Tunnelvisie? De digitale strijd rond het Gazaconflict

Luitenant-kolonel ing. K.L. Arnold EMSD MSc*

Op 7 oktober 2023 lanceerde Hamas[1] een aanval op Israëlisch grondgebied, waarbij extreem geweld werd ingezet. Israël reageerde met operatie Iron Swords en viel de Gazastrook binnen. Vrijwel tegelijkertijd begonnen andere entiteiten zich actief te bemoeien met dit conflict. Zij vochten niet fysiek, noch ter plaatse, maar aan het online cyberfront. In tegenstelling tot het intense kinetische conflict is informatie over de digitale oorlogsvoering slechts beperkt beschikbaar. Eén aspect is al wel duidelijk: de strijdende cyberpartijen lijken vooralsnog niet in staat geweest om kritieke systemen of diensten beslissende strategische schade toe te brengen. Dat roept vragen op over de relevantie van cyberoorlogvoering. Hebben de strijdende partijen eigenlijk wel cybercapaciteit? Als de strijd eenmaal losbarst, spelen cyberaanvallen dan nog wel een rol? Heeft Hamas digitale infrastructuur die het aanvallen waard is? Als er aanvallen zijn, wat zijn dan de doelwitten en welke effecten zijn mogelijk?

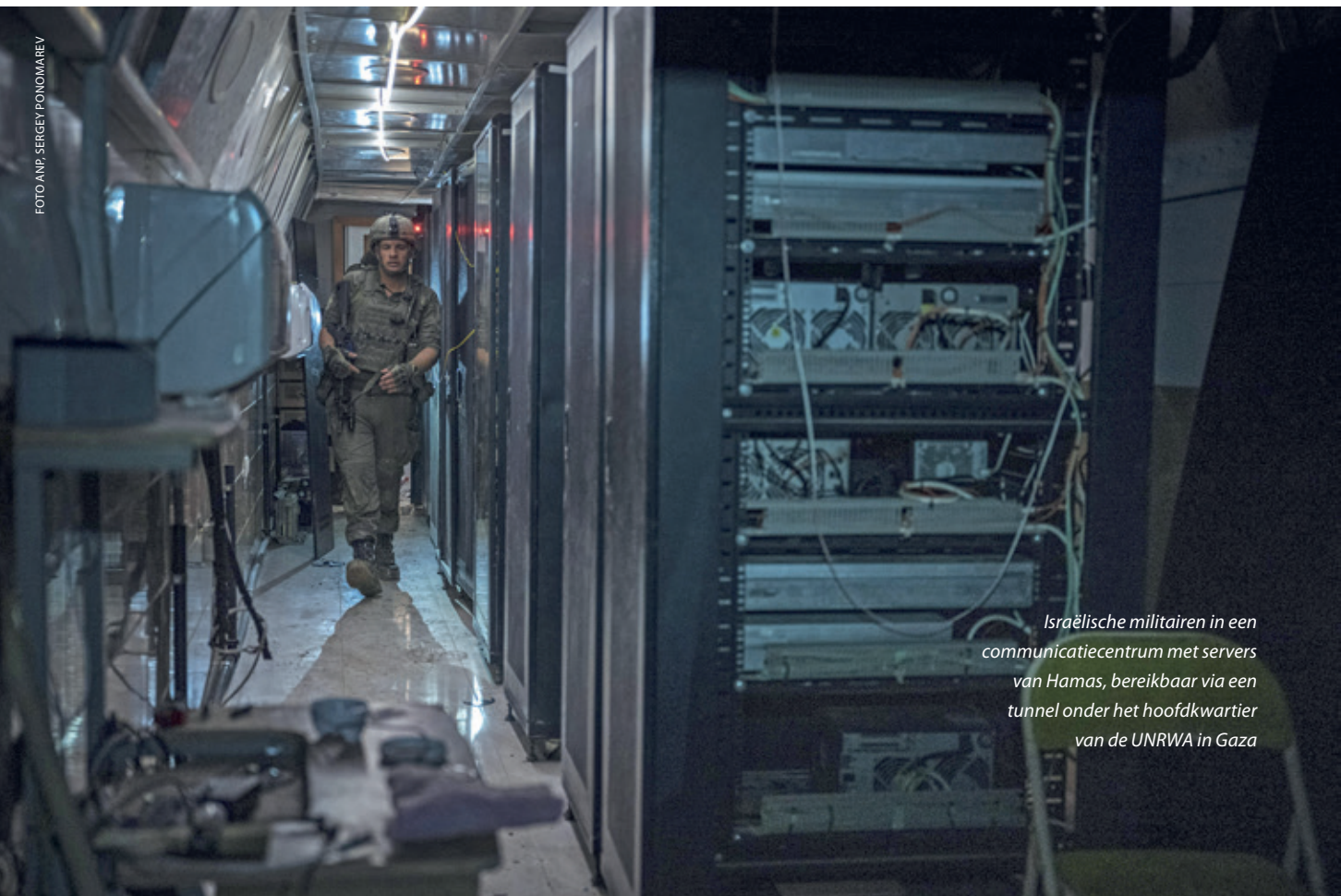

FOTO ANP, SERGEY PONOMAREV

Israëlische militairen in een communicatiecentrum met servers van Hamas, bereikbaar via een tunnel onder het hoofdkwartier van de UNRWA in Gaza

Cyberoorlogvoering kent meerdere aspecten. Hacken van computers en netwerken is één ding, maar het gebruik ervan om anderen te beïnvloeden is van een andere orde. Dit artikel gaat in op de cyberoorlogvoering rond het Hamas-Israëlconflict, om te bezien in hoeverre cyberoperaties relevant zijn in dit hedendaagse gewapende, irreguliere conflict. De inzet van cybermiddelen in het huidige conflict vormt een unieke casestudie over een digitale strijd, gevoerd tussen een gedigitaliseerde natiestaat en een hybride terroristische organisatie.

