Cyberspace coercion door IS

Met de komst van het Defensie Cyber Commando in 2014 betrad de Nederlandse krijgsmacht het digitale domein, assertief, maar ook met als doel bij te dragen aan de bescherming van vitale belangen tegen virtuele dreigingen. Want waar de mogelijkheden van dit digitale domein ongelimiteerd zijn, geldt dit ook voor de bedreigingen. Een nieuw domein vraagt om nieuwe oplossingen. Een krijgsmacht zoekt de oplossingen vaak in het verleden. Ook in militaire opleidingen worden beproefde strategieën, zoals coercion, toegepast op nieuwe opponenten. Dat er van het verleden kan worden geleerd is goed, maar niet alles wat is geleerd kan toegepast worden op de toekomst, zeker niet in het digitale domein. Snel innoveren is essentieel om deelname aan het toekomstige gevecht mogelijk maken. Het blijkt dat de toepassing van cyber coercion en cyberstrategie voor staten minder gemakkelijk is dan voor een niet-statelijke actor als Islamitische Staat.

*M.W. Passchier BA – tweede-luitenant**

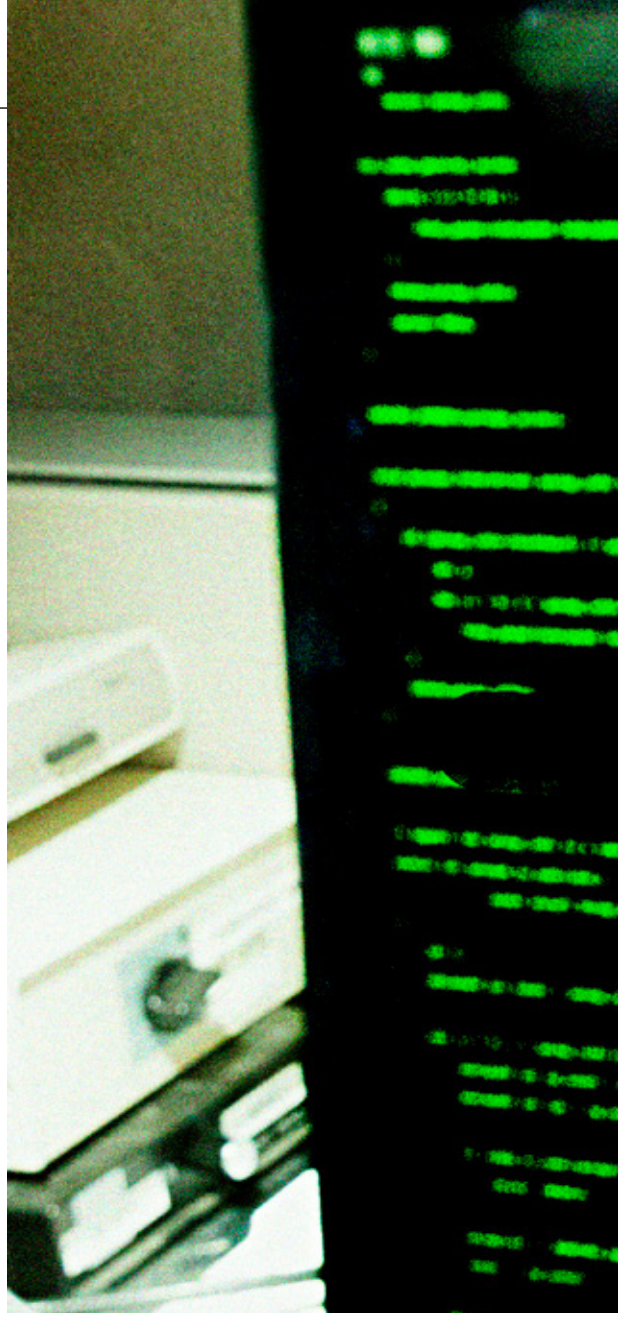


FOTO US AIR FORCE, GRIFFIN SWARTZELL

Binnen de studierichting Krijgswetenschappen aan de Faculteit Militaire Wetenschappen van de Nederlandse Defensie Academie volgen cadetten de minor 'Info at War' over de ongrijpbare omvang van het informatiedomein. Dit is niet een eerste kennismaking, want cadetten zijn anno 2020 van een generatie waar de grenzen tussen online en offline nagenoeg afwezig zijn. Deze grens blijft vervagen, elke generatie steeds iets meer. Grootouders leren whatsappen, ouders hebben sinds kort Instagram of Facebook en jongere broertjes of zusjes zitten op de nieuwste socialemedia-applicaties waar generaties boven hen niets van snappen. De samenleving wordt steeds afhankelijker van het digitale domein en met een tempo dat amper bij te houden is. Hoe sneller een actor, ongeacht zijn intentie, weet te manoeuvreren binnen dit digitale domein, hoe meer hij mee krijgt wat er allemaal speelt, wat van belang is en wat er kan in dit domein. Snel innoveren is essentieel om deelname aan het toekomstige gevecht mogelijk te maken. Staten zijn echter actoren die allesbehalve snel kunnen handelen, zeker in vergelijking met niet-statelijke actoren (NSA's). Een kleinere organisatiestructuur, andere rationaliteit en verschil in *checks and balances* laten *insurgents*, guerrilla's en terroristen niet per se beter, maar wel gemakkelijker en sneller innoveren dan staten. Toen de Nederlandse krijgsmacht op 25 september 2014 het Defensie Cyber Commando[1] oprichtte had al-Qaida al

