een korte analyse van 'cyberterrorisme' op basis van de laatste ontwikkelingen. Eerst zal een literatuuranalyse een overzicht geven van het academisch onderzoek en kort de definitiekwestie behandelen. Vervolgens wordt gekeken naar intenties en capaciteiten van terroristische groeperingen om 'acts of cyberterrorism' te ondernemen.

Definities en literatuur

Het academisch debat met betrekking tot cyberterrorisme kent eveneens zijn alarmisten en sceptici.

Alarmisten

Barry Collin, die verantwoordelijk is voor de term in de jaren '80 van de vorige eeuw, bevindt zich duidelijk in het kamp van de alarmisten, en zette al in 1997 de toon. Veel andere auteurs volgen in zijn voetstappen; de redenering dat cyberterrorisme een grote dreiging vormt, is niet alleen gebaseerd op de intenties van terroristische organisaties, maar vooral op de kwetsbaarheden van westerse samenlevingen. Inmiddels is een groot gedeelte van de maatschappij volledig afhankelijk van de kritische (informatie) infrastructuur geworden, en als deze op een of andere manier ontregeld wordt, is de vrees dat er onvoorziene cascades optreden.

'Eenvoudige middelen kunnen op zichzelf zeer effectief zijn bij terroristische aanslagen'.

Een aansprekend voorbeeld vond plaats in december 2015, toen in West Oekraïne drie energiemaatschappijen gehacked werden en – weliswaar voor een korte tijd – bijna een kwart miljoen mensen als gevolg hiervan zonder stroom kwamen te zitten. Een handmatige back-up functie – standaard in veel oudere (Sovjet) centrales, maar niet altijd in (westerse) nieuwe – heeft ervoor gezorgd dat de crisis relatief snel opgelost kon worden.[5]

Sceptici

Aan de meer sceptische kant van het debat staan auteurs als Nissenbaum, die de 'Copenhagen securitization theorie' gebruikt om te illustreren hoe een bepaalde dreiging 'opgeklopt' wordt om tot een politieke prioriteit te worden verheven.[6] Maura Conway illustreert hoe cyberterrorisme een veiligheidskwestie *par excellence* is, omdat (de dreiging van) terrorisme, dat vaak 'dehumanized' wordt, perfect past bij het gevoel dat men door technologie grip verliest op de wereld.[7] De combinatie van beide leent zich dus uitstekend voor alarmistisch denken, waarbij scenario's als een *digital nine-eleven* de boventoon gaan voeren.

Definities

Terwijl terroristische organisaties het internet op veel manieren benutten (voor rekrutering, propaganda, financiering en voorbereiding van aanslagen), neigen veel onderzoekers naar een minder brede definitie van cyberterrorisme. In een door de Universiteit van Swansea uitgevoerde enquête hebben de respondenten vier belangrijke elementen voor een definitie aangedragen, en wel: (1) het politiek motief; (2) een digitaal middel of doel; (3) angst als beoogd effect; en (4) fysieke gevolgen voor de kritische infrastructuur.[8]

In een verklaring voor de Armed Services Committee van het Amerikaanse Congres in 2000 heeft professor Dorothy Denning de volgende, overzichtelijke definitie van cyberterrorisme gegeven:

> *"Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber terrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not."*[9]

Deze definitie is vooral gericht op het motief en het resultaat, terwijl ook andere criteria in de overweging kunnen worden meegenomen. Net zo min als er consensus over een definitie bestaat, zijn wetenschappers het eens of er zich al een geval van cyberterrorisme heeft voorgedaan.

© Flickr / Ibai

Protesten van Anonymous in Spanje, 2011.

De definitie van cyberterrorisme is belangrijk om het te kunnen onderscheiden van ‘cybercrime’, ‘hactivism’ en ‘cyberwar’ of conflict. Vaak immers zijn de technieken die worden gehanteerd bij het hacken van een netwerk of systeem hetzelfde, maar verschillen de dader en het motief. Hactivism – de combinatie van activism en hacken – kan door het politiek motief en de niet-statelijke dader dicht tegen cyberterrorisme aan liggen. De meeste bekende acties van hactivists betreffen tot nu toe Distributed Denial of Service (DDoS)-aanvallen en ‘doxing’, waarbij zij toegang krijgen tot privégegevens van personen of organisaties en deze op het internet zetten om hen in discrediet te brengen.