Dit artikel schetst eerst het cyberpotentieel van beide partijen, waarna een overzicht volgt van cyberaanvallen uit het recente verleden. In het huidige conflict komen eerst 'hard cyber-operaties' aan bod en vervolgens cyber-enabled beïnvloedingsoperaties ('soft cyberoperaties').[2] Het blijkt dat cyberoorlogvoering en de strijdende partijen onderdeel zijn van een breder geopolitiek conflict.

Scheve verhoudingen?

Israël heeft een uitgebreid cyberpotentieel, met honderden hightechbedrijven die met hun hoogopgeleide en bekwame personeel geavanceerde producten en diensten creëren. Het land vormt dan ook een van de grootste cybersecurity-ecosystemen ter wereld.[3] Het International Institute for Strategic Studies beschouwt Israël daarom als 'Tier Two' cyberstaat.[4] Het land excelleert in cyberbeveiliging en (cyber)inlichtingen verzamelen,[5] maar heeft ook een sterk ontwikkelde offensieve (cyberwapen)capaciteit.[6]

Men kan redelijkerwijs aannemen dat een niet-statelijke organisatie als Hamas dergelijke middelen, kennis en ervaring niet heeft.[7] Israël heeft bovendien de controle over de internet-infrastructuur en telecommunicatiefrequenties in Gaza. Tel daarbij op de chronische elektriciteitstekorten in het Palestijnse gebied, en het is des te opmerkelijker dat Hamas überhaupt een cyberdreiging *zou kunnen* vormen. Daar staat tegenover dat de groep de afgelopen vijftien jaar met geld, middelen en training is ondersteund door statelijke actoren vanuit Qatar, Iran en Turkije.[8] De digitale slagkracht van Hamas is daarnaast versterkt door een ideologische en strategische alliantie met Hezbollah en Iran.[9]

Cyberspace wordt niet beperkt door geografische grenzen. Dit impliceert dat elke actor, vanuit elke locatie waar een internetverbinding voorhanden is, actief betrokken kan raken bij deze cyberoorlog; niet alleen als aanvaller, maar ook als slachtoffer.