Strategieën die vroeger werkten worden in een nieuw, digitaal jasje gehesen, maar het is nog niet zo eenvoudig om ze dan ook toe te passen als cyberstrategie

ruim 14 jaar eigen websites,[2] was de cyber-jihad al een decennium lang een van de principes van jihad en had het Twitteraccount van het Cyber Caliphate, eigendom van Islamitische Staat (IS), bijna 110.000 volgers.[3]

Cyberstrategieën worden gevormd om digitale dreiging tegen te gaan. Strategieën die vroeger werkten worden in een nieuw, digitaal jasje gehesen om vervolgens toe te kunnen passen als cyberstrategie. Dit klinkt vrij simpel, maar is in de praktijk nog niet zo eenvoudig, blijkt uit de onderzoeksresultaten van Nance en Sampson naar de theorie van cyberspace coercion (cyber coercion).[4] Het lukt staten nog niet coercion succesvol toe te passen binnen het digitale

* Tweede-luitenant Mark Passchier volgt de Vaktechnische Opleiding Infanterie. Dit artikel is een bewerking van zijn gelijknamige bachelorscriptie aan de Nederlandse Defensie Academie.

1 Hans Folmer, 'Het Defensie Cyber Commando, een nieuwe operationele capaciteit', in: *Nationale veiligheid en crisisbeheersing*, No. 5 (2014) 36-37.

2 Abdel Bari Atwan, *Islamic State. The Digital Caliphate* (Oakland, University of California Press, 2015) 16-17.

3 Ibid, 27.

4 Malcom Nance en Chris Sampson, *Hacking ISIS. How to Destroy the Cyber Jihad* (New York, Skyhorse Publishing, 2017).

domein, maar zoals aangegeven zijn NSA's belangrijke innoverende actoren voor deze cybertheorie. Dit artikel komt voort uit het gelijknamige bacheloreindwerkstuk waarin onderzoek is gedaan naar cyber coercion en de cyberstrategie van IS om overeenkomsten en verschillen te onderkennen met cyber coercion door staten. Eerst wordt er ingegaan op de cyberspace coercion-theorie en vervolgens worden de activiteiten van IS in het virtuele domein behandeld. Tot slot worden verbanden gelegd tussen de strategie van IS en de toepassing van coercion in het digitale domein. De centrale vraag hierbij is: in hoeverre kan de cyber coercion-theorie toegepast worden op het online-beleid van het virtuele kalifaat van IS?

Cyberspace coercion door staten

Coercion is het concept waarbij een actor een andere actor probeert te dwingen tot onvrijwillige gedragingen of beslissingen. De reikwijdte en de omvang van het concept coercion zijn onderwerp van een permanent academisch discours.[5] Bryman en Waxman beschrijven coercion bijvoorbeeld niet als iets destructiefs, maar als gelimiteerd geweld dat gebruikt kan worden om dreigen met meer geweld geloofwaardiger te doen lijken.[6] Dit is in strijd met de zienswijze van Thomas Schelling, een specialist op het gebied van nucleaire strategie die juist aangeeft dat bruut geweld iets anders is dan coercion. Kracht om schade toe te brengen zal ingehouden moeten worden om zo de dreiging van het toebrengen van schade (of meer schade) effect te laten hebben op beslissingen van actoren.[7] Hoe geweld wel of niet toegepast moet worden blijft een discussiepunt binnen de coercion-theorie. Wel is zeker dat de rationaliteit van een actor invloed heeft op het succes van afschrikking en dat staten de actoren zijn die coercion succesvol kunnen gebruiken als strategisch middel.[8]

De rationaliteit van actoren binnen de coercion-theorie heeft invloed op de vier externe kernprincipes van coercion. Klassieke coercion wordt normaliter door statelijke actoren toegepast op andere staten, binnen rationele kaders. De vraag is echter of NSA's en terroristische organisaties (met Arabische/Oosterse origine) eenzelfde rationaliteit aanhangen als een (Westerse) staat. Hiermee wordt niet gesteld dat staten rationeel zijn – rationaliteit hang immers van veel factoren af – maar NSA's zijn geen soevereine staten die zich om het behoud van deze status aan internationale wetten en regels hoeven te houden. Het ontbreken van soevereiniteit geeft dit soort NSA's per definitie een andere rationaliteit dan een staat, met als gevolg dat hun besluitvorming ook anders zal zijn dan die van statelijke actoren.
Er is een viertal externe kernprincipes te onderscheiden binnen klassieke (niet-cyber) coercion: de kosten en baten, geloofwaardigheid, communicatie en reassurance (zekerstelling).[9] De kernprincipes van het dreigen met geweld als middel zijn daarom van belang bij het toepassen en toetsen van de coercion-theorie op cyber en IS. Deze kernprincipes dienen hier als de primaire handvatten voor het toetsen van de theorie aan de casus, wetende dat rationaliteit en de toepassing van geweld eveneens van invloed zijn op de klassieke- en cyber-coercion. Borghard en Lonergan hebben elk van de vier coercion-kernprincipes vertaald naar het virtuele domein. Hier wordt ook de vraag gesteld of het voor staten mogelijk is coercion via cyberpower toe te passen op vijanden.[10] Wat al snel duidelijk wordt is dat het virtuele domein ongeschikt is voor elk van de klassieke coercion-kernprincipes.

Kosten- en batenanalyse

Als er verkeerd wordt ingeschat wat een doelwitactor als waardevol beschouwt kan coercion falen, zowel binnen als buiten het cyberdomein.