> Een belangrijk aspect van terroristische aanvallen is het genereren van een psychologisch en dramatisch effect; dit lijkt echter lastig te bereiken met cyberaanvallen

Een voorbeeld is de groep Anonymous, die tot op heden zijn aandacht heeft gericht op onder meer de Scientology kerk, grote multinationals en ook de Islamitische Staat/Daesh. Ook is het mogelijk dat terroristische organisaties activiteiten uitbesteden aan cybercrime-groeperingen, zoals sommige staten ook doen voor spionage, subversie en sabotage. Voor staten is dit een manier om de herleidbaarheid van malfide activiteiten te frusteren, maar voor terroristen zou het een manier kunnen zijn om over hoogwaardige aanvalstechnieken te beschikken, die ze zelf niet in huis hebben. Ook hier vervagen de grenzen tussen het optreden van statelijke en niet-statelijke actoren.

Een toekomstige dreiging?

Dat academici het niet eens zijn over de definitie van cyberterrorisme en de kans hierop, wil niet zeggen dat het niet plaats zal vinden. Kijkend naar de intentie, het vermogen en de gelegenheid voor terrorisme, kan een meer gestructeerde inschatting worden gemaakt of de dreiging reëel is. Zoals al eerder aangegeven is het genereren van een psychologisch en dramatisch effect vaak een belangrijk aspect van terroristische aanvallen. De huidige consensus binnen de academische wereld is dat dit aspect lastig te bereiken is met cyberaanvallen.

De relatief eenvoudige DDoS-aanvallen liggen per definitie binnen het technische bereik van terroristische groeperingen, maar ze sorteren uiteindelijk weinig schrikeffect. Dat een specifieke dienst of website een bepaalde tijd niet bereikbaar is, zal weinig 'terreur' veroorzaken. Wil een cyberaanval een geslaagde terreuractie zijn, dan zullen er aanzienlijke aantallen slachtoffers moeten vallen of een aanzienlijke schade moeten ontstaan. Dit impliceert het treffen van transport of kritische infrastructuur. In de meeste gevallen is het nog steeds gemakkelijker om fysiek iets te verstoren dan een ingewikkelde code te schrijven die hetzelfde effect heeft.

Een antwoord op de vraag naar de mogelijke keuze voor de inzet van het 'cyberwapen' kan ook worden gegeven met behulp van een kosten-baten-analyse: het moet lonen dit te verkiezen boven een aanslag met meer traditionele en beschikbare middelen. Maar eenvoudige middelen kunnen op zichzelf zeer effectief zijn bij terroristische aanslagen. Zo is 9/11 (2001) met vlieglessen en stanleymessen uitgevoerd, de Boston bombings (2013) met pressure-cookers, de aanslag op Charlie-Hebdo in Parijs (2015) met Kalashnikovs en de aanslag in Nice (2016) met een vrachtwagen.

Technische kennis

Twee onderzoekers, Al-Garni en Chen, hebben getracht te analyseren hoeveel de Stuxnet-cyberaanval – uiteindelijk door Ralph Langer beschreven als een *weapon of mass destruction* – de (statelijke) daders heeft gekost qua tijd en geld. Het antwoord is een aanzienlijke spionage-inspanning om de netwerken, software en hardware van het Iraanse kernprogramma te verkennen, en vervolgens gericht te saboteren. Hiervoor was een team hackers van wereldklasse-niveau nodig, en de cyberaanval is uiteindelijk proefgedraaid op een cascade van centrifuges in de Verenigde Staten. Kortom, de auteurs concluderen dat een niet-statelijke actor grote moeite zou hebben om dit op te brengen.[10] Een kritische noot bij hun analyse is wel dat de Amerikaans-Israëlische operatie bedoeld was om bijzonder subtiel en geleidelijk sabotage te plegen, en dat zij juist daardoor technisch zo ingewikkeld was.

Organisatorische capaciteit

Naast de technische kennis die benodigd is voor cyberterrorisme, zijn ook andere elementen, zoals organisatorische capaciteiten, van belang. Dit was ook de conclusie van het rapport *Cyberterror: Prospects and Implications* (School, 1999). Daarin wordt de waarschijnlijkheid onderzocht dat terroristische groeperingen cyberterrorisme als wapen zouden kiezen. De conclusie luidde toen – weliswaar ruim 15 jaar geleden – dat een aanval die enig effect zou sorteren veel inspanning kost. Het werd waarschijnlijker geacht dat cyberaanvallen meer als aanvullend middel zouden worden gebruikt, en niet in eerste instantie gericht zouden zijn op geweld of fysieke gevolgen.