* Lt-kol Kraesten Arnold is als cyberonderzoeker en -docent verbonden aan de Faculteit Militaire Wetenschappen van de Nederlandse Defensie Academie te Breda. Zijn focus ligt met name op offensieve cyberoperaties door statelijke actoren.

1 Een Arabisch acroniem voor Harakat al-Muqawamah al-Islamiyyah ('de Islamitische Verzetsbeweging').

2 Hard cyberoperaties zijn cyberaanvallen gericht tegen cyberspace zelf, zoals hardware en software. Soft cyberoperaties gebruiken cyberspace voor bijvoorbeeld informatieoperaties of psychologische oorlogvoering. Zie: Peter B.M.J. Pijpers en Kraesten L. Arnold, 'Conquering the invisible battleground', *Atlantisch Perspectief* 44 (2020) (4).

3 Naast de bekende high-tech clusters Silicon Valley en Washington, D.C. Bron: Tali Hataku en Erran Camel, *The Dynamics of the Largest Cybersecurity Industrial Clusters: San Francisco Bay Area, Washington D.C. and Israel*, Blavatnik Interdisciplinary Cyber Research Center (ICRC), januari 2021. Zie: https://icrc.tau.ac.il/sites/cyberstudies-english.tau.ac.il/files/media_server/all-units/Cyber%20DIGITAL%20Final%20unlocked-1.pdf.

4 Tezamen met Australië, Canada, China, Frankrijk, Duitsland, Rusland, Nederland en het Verenigd Koninkrijk. De Verenigde Staten (VS) zijn overigens de enige 'Tier One' staat. Bron: 'Cyber Capabilities and national Power: A Net Assessment', The International Institute for Strategic Studies (IISS), IISS research Paper, 28 juni 2021, 10. Zie: https://www.iiss.org/research-paper//2021/06/cyber-capabilities-national-power.

5 Het Israëlische *NSO Group Technologies* is bijvoorbeeld de maker van de beruchte 'Pegasus' spionagesoftware; wereldwijd in gebruik bij overheden en waarmee, naar verluidt, de AIVD in 2019 de telefoon van Ridouan Taghi wist te hacken. Bron: Huib Modderkolk, 'AIVD gebruikt omstreden Israëlische hacksoftware', *de Volkskrant*, 2 juni 2022. Zie: https://www.volkskrant.nl/nieuws-achtergrond/aivd-gebruikt-omstreden-israelische-hacksoftware~b05a6d91/.

6 De meest tot de verbeelding sprekende cyberaanval tot op heden (de Stuxnet-cyberaanval tegen het Iraanse kernwapenprogramma in de periode 2007-2010) wordt toegeschreven aan een Amerikaans-Israëlisch samenwerkingsverband. Bron: Kim Zetter,*Countdown to zero day: Stuxnet and the launch of the world's first digital weapon* (Crown, 2015).

7 Desondanks bleek Hamas aan de vooravond van de 7 oktober-inval over een Militaire Inlichtingendienst te beschikken die bestond uit zo'n 2.100 krachten, verdeeld over vijf subafdelingen: observatie, cyber, signals intelligence (SIGINT), open source intelligence (OSINT), en human intelligence (HUMINT). Bron: Itay Ilnai, *The road to Oct. 7: How Hamas got the intelligence it needed*, Israel Hayom, 16 maart 2024. Zie: https://www.israelhayom.com/2024/03/16/the-road-to-oct-7-how-hamas-got-the-intelligence-it-needed/.

8 Jean-Luc Mounier, 'Qatar, Iran, Turkey and beyond: Hamas's network of allies', *France24*, 14 oktober 2023. Zie: https://www.france24.com/en/middle-east/20231014-qatar-iran-turkey-and-beyond-the-galaxy-of-hamas-supporters.

9 Marcin Andrzej Piotrowski, 'Iran's Relations with Hezbollah and Hamas Evolving', The Polish Institute of International Affairs, 24 oktober 2023. Zie: https://www.pism.pl/publications/irans-relations-with-hezbollah-and-hamas-evolving.