5 Ahmad Maryudi, *The Contesting Aspirations in the Forests. Actors, Interests and Power in Community Forestry in Java, Indonesia* (Göttingen, Universitätsverlag Göttingen, 2011) 11.

6 Ibid, 11.

7 Thomas C. Schelling. *Arms and Influence* (New Haven, Yale University Press, 2008) 3.

8 Emilio Iasiello, 'Is Cyber Deterrence an Illusory Course of Action?', in: *Journal of Strategic Security* 7, No. 1 (2013) 64.

9 De Nederlandse vertaling van het kernprincipe *reassurance* is geruststelling maar dekt, anders dan de andere drie begrippen, onvoldoende de lading. Het draait er bij dit kernbegrip om dat als de gestelde eisen worden nageleefd er zekerheid heerst dat de actie waarmee gedreigd wordt daadwerkelijk niet tot uiting komt. 'Zekerstelling' of 'overtuigingskracht' dekken dit begrip al beter. In dit artikel wordt 'zekerstelling' gebruikt.

10 Erica Borghard en Shawn Lonergan, 'The logic of Coercion in Cyberspace', in: *Security Studies* Vol. 26, No. 3 (mei 2017) 452-453.

Het primaire effect van een cyberaanval (een systeem plat leggen) lijkt een snelle, goedkope operatie met minimale gevolgen.[11] Als een *coercer* niet specifiek genoeg dreigt of een verkeerde afweging maakt aan welke systemen (en indirecte neveneffecten) het doelwit veel waarde hecht, is het dreigement weinig tot niks waard. Optimaal is wanneer actoren dreigen specifieke systemen plat te leggen (militaire of kritieke infrastructuur). Zo kan het secundaire effect wel grote gevolgen hebben voor de samenleving van een doelwitstaat en daarmee de kosten-batenberekening de juiste kant opsturen. Het verschil tussen primaire en secundaire effecten van cyberaanvallen in het digitale domein maakt *targeting* lastig. Coercion buiten cyberspace kan falen bij een verkeerde inschatting wat als waardevol wordt gezien en wat niet.[12] Dit geldt ook voor cyber coercion.

Geloofwaardigheid in het digitale domein

De geloofwaardigheid van cyber coercion wordt beïnvloed door de anonimiteit van actoren, de betrouwbaarheid van communicatie en de kennis over de capaciteiten van actoren. Binnen de coercion-theorie is de geloofwaardigheid afhankelijk van het vermogen om de bedreigde kosten op te kunnen leggen (capaciteit) en de wil om de opgelegde straf uit te kunnen voeren als de bedreigde actor niet voldoet aan de gestelde eisen.[13] Hierbij wordt ervanuit gegaan dat de actor rationele keuzes maakt.

Een heersend probleem is dat cyber-persona totaal andere actoren kunnen zijn buiten het digitale domein dan daarbinnen. Zo kan een

11 Ibid, 463.
12 Ibid, 460.
13 Ibid, 464.

Als er verkeerd wordt ingeschat wat een doelwit-actor als waardevol beschouwt kan coercion falen, zowel binnen als buiten het cyberdomein

FOTO FORT GEORGE G. MEADE PUBLIC AFFAIRS OFFICE

Een online-identiteit maakt cyber-persona anoniem en daarmee onbetrouwbaar

serieus dreigement onbelangrijk lijken doordat de online-actor ongeloofwaardig is, ongeacht wie de reële actor is. Als vage dreigementen afkomstig zijn van anonieme actoren verliest de beoogde coercion aan geloofwaardigheid. Achter de cyber-persona kan een niet-rationele actor schuilen, waardoor de capaciteit en de wil van deze actor onbekend blijven. Doelwitten moeten geloven waar een dwingende actor toe in staat is, gelet op deze rationaliteit, capaciteit en de wil bepaalde acties uit te voeren.[14] Een online-identiteit maakt cyber-persona anoniem en daarmee onbetrouwbaar, wat invloed heeft op de geloofwaardigheid van deze actor.

Communicatie in het digitale domein

Goede communicatie is essentieel voor het succesvol toepassen van de coercion-theorie, ook binnen het digitale domein, waarbij het overbrengen van de intentie van de coercer de kern is.[15] Dit is echter niet gemakkelijk, want communicatie via cyber bestaat uit een signaal dat van mensen afkomstig is en verstuurd is via machines. Hierdoor kunnen de zender, ontvanger en de aard van het signaal onbekend blijven.[16] Zoals coercion buiten het digitale domein waarde hecht aan goede communicatie – miscommunicatie doet coercion immers mislukken – geldt dit ook voor cyber coercion. In het digitale domein is communicatie uitdagend omdat er geen overeenstemming is over de algemene online-gedragsnormen, een gemeenschappelijke taal en het medium waar staten op diplomatiek niveau met elkaar kunnen communiceren.[17] Rusland, China en de VS konden bijvoorbeeld geen overeenstemming vinden over de omvang van het digitale domein en wat tot information security of cyber security behoort.[18] Daarnaast wisten de twee cybergrootmachten, China en de VS, bij een vergadering van hun gezamenlijke werkgroep over cyber security, niet tot een consensus te komen over een gemeenschappelijke taal.[19] Daar komt nog bij dat de individuen die op statelijk niveau beslissingen nemen, basiskennis van het digitale domein missen. Borghard en Lonergan noemen dit een intellectuele tekortkoming die laat zien dat *high-level decision makers* (invloedrijke politici) niet voldoende voorbereid zijn om met een cybercrisis om te kunnen gaan.[20] Het is daarom ook moeilijk voor te stellen dat dezelfde politieke beslissingsverantwoordelijken de digitale capaciteiten van staten optimaal toepassen. De complexe digitale communicatie heeft niet de essentiële gemeenschap in taal en communicatiemedium, wat leidt tot onduidelijkheid en zo ook het mislukken van cyber-coercion.