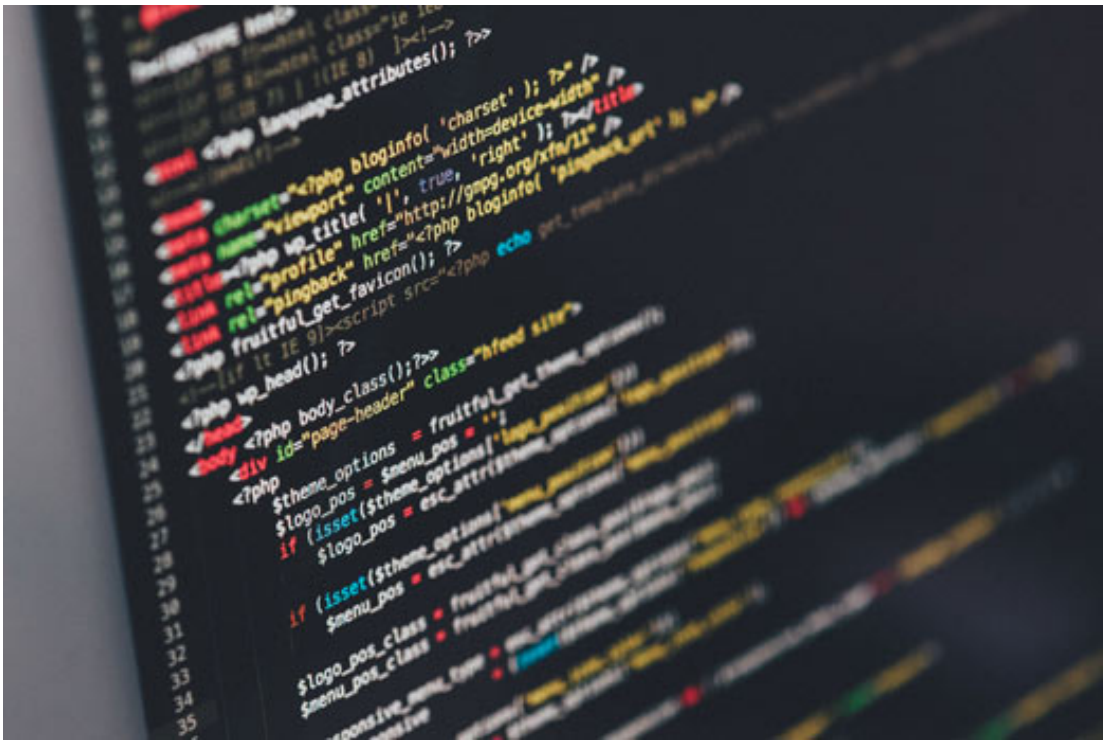
Het rapport onderscheidde voorts de verschillende technische niveaus die een groep zou moeten doorlopen om zelfstandig geavanceerde cyberaanvallen te kunnen uitvoeren, en schatte dat daarvoor 6 tot 10 jaar nodig was. Zo is de Islamitische Staat/Daesh inmiddels hard op weg, maar worden hun stappen op allerlei fronten bemoeilijkt danwel vertraagd door de internationalen coalitie.

Eenvoudige middelen kunnen zeer effectief zijn bij terroristische aanslagen

Overigens kan een groep ook het werk outsourcen of beschikbare software gebruiken. Zo is in de Syrische burgeroorlog de malware Blackshades aangetroffen bij groepen die tegen Assad vechten. Blackshades is ontwikkeld door cybercriminelen en stelt de gebruiker in staat anderen te hacken en te bespioneren. Dit toont aan hoe een platform ontwikkeld door cybercriminelen ook benut kan worden door niet-statelijke actoren in een conflict.

Het ontwikkelen van kleine aanvallen is beduidend goedkoper geworden, en hiervoor zijn *open source tools* beschikbaar. Veel van de *tools* zijn echter ontwikkeld voor demonstratie- en testdoeleinden. Dit betekent dat men nog veel werk moet verzetten en kennis moet vergaren om deze *tools* tot een echt effectief wapen om te vormen. Vaak beperken de *tools* zich tot één type kwetsbaarheid in de software, terwijl een effectieve aanval met fysieke gevolgen meestal een combinatie van meerdere zwakheden tegelijkertijd vereist. Tevens zijn er, omdat de *tools* 'open source' zijn en er een bloeiende cybersecurity-industrie bestaat, veel beschermende en mitigerende maatregelen mogelijk.

Thans lijken de meeste groepen die indicaties hebben afgegeven cyberterrorisme als wapen te willen gebruiken, bijvoorbeeld de United Cyber Caliphate, nog steeds geen geavanceerd technisch niveau te hebben bereikt. Terwijl zij qua cybercapaciteit wel al beduidend verder zijn dan een aantal jaren terug, staat daar tegenover dat veel organisaties hun cybersecurity-protocollen (zowel technisch als organisatorisch) hebben verbeterd.



© Pixabay

'Naast criminelen, hactivists en staten, zijn ook terroristische organisaties op zoek naar kwetsbaarheden in soft- en hardware om deze uit te buiten.'