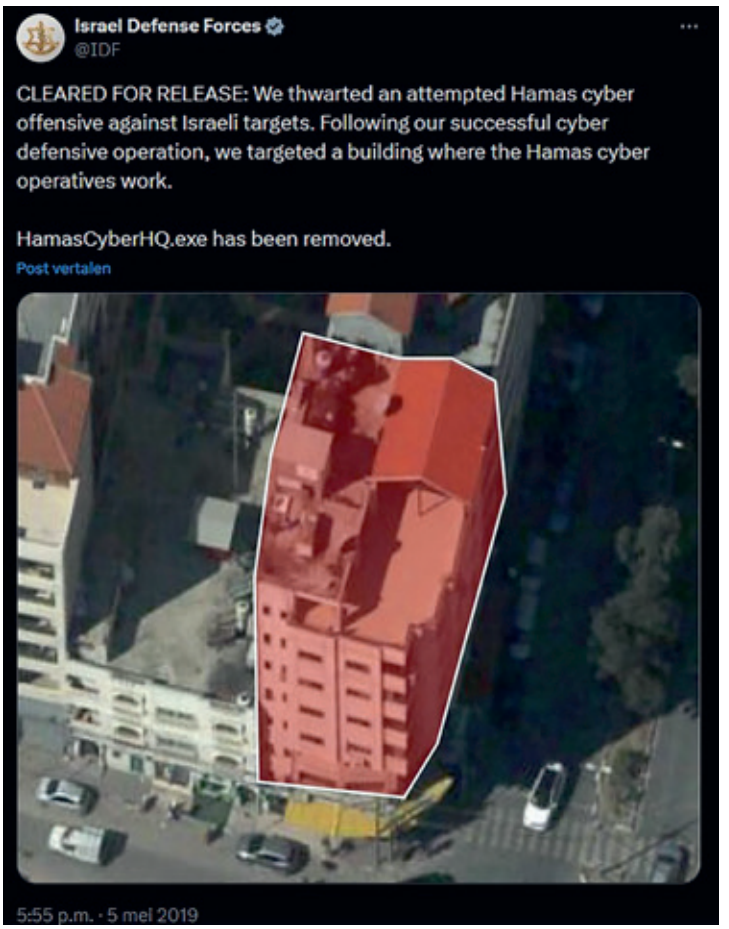

FOTO ISRAEL DEFENSE FORCES

Het Twitterbericht waarin de IDF de eerste kinetische vergeldingsactie voor een cyberaanval bekend maakte

Voorafgaande virtuele vijandelijkheden

Tijdens een eerder Gaza-conflict (2009) benutte zowel Hamas als Israël uitgebreid de inherente voordelen van sociale media. Het intense fysieke grondgevecht kreeg daarmee een digitale weerspiegeling. Beide partijen verkondigden online hun respectievelijke narratief en zochten, en vonden, steun van patriottische hackers en activisten elders in de wereld. Foto's, videobeelden, cartoons, objectieve informatie en propaganda werden verspreid, bewust hergebruikt (misinformatie) of ronduit vervalst (desinformatie). Beide partijen richtten zich daarnaast op het verstoren van websites, platforms, accounts en blogs die steun verleenden aan de tegenpartij.[10]

Traditionele media hadden ook destijds vrijwel geen toegang tot de grondstrijd. Voor informatieverspreiding leunden beide partijen zwaar op het internet en sociale media. Iedere niet-professionele *citizen journalist* kon voortaan in *real time* de strijd vastleggen, bewerken en uploaden. Traditionele mediabedrijven gebruikten de online informatie om die vervolgens via reguliere mediakanalen te verspreiden. Deze indirecte nieuwsverspreiding zorgde vervolgens weer voor een verhoogde focus op het conflict via socialemediaplatforms.[11]