Zekerstelling en cyber

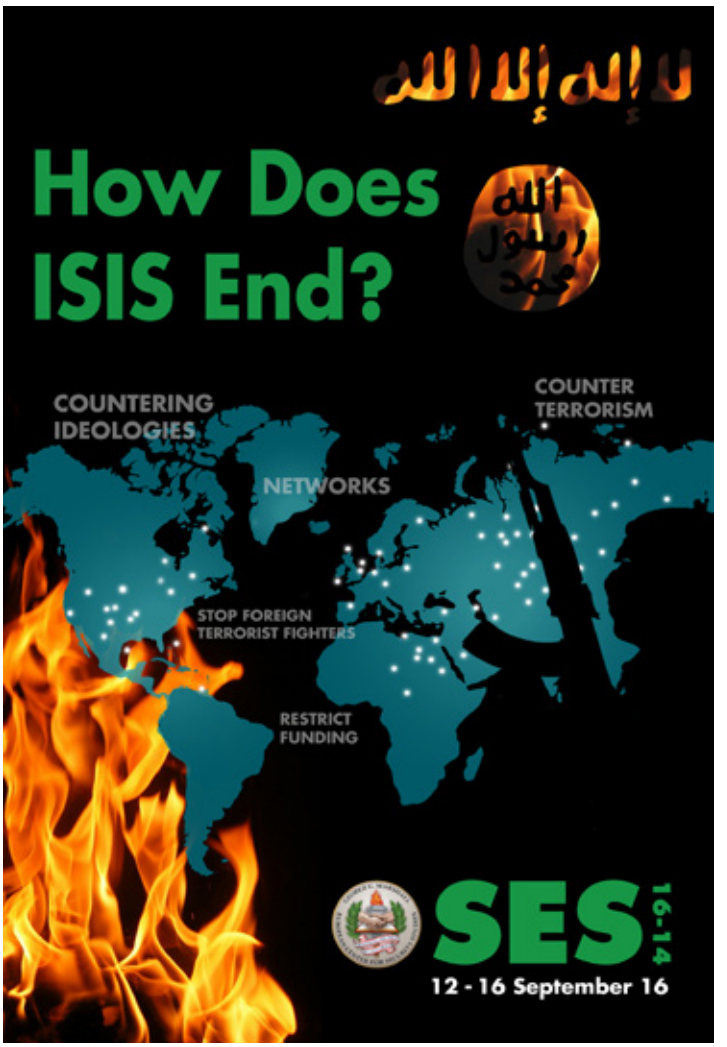
De aard van de gestelde dreiging en *command and control* van de coercer hierover bepalen de mate van zekerstelling binnen het digitale domein. Volgens Borghard en Lonergan is het lastigste van cyber coercion het verzekeren dat de genoemde consequenties verdwijnen als de doelwitstaat capituleert voor de gestelde eisen van de coercer.[21] Het is essentieel dat de coercer een goede controle over de eigen capaciteiten en gestelde consequenties heeft (command and control) voor het creëren van zekerheid bij een doelwit.[22] Dreigen met of het uitvoeren van

14 Ibid., 466-467.
15 Ibid., 456.
16 Ibid, 457-458.
17 Iasiello, 'Is Cyber Deterrence an Illusory Course of Action?', 56-57; Borghard en Lonergan, 'The logic of Coercion in Cyberspace'Borghard en Lonergan, 456.
18 Tim Farnsworth, *China and Russia Submit Cyber Proposal* (Washington, D.C., Arms Control Association, 2011).
19 Bill Gertz, 'U.S., China Strategic and Economic Dialogue Criticized', *The Washington Free Beacon* (16 juli 2013).
20 Borghard en Lonergan, 'The logic of Coercion in Cyberspace', 456.
21 Ibid., 471.
22 Ibid., p. 472.

verstorende cyberaanvallen is hierbij effectiever dan een onomkeerbare destructieve aanval.[23] Vertrouwen op het terugdraaien van een verstorende aanval, of het voorkomen van een destructieve aanval, kan enkel dankzij goede communicatie, kennis over de actor en zekerheid over de capaciteiten van de coercer.
Een coercer kan de controle over een verstorende of destructieve aanval verliezen, waardoor coercion mislukt. Een voorbeeld hiervan is het verliezen van controle door de VS en Israël over het Stuxnet-virus.[24] Daardoor was er weinig zekerheid over het beëindigen van deze verstorende cyberbaanval. Daarnaast was de identiteit van de coercer formeel gezien onbekend ten tijde van de aanval en kon niet met zekerheid gesteld worden dat de aanval zou stoppen als aan bepaalde voorwaarden werd voldaan. Binnen cyber coercion een vorm van zekerstelling creëren gaat dus samen met geloofwaardigheid en de juiste command en control over de gestelde consequenties.

Het is duidelijk dat de vier kernprincipes van klassieke coercion onvoldoende tot hun recht komen in het digitale domein als staten dit willen toepassen. Doordat een staat die coercion gebruikt in het cyberdomein niet overtuigend geloofwaardig kan zijn, zekerstelling niet kan garanderen en niet duidelijk genoeg kan communiceren zal het einddoel van coercion, iemand een onvrijwillig besluit laten nemen om zijn gedrag aan te passen, niet worden gehaald. Aangezien klassieke coercion uitgaat van statelijke actoren en een directe vertaling naar het digitale domein niet mogelijk lijkt, is de toepassing van cyber coercion door een andere soort actor mogelijk wel een optie.