Dit geldt natuurlijk vooral voor de grote veiligheidsdiensten en multinationals, waarbij de kritische infrastructuur in het Westen ook grote sprongen heeft gemaakt wat de verdediging tegen cyberaanvallen betreft. Voor kleine bedrijven, en publieke of private organisaties die minder financieel vermogend zijn, geldt dit natuurlijk in veel mindere mate. Zo werden in de week na de aanslag op Charlie Hebdo (januari 2015), bijna twintigduizend Franse websites, voornamelijk van het Midden- en Kleinbedrijf, bestookt door DDoS-aanvallen, die werden opgeëist door het hackers-collectief 'Middle East Cyber Army'.[11]

Conclusie

De term cyberterrorisme is veelvuldig onderwerp van debat, terwijl maar weinig terreurorganisaties cyberterrorisme in de praktijk hebben kunnen brengen. Dit kan meerdere oorzaken hebben. De vereiste technische kennis is afwezig, de doelwitten zijn te 'cyber secure' of inlichtingendiensten – die zeer actief zijn in cyberspace – hebben veel aanslagen verijdeld. Het belangrijkste is misschien wel dat terroristische organisaties juist met makkelijk te verkrijgen middelen, van vuurwapens tot pressure-cookers, effectief aanslagen (hebben) kunnen plegen. Voor veel doelwitten – van de energiecentrale tot het treinstation – is het nog steeds makkelijker om met fysieke middelen – messen, vuurwapens of bommen – schade aan te richten dan een geslaagde cyberaanval uit te voeren.

Daarnaast is angst zaaien een belangrijk aspect van terrorisme, en dit wordt veroorzaakt door ingrijpende beelden van slachtoffers en schade die door de media worden verspreid. Een online-platform of dienst dat enkele uren niet beschikbaar is door een DDoS-aanval, zaait daarentegen weinig terreur.

Toch zal de discussie over cyberterrorisme waarschijnlijk niet in het hypothetische blijven. Zo is een hacker er waarschijnlijk al in geslaagd om via het *onboard entertainment system* van een vliegtuig bij het besturingssysteem te komen. Kortom, naast criminelen, hactivists en staten, zijn ook terroristische organisaties op zoek naar kwetsbaarheden in soft- en hardware om deze uit te buiten. Het zal niet gelijk een digital 9/11 worden, maar dat terroristen op termijn cyber ook effectief als wapen gaan hanteren, lijkt waarschijnlijk.

Noten

[1]
Een langere versie van dit artikel verschijnt in het *Handboek Terrorisme* (ed. Muller, Bakker, De Wijk & Rosenthal, 2017).

[2]
I. Duyvesteyn, 'Between doomsday and dismissal; Collective defence, cyber war and the parameters of war', *Atlantisch Perspectief,* 2014, pp. 20-24.

[3]
T. Rid, 'Cyber war will not take place', *Journal of Strategic Studies,* 2012, 35(1), pp. 5-32.

[4] L. Weinberg, A. Pedahzur & S. Hirsch-Hoefler, 'The challenges of conceptualizing terrorism', *Terrorism and Political Violence,* 2004, 16(4), pp.777-794.

[5]
K. Zetter, 'Inside the cunning, unprecedented hack of Ukraine's power grid', *WIRED,* 2016.

[6]
L. Hansen & H. Nissenbaum, 'Digital disaster, cyber security, and the Copenhagen school', *International Studies Quarterly,* 2009, 53(4), pp.1155-1175.

[7]
M. Conway, *The media and cyberterrorism: a study in the construction of 'reality'*, 2005.

[8]
L. Jarvis & S. Macdonald, 'What is cyberterrorism? Findings from a survey of researchers', *Terrorism and Political Violence,* 2015, 27(4), pp. 657-678.

[9]
D.E. Denning, *Cyberterrorism*, 2000.

[10]

T. Al-Garni & T.M. Chen, 'An updated cost-benefit view of cyberterrorism', in: *Terrorism Online*, edited by L. Jervis, S. MacDonald & T.M. Chen, Routledge, 2015.

[11]
G. Russell, 'La France face à une vague sans précédent de cyberattaques', *Le Figaro*, 15 januari 2015.

Auteurs

André Hoogstrate
Als universitair hoofddocent verbonden aan de Nederlandse Defensie Academie (NLDA) ▸
(http://leidensafetyandsecurityblog.nl/contributors/andre-hoogstrate)

Sergei Boeke
Als onderzoeker / docent verbonden aan het Institute of Security and Global Affairs (ISGA) van de Universiteit Leiden. ▸
(https://www.universiteitleiden.nl/medewerkers/sergei-boeke)