In 2012 kondigde de woordvoerder van de Israëlische strijdkrachten een aanval op Gaza aan via Twitter. De tegenstanders verzandden in een *battle of the narratives* waarbij ze nieuwsberichten, verhalen en afbeeldingen deelden die vooral de misstappen van de ander benadrukten. Via hashtags (#) als #BringBackOurBoys, #GazaUnderAttack en #IsraelUnderFire trachtten beide zijdes hun gelijk te halen.[12]

Tot 2014 betrof de cyberoorlog voornamelijk 'digitale beïnvloeding' of 'soft cyberoperaties'. Sindsdien richtten zowel pro-Palestijnse als pro-Israëlische groepen zich ook op het hacken van computers en netwerken via Distributed-Denial-of-Service (DDoS)-aanvallen en defacements;[13] vervelend, maar met een relatief beperkte (herstelbare) schade. Dat veranderde in

10 David Patrikarakos, *War in 140 characters: how social media is reshaping conflict in the twenty-first century* (First Edition, New York, Basic Books, 2017).

11 Naila Hamdy, 'Arab media adopt citizen journalism to change the dynamics of conflict coverage', *Global Media Journal Arabian Edition* 1 (2010) (1) 4.

12 Patrikarakos, *War in 140 characters*.

13 Bij een Denial-of-Service (DoS)-aanval wordt een computer, netwerk of applicatie bestookt met zoveel opdrachten of verzoeken dat de werking van die computer of dat netwerk ernstig wordt beperkt of zelfs onmogelijk gemaakt. Voor een Distributed DoS-aanval worden meerdere computers gebruikt. Bij een website defacement verandert de aanvaller 'het uiterlijk' van een website door die te vullen met andere inhoud (tekstueel en/of visueel), zoals politieke, sociale of religieuze boodschappen.

2018, toen een aan Hamas-gelieerde hackergroep een nepversie wist te maken van Israëls raketwaarschuwingsapp 'RedAlert'. De vervalste app imiteerde de reguliere versie, maar zodra deze was gedownload, kreeg de aanvaller via de gemanipuleerde software de volledige controle over de betreffende mobiele telefoon. Naar verluidt werd de spionagesoftware (spyware) in een vroeg stadium ontdekt en was uiteindelijk weinig schade aangericht.[14]

In 2018 manipuleerde een aan Hamas-gelieerde groep de legitieme (WK-voetbal) softwareapplicatie 'Golden Cup' met spyware. Om vroegtijdige ontdekking van de gemanipuleerde software te voorkomen en beveiligingsmaatregelen te omzeilen, werd de spyware pas actief *nadat* de app was gedownload.[15] Na installatie van de app zochten de aanvallers via fictieve personages contact met hun slachtoffers, waaronder vele Israëlische militairen. Een soortgelijke truc werd uitgehaald via een fitness-app voor hardlopers.

In 2020 slaagde een aan Hamas-gelieerde groep (*Arid Viper*)[16] erin mobiele telefoons van IDF-soldaten te hacken. Ditmaal maakten de aanvallers gebruik van populaire dating-apps waarop (gefingeerde) vrouwelijke immigranten Israëlische soldaten versierden. Achter de geloofwaardig opgebouwde profielen schuilden hackers. Was het initiële contact gelegd, dan werden de slachtoffers verleid extra software te downloaden. De slachtoffers haalden daarmee zelf een 'digitaal Trojaans paard' binnen, waarna de aanvaller ongemerkt de volledige controle over geïnfecteerde mobieltjes had.[17]

Dankzij de geïnstalleerde spyware verkregen de hackers de volledige controle over de mobiele telefoons van hun slachtoffers. De apparaten veranderden in ultieme spionageapparatuur. Het stelde de aanvallers in staat het apparaat onopgemerkt te volgen, heimelijk foto's en videobeelden te maken, en stiekem geluidsopnames te maken en te versturen. Zo verzamelden de hackers ongemerkt inlichtingen over Israëlische troepen, troepenbewegingen, bases en militair materieel rondom de Gazastrook.[18]