FOTO GEORGE C. MARSHALL CENTER FOR SECURITY STUDIES, ZACHARY SHERMAN



Tijdens een seminar in de VS in 2016 werd duidelijk dat IS niet alleen conventioneel, maar ook in het cyberdomein verslagen zou moeten worden

IS in het digitale domein

Op 3 februari 2015 deelde de terreurbeweging IS een 22 minuten durende video waarin de gevangengenomen Jordaanse F-16-vlieger Muadh al-Kasasbeh levend werd verbrand in een kooi. Het aanvankelijke Twitterbericht met deze video werd snel op meerdere mediakanalen gedeeld. De beelden waren afkomstig van de al-Furqan Media Foundation,[25] sinds 2006 de primaire

23 Ibid., p. 472.

24 David E. Sanger, 'Obama Order Sped Up Wave of Cyberattacks Against Iran', in: *The New York Times*, 1 juni 2012). Onder de codenaam 'Olympic Games' lanceerde de VS een schadelijk computerprogramma voor Siemens-apparatuur. Deze digitale 'worm' was gemaakt om cyberaanvallen uit te kunnen voeren op het Iraanse nucleaire programma toen het in 2010 werd ontdekt. Aanpassingen op de worm door Israël zorgde ervoor dat niet alleen Iraanse apparatuur werd aangevallen, maar ook 'onschuldige' computersystemen over heel de wereld. Officiële deelname aan de ontwikkeling en het delen van dit cyberwapen door de VS en Israël is echter nooit erkend.

25 Nance en Sampson, *Hacking ISIS*, 136.; Nicky Woolf, 'Fox News site embeds unedited Isis video showing brutal murder of Jordanian pilot', in: *The Guardian*, 4 februari 2015.

Het maken en wereldwijd delen van executievideo's is een methode die al-Qaida al toepaste, maar die IS vervolmaakte

mediaproducent voor IS. YouTube wist de video binnen enkele uren te verwijderen en Facebook gaf aan de video of een link ernaar direct te zullen verwijderen als die werden gepost.[26] In de korte periode waarin de video online stond konden velen de beelden van de brandende Jordaanse vlieger toch via een openbaar IS-Twitterkanaal bekijken. Ook nationale en internationale media, zoals al-Jazeera, CNN en BBC, schreven over de gruwelijke beelden, inclusief schermafbeeldingen en een gedetailleerde uitleg.[27] De video van Muadh al-Kasasbeh was niet de enige film geplaatst op (sociale) mediapagina's waarop leden van IS executies uitvoerden. Klausen heeft in haar artikel 'Tweeting the Jihad' meerdere voorbeelden genoemd waar executievideo's en schermafbeeldingen hiervan op Twitter en Instagram zijn geplaatst.[28] Nance en Sampson zijn eveneens ingegaan op dit gebruik van online-executievideo's door IS.[29] Het maken en wereldwijd delen van executievideo's is een methode die al-Qaida al toepaste, maar die IS vervolmaakte. Nance en Sampson noemen deze 'Hollywood style'-video's van zeer hoge kwaliteit een perfectionering van de vergelijkbare angstzaaiende mediastrategie van al-Qaida.[30] Met het gebruik van sociale media wist IS snel veel mensen te bereiken. Het maken en versturen van zulke beelden was tien jaar geleden nog omslachtig, maar met de komst van sociale media zoals Twitter en Instagram kon IS dit gemakkelijker en sneller doen.[31] Zo waren er in 2004 ruim een half miljoen weergaves van de video waarin al-Qaidaleider Abu Musab al-Zarqawi de Amerikaan Nicholas Berg vermoordde. Op 19 augustus 2014 deelde IS een soortgelijke video waarop de onthoofding van de Amerikaanse journalist James Foley te zien was. De tientallen miljoenen downloads van deze video, 'A message to America',[32] de spot richting president Obama en het dreigen met geweld tegen andersdenkenden lieten zien wat voor angstzaaiend effect IS via visuele media kon realiseren.[33]

Klausen geeft aan dat sociale media voor terroristen een effectief communicatiemiddel zijn voor het beïnvloeden van bevolkingen.[34] Terroristische groeperingen zoals IS ervoeren dankzij internet dan ook amper geografische belemmeringen om het Westen, hun vijand, gemakkelijk te bereiken. Door slim gebruik te maken van dit middel wist IS zijn invloed internationaal snel te vergroten en een groot netwerk op te bouwen met sympathisanten over heel de wereld. Nance en Sampson noemen dit de 'electronic jihad' die de elektronische 'zwaarden' van IS, beter bekend als 'the cyber soldiers of the Caliphate', voeren.[35] Tijdens het offensief van 2014 in Syrië en Irak gebruikte IS Twitter als platform voor het delen van beeldmateriaal waarop IS-strijders executies uitvoerden.[36] Niet alleen essentiële communicatie ging via sociale media, maar ook het delen van propaganda en jihadistische successen, met het doel vijanden te bedreigen en bang te maken.

26 Woolf, 'Fox News site embeds...'.
27 *Trouw*, 'IS verbrandt Jordaanse piloot levend' (Twitter, 3 februari 2015); *Al-Jazeera*, ISIL video purports to show Jordanian pilot's killing' (3 februari 2015); Laura Smith-Spark en Michael Martinez, 'Who was Jordanian pilot Moat al-Kasasbeh, killed by ISIS?' (*CNN*, 4 februari 2015); 'Jordan pilot murder: Islamic State deploys asymmetry of fear (*BBC*, 4 februari 2015).
28 Jytte Klausen, 'Tweeting the Jihad. Social Media Networks of Western Foreign Fighters in Syria and Iraq', in: *Studies in Conflict & Terrorism* Vol. 38, No. 1 (2014) 5-6.
29 Nance en Sampson, *Hacking ISIS*, 134-135.
30 Ibid., 134-135.
31 Ibid., pp. 134-135.
32 Zack Beauchamp, 'ISIS captured and executed James Foley and Steven Sotloff, two American journalists', *Vox* (17 november 2015).
33 Nance Nance en Sampson, *Hacking ISIS*, 134-135.
34 Klausen, 'Tweeting the Jihad', 20.
35 Nance en Sampson, *Hacking ISIS*, 30-31.
36 Klausen, 'Tweeting the Jihad', 4.

Mosul in Irak werd deels verwoest in de strijd tegen IS: voor de terreurgroep is het cyberdomein voornamelijk het medium dat de boodschap achter het geweld deelt

FOTO EUROPESE UNIE, PETER BIRO

Met de toetreding tot het digitale domein, de inzet van cyber soldiers en het dreigen met (meer) geweld lijkt IS een coercionstrategie uit te voeren in dat domein, vergelijkbaar met de cyber coercion-theorie van Nance en Sampson.[37] De kenmerken van de klassieke coercionstrategie, te weten het dreigen met aanslagen en het zaaien van angst bij politici en samenlevingen, zijn immers nu ook aanwezig. De theorie rondom cyber coercion is nog in ontwikkeling en initieel toegespitst op staten en niet op NSA's als IS.[38] Voordat er geconstateerd kan worden of IS daadwerkelijk een bepaalde vorm van coercion gebruikt in het digitale domein, wordt eerst dieper ingegaan op cyber coercion als theorie.

Cyber coercion door IS

De Nationaal Coördinator Terrorismebestrijding en Veiligheid heeft een definitie opgesteld van terrorisme, waarbij 'de politieke besluitvorming beïnvloeden' onderdeel is van dit begrip.[39] Terroristen hebben ideologische motieven, willen maatschappijen ontwrichten, bevolkingen vrees aanjagen en destabilisatie bewerkstelligen. Dat terroristische organisaties politieke besluitvorming willen beïnvloeden komt overeen met coercion, waarbij de ene actor de andere probeert te dwingen tot het onvrijwillige gedragingen of beslissingen. Puur theoretisch betekent dit dat terroristische organisaties aan coercion doen. Bij IS is de dwingende kracht die toegepast wordt op andere actoren afhankelijk van geweld. Het cyberdomein dient voornamelijk als medium dat de boodschap achter dit geweld deelt.

Met de executievideo's, beelden van trainingskampen en berichten van het front[40] heeft IS twee verschillende doelen. Het eerste doel is

37 Borghard en Lonergan, 'The logic of Coercion in Cyberspace', 452-455.
38 Ibid., 4.
39 Nationaal Coördinator Terrorismebestrijding en Veiligheid, *Definities gebruikt in het Dreigingsbeeld Terrorisme Nederland* (NCTV, z.d.). Zie: nctv.nl/onderwerpen/dtn/definities-gebruikt-in-het-dtn.
40 Nance en Sampson, *Hacking ISIS*, 134-135.; Klausen, 'Tweeting the Jihad', 5-6.

het eigen gedachtegoed verspreiden om zo aanhangers te rekruteren, gevolgd door het vergroten van internationale invloed. Het tweede doel is intimideren en angst zaaien en zo samenlevingen van IS-opponenten te destabiliseren. Dit tweede doel moet uiteindelijk een apocalyptische oorlog met het Westen ontketenen.[41] Bij het realiseren van deze doelen kent IS, anders dan staten, een andere rationaliteit. Ook de Arabisch-religieuze achtergrond zorgt ervoor dat de keuzes die IS maakt gebaseerd zijn op andere normen, waarden en rationele fundamenten dan westerse staten. Dit beïnvloedt de communicatie, geloofwaardigheid en beslissingen omtrent de kosten en zekerstelling van IS als coercer in het cyberdomein.

41 Willem Oosterveld, e. a. *The Rise and Fall of ISIS. From Evitability to Inevitability* (Den Haag, *The Hague* Centre for Strategic Studies, 2017) 9.

Om het online-gedrag van IS te kunnen toetsen aan de bestaande cyber coercion-theorie, zijn de vier eerder genoemde kernbegrippen bepalend. Het is, gelet op deze kernbegrippen, duidelijk dat staten klassieke coercion niet met succes naar het cyberdomein kunnen vertalen. Maar IS is geen staat, gebruikt geweld op een andere manier en hanteert een andere rationaliteit. Daarom worden de acties van IS getoetst aan hetzelfde kader als de acties van staten in het digitale domein.