In 2019, in een periode dat vanuit Gaza honderden raketten werden gelanceerd richting Israël, initieerde een aan Hamas-gelieerde hackergroep – eveneens vanuit Gaza – een cyberaanval op Israël. Over de exacte doelwitten of verwachte effecten van deze cyberaanval is nauwelijks openlijk informatie beschikbaar. Wat wel bekend is, is dat Israël deze cyberaanval tijdig onderkende en verijdelde, om vervolgens met een luchtaanval het gebouw in Gaza van waaruit de cyberaanval plaatsvond te vernietigen. Deze reactie is daarmee, voor zover bekend, de eerste kinetische vergeldingsactie voor een (geplande) cyberaanval. De IDF maakte deze actie op een nogal ironische wijze bekend: 'HamasCyberHQ.exe has been removed',[19] als ware het gebouw en zijn bewoners een softwareprogramma dat was gewist.

Ondanks Israëls optimistische claim volgden ook daarna nog cyberaanvallen; weliswaar niet vanuit Gaza, maar daarbuiten. De meest voor de hand liggende reden hiervoor is dat Hamas ook buiten Gaza beschikt over de nodige cyberfaciliteiten, zoals in Turkije,[20] Iran en Qatar.[21]

14 Toi Staff, 'Hamas tries to hack Israelis with fake rocket warning app', *The Times of Israel*, 10 augustus 2018. Zie: https://www.timesofisrael.com/hamas-tries-to-hac-israelis-with-fake-rocket-warning-app/.

15 Taylor Armerding, 'Golden Cup App Was a World Cup of Trouble', *Synopsys*, 12 juli 2022. Zie: https://www.synopsys.com/blogs/software-security/golden-cup-app-world-cup-trouble/.

16 De groep *Arid Viper* is een Arabisch sprekende, politiek gemotiveerde Advanced Persistent Threat (APT). Een APT betreft een veelal statelijke tegenstander die beschikt over technologisch hoogwaardige kennis en voldoende middelen om langdurig en via meerdere aanvalspaden zijn doelen te bereiken. De groep staat ook (onder meer) bekend onder de naam 'APT-C-23'.

17 Cybereason Nocturnus, 'Operation Bearded Barbie: APT-C-23 Campaign Targeting Israeli Officials'. Zie: https://www.cybereason.com/blog/operation-bearded-barbie-apt-c-23-campaign-targeting-israeli-officials.

18 Yaniv Kubovich, 'Hamas Cyber Ops Spied on Hundreds of Israeli Soldiers Using Fake World Cup, Dating Apps', Haaretz, 3 juli 2018. Zie: https://www.haaretz.com/israel-news/hamas-cyber-ops-spied-on-israeli-soldiers-using-fake-world-cup-app-1.6241773.

19 IDF woordvoerder op Twitter, 5 mei 2019. Zie: https://twitter.com/IDF/status/1125066395010699264.

20 Anshel Pfeffer, 'Hamas Uses Secret Cyberwar Base in Turkey to Target Enemies', *The Times* (UK), 22 oktober, 2020. Zie: https://www.thetimes.co.uk/article/hamas-running-secret-cyberwar-hq-in-turkey-29mz50sxs.

21 Simon Handler, 'The cyber strategy and operations of Hamas: Green flags and green hats', Atlantic Council Report, 7 november 2022. Zie: https://www.atlanticcouncil.org/in-depth-research-reports/report/the-cyber-strategy-and-operations-of-hamas-green-flags-and-green-hats/.

(Geen) digitale voorwaarschuwing?

'Harde' cyberaanvallen door Hamas, gericht op fysieke schade, deden zich de afgelopen jaren niet meer voor. De terreurgroep leek zich te focussen op cyberspionage en digitale beïnvloedingsoperaties. Israël, het land met de hoogstaande reputatie omtrent cyberbeveiliging en (cyber)inlichtingen verzamelen, dat bovendien controle uitoefent over de telecommunicatiefrequenties en internetinfrastructuur in de Gazastrook, leek zich dan ook weinig zorgen te maken over de digitale slagkracht van zijn tegenstander.