Bij staten vormen het ontbreken van een gemeenschappelijke online-taal en een algemeen geaccepteerd medium voorbeelden van het mislukken van coercive communicatie in het cyberdomein

FOTO US JOINT MISSION OPERATIONS CENTER

Kosten- en batenanalyse door IS

Het is voor succesvolle coercion van essentieel belang de juiste doelen te kiezen. Zeker in het cyberdomein is de primaire aanval op of actie tegen een vijand minder significant dan de secundaire effecten ervan. Staten kijken binnen het cyberdomein veelal naar klassieke methodes zoals hacken en cyberaanvallen[42] (Stuxnet) op kritieke infrastructuur, zodat civiele instanties en burgers zo min mogelijk geschaad worden. IS kent een andere rationaliteit en gebruikt naast het fysieke netwerk ook softwarecapaciteiten en eigenschappen van cyber-persona in het cyberdomein om invloed op staten uit te oefenen. Als NSA gebruikt IS het hele cyberdomein zo om te groeien, samenlevingen af te schrikken en overheden te beïnvloeden.

Met IS als coercer zijn westerse staten het doelwit en worden ze geforceerd een keuze te maken: de geplande kosten accepteren en een conflict aangaan met IS, of concessies doen, wat inhoudt dat IS wereldwijd als staat mag groeien, met als gevolg het tolereren van hun gedachtegoed en gedragingen. Het was snel duidelijk dat westerse staten IS niet wilden laten groeien, maar ook terughoudend waren om een fysieke oorlog te starten. Westerse staten wilden militairen uit de handen van IS houden om doden en online-executies te voorkomen.[43] Na video's waarop James Foley en later Steven Sotloff[44] vermoord werden kondigde president Obama aan dat de VS toch actie ging ondernemen.[45] Aanslagen van IS in Europa leidden tot

42 Borghard en Lonergan, 'The logic of Coercion in Cyberspace', 452-453.

43 Gilles Hertzog, 'Fighting the wrong war on ISIS', *Tabletmag*, 25 oktober 2019); Alcides Peron en Rafael Dias, 'No Boots on the Ground, Reflections on the US Drone Campaign through Virtuous War and STS Theories', in: *Contexto Internacional* Vol. 40, No. 1 (2018) 53-54.

44 Beauchamp, 'ISIS captured and executed...'.

45 Jessica Stern en J.M.Berger, *ISIS: The State of Terror* (New York, Ecco/HarperCollins, 2015) XXI.

steun van Europese coalitiepartners in de oorlog tegen de organisatie.[46] De kosten om een oorlog aan te gaan met IS wogen minder zwaar voor westerse staten dan de kosten om IS zijn gang te laten gaan.

IS heeft cyberbedreigingen via (sociale) media gebruikt en met fysiek geweld en aanslagen zijn gewelddadige capaciteit bewezen, allemaal om een confrontatie met het Westen aan te kunnen gaan. Hieruit volgt dat er coercion zichtbaar is in de bedreigingen van IS. IS laat zijn capaciteiten zien via aanslagen en dwingt zijn opponenten zo een onvrijwillige keuze te maken. Geweld is overigens geen eenduidig begrip binnen coercion. Daarom kan het toegepaste geweld op video's of bij aanslagen voor sommige critici een teken zijn van simpel gebruik van geweld en geen onderdeel van coercion.

Digitale geloofwaardigheid van IS

Het is duidelijk dat geloofwaardigheid in het cyberdomein in het geding komt als gevolg van de anonimiteit van cyber-persona. Het succes van coercion hangt onder meer af van de geloofwaardigheid van de dreiging. Anonimiteit maakt dreigementen minder geloofwaardig, maar anonimiteit kan ook in het voordeel worden gebruikt om juist onduidelijkheid te creëren bij de opponent. Grote hoeveelheden anonieme volgers via verschillende socialemedia-accounts laten de niet te bestrijden omvang van het virtuele kalifaat zien. IS eist aanslagen vooral op via (sociale) mediakanalen, via cyber-persona. De (Twitter)berichten op IS-gerelateerde pagina's en nieuwszenders als Amaq na aanslagen in Brussel (2017)[47] en Nice (2016)[48] zijn hier voorbeelden van. De terroristische aanvallen die buiten het cyberdomein worden uitgevoerd in de naam van IS tonen aan dat het kalifaat niet alleen dreigt, maar de daad bij het woord voegt. Dit maakt de dreiging zelf geloofwaardiger.[49] Het claimen van aanslagen door cyber-persona die in naam van IS zulke dreigementen maken en aanslagen opeisen, is anoniem en zo minder geloofwaardig.

Online-communicatie door IS

De communicatie is geslaagd als de intentie en de gestelde eisen van de coercer, IS, op het doelwit, het Westen, juist overkomt. IS kijkt bewust wie ze proberen te bereiken via het digitale domein en hoe ze dit het beste kunnen doen. Zo is de rekrutering voornamelijk afhankelijk van moslims en Arabischsprekende bevolkingen, waarop online-berichten dan ook worden toegesneden. Eufemistische propaganda in het Arabisch, over een luxe leven in het kalifaat en de daar heersende opvattingen over de islam, bleek hiervoor nodig te zijn.[50] Dat is duidelijk anders dan bij op het Westen gerichte berichten, waar aan propagandavideo's Engelstalige ondertiteling of commentaar wordt toegevoegd om de communicatie te bevorderen. Waar bij staten het ontbreken van een gemeenschappelijke online-taal en algemeen geaccepteerd medium voorbeelden zijn van het mislukken van coercive communicatie in het cyberdomein, is dit voor IS niet zo'n groot probleem. IS gebruikt immers andere manieren van communicatie. Zo worden sociale media en cyber-persona juist gebruikt om een groot netwerk aan ontvangers te bereiken, terwijl statelijke actoren liever via één veilig medium één andere staat willen aanspreken. IS gebruikt dus meerdere fysieke middelen (geweld/aanslagen als dreigement) en cybercommunicatie om meerdere doelen te realiseren. Een gemeenschappelijke online-taal of communicatiemedium lijkt hierbij overbodig. Videobeelden in verschillende talen voor een zo groot mogelijk publiek en sociale media bieden alles wat IS nodig heeft.

Online-zekerstelling door IS

IS stimuleert en inspireert volgers virtueel in het plegen van aanslagen, waardoor de organisatie niet altijd in direct verband kan worden

46 'Rutte: we zijn in oorlog met IS', *NOS* (14 november 2015); Simon Andries, 'Frankrijk en internationale gemeenschap verklaren de oorlog aan ISIS', *Het Nieuwsblad* (15 november 2015).

47 Kelly McCleary e.a. 'ISIS claims attack on soldiers in Brussels', *CNN* (26 augustus 2017).

48 Sam Jones, Angelique Chrisafis en Caroline Davies, 'Nice truck attack: Islamic State claims responsibility', *The Guardian* (16 juli 2016).

49 Clara Pellerin, 'Communicating Terror: an Analysis of ISIS Communication Strategy', *SciencesPo Kuwait Program* (Spring 2016) 4.

50 Peter Neumann, *Victims, Perpetrators, Assets: The Narratives of Islamic State Defectors* (ICSR, King's College London, 2015) 11; Paul van der Bas, 'Steeds meer teleurgestelde strijders verlaten ISIS. ''We kregen geen luxe auto!''', *De Dagelijkse Standaard* (22 september 2015).

gebracht met het toegepaste geweld.[51] De aanslagen van door IS beïnvloede individuen zijn geen onderdeel van coercion, maar de combinatie van het opeisen van deze aanslagen en het stimuleren via het virtuele kalifaat neigt hier wel naar. Als een vorm van *show of force* laat IS zien hoe ver zijn invloed rijkt, wat zijn capaciteiten zijn en waar het kalifaat mensen toe kan aanzetten. IS claimt de aanslagen die in zijn naam worden gepleegd om westerse samenlevingen angst in te boezemen.[52]
Met inzichtelijke capaciteiten en de zekerstelling dat dreigen met aanslagen ook resulteert in het uitvoeren daarvan, lijkt IS zekerstelling te realiseren. Aanslagen worden echter vaak uitgevoerd door volgers geïnspireerd door IS. Gecentraliseerde coördinatie is vaak afwezig en daarmee ook de command and control over de dreigementen en fysieke aanvallen. Dit laat zien dat IS toch geen zekerstelling kan creëren, maar enkel angst voor aanslagen, wat geen kernprincipe is van coercion.
Hoewel cyber coercion bij IS in een bepaalde mate herkend kan worden binnen de vier kernprincipes, is dit constant in combinatie met het fysieke optreden van de terreurgroep. Zo verliezen virtuele bedreigingen geloofwaardigheid zonder aanslagen of executies. Het gedecentraliseerde fysieke geweld om westerse samenlevingen te ontwrichten dat virtueel wordt gevoed door cybercoaches[53] en online-stimulatie[54] lijkt eerder een primair doel van IS te zijn dan een neveneffect van een geloofwaardige en succesvolle coercion strategie.

Conclusie

IS heeft als NSA laten zien succesvol te zijn binnen het digitale domein en zelfs een bepaalde mate van coercion toe te passen via het cyberdomein. Staten namen de beslissing een oorlog met IS aan te gaan, nadat de terreurgroep ze had beïnvloed deze keuze te maken. De cyber coercion-theorie gaat nog te veel uit van de klassieke coercion-kernprincipes en de aanname dat staten coercers zijn. Het cyberdomein is simpelweg niet een-op-een verenigbaar met de klassieke coercion zoals we die kennen. Daarom kan de cyber coercion-theorie niet correct toegepast worden op het online-beleid van IS, maar heeft het wel geholpen om in te zien dat het cyberdomein vraagt om innovatief, onconventioneel gebruik. Het inzicht dat een terroristische organisatie keuzes van machtsblokken als het Westen kan beïnvloeden via het cyberdomein laat zien dat dit domein voor veranderingen zorgt binnen de klassieke hiërarchische verdeling van macht. Elke statelijke actor, terroristische organisatie of individu kan via slim gebruik van het cyberdomein als anonieme cyber-persona meedoen op het hoogste machtsniveau.

Het cyberdomein vraagt om innovatief, onconventioneel gebruik

De realistische angst om als staat achter te lopen bij digitale dreigingen van buitenaf is daarom maar een klein facet van de lastige situatie die de komst van het digitale domein heeft weten te creëren. Het digitale domein biedt namelijk ook kansen voor NSA's, van individuen tot goed georganiseerde organisaties als IS, om op politiek-strategisch niveau invloed uit te oefenen. Dit vraagt om snellere innovatie bij staten om te voorkomen achter te lopen in de virtuele wereld. ■

51 Algemene Inlichtingen- en Veiligheidsdienst, 'Aangestuurde, gestimuleerde en geïnspireerde aanslagen' (z.d.); 'IS eist elke aanslag op, maar is niet altijd verantwoordelijk', *RTL nieuws* (29 juli 2016).
52 Stern en Berger, *ISIS*, 201.
53 Voor de betekenis van cybercoaches, zie hoofdstuk 4.2.3.
54 Algemene Inlichtingen- en Veiligheidsdienst, 'Aangestuurde, gestimuleerde en geïnspireerde aanslagen'.