Israël wist dat Palestijnse militanten gebruik maakten van bekabelde communicatiemiddelen om afluisteren te bemoeilijken. Maar dat Hamas-planners hun specifieke terreurdaad kennelijk voorbereidden door alléén te communiceren (en te coördineren) via bekabelde verbindingen in de Gazatunnels spreekt tot de verbeelding. Door geen draadloze, digitale communicatiemiddelen te gebruiken, vermeden ze interceptie en analyse van signalen uit satelliet- en radiocommunicatie door de Israëlische militaire inlichtingendienst.[22]

Die dienst wist overigens dat een Hamas cyberactor (Gaza Cybergang) actief het internet verkende, op zoek naar IP-adressen van beveiligingscamera's die online toegankelijk waren.[23] Waren de IP-adressen eenmaal bekend en hadden de legitieme gebruikers het wachtwoord niet gewijzigd, dan konden de aanvallers heimelijk toegang krijgen tot die camera's via de (online beschikbare) standaard wachtwoorden.

De hackers verkregen daarmee real-time videobeelden van verschillende dorpen, militaire bases en de bredere Gaza-grensstreek. Naar later bleek verzamelde Hamas zo bruikbare inlichtingen in de aanloop naar zijn aanvallen op 7 oktober.[24]

De cyberstrijd barst los

Toen die aanval eenmaal begon, barstte ook de cyberstrijd los. De hard en soft cyberoperaties van beide zijdes vormen een unieke casestudie over een digitale strijd.

Hard cyberoperaties

Het merendeel van de cyberaanvallen rond het uitbarsten van het '7-oktoberconflict' betrof Distributed-Denial-of-Service (DDoS)-aanvallen, gericht op het (tijdelijk) verstoren van toegang tot, of het gebruik van, de aangevallen websites of applicaties en daarmee de (digitale) bedrijfsvoering van de slachtoffers. Het nagestreefde effect is veelal onzekerheid en chaos creëren onder de burgerbevolking, zeker als aanvallen zijn gericht op civiele objecten als nieuwswebsites, banken of de gezondheidszorg.

Pro-Palestijnse aanvallers voerden zo'n twaalf minuten na de Hamas-inval DDoS-aanvallen uit op Israëlische websites. Hoewel pro-Israëlische actoren soortgelijke aanvallen uitvoerden tegen Palestijnse websites, lag het aantal getroffen Israëlische entiteiten significant hoger dan het aantal Palestijnse.[25] De direct aangerichte schade van een DDoS-aanval is vaak beperkt en herstelbaar, maar doordat deze aanvallen vaak de aandacht trekken, kunnen ze ook dienen als bliksemafleider voor een heimelijke aanval op andere doelwitten. Of dat hier het geval was, is momenteel niet vast te stellen.

Andere cyberaanvallen betroffen website defacements, een soort digitale graffiti waarbij het 'uiterlijk' (de startpagina) van de aangevallen website werd aangepast, vaak met een specifieke politieke of religieuze boodschap. Deze cyberaanvallen zijn uitgevoerd door beide zijdes, maar ook hier overtrof het aantal pro-Palestijnse acties de pro-Israëlische. Tussen 7 en 16 oktober

22 Pamela Brown en Zachary Cohen, 'Hamas operatives used phone lines installed in tunnels under Gaza to plan Israel attack', CNN Politics, 25 oktober 2023. Zie: https://edition.cnn.com/2023/10/24/politics/intelligence-hamas-israel-attack-tunnels-phone-lines/index.html.

23 Het Internet Protocol (IP) is een wereldwijd afgesproken verzameling regels voor de wijze waarop computers op een computernetwerk (zoals het internet) met elkaar kunnen communiceren. Een IP-adres is een uniek identificatienummer ('digitaal postadres') dat door een Internet Service Provider wordt toegekend aan een apparaat dat is aangesloten op internet of een lokaal netwerk.

24 Ilnai, *The road to Oct. 7*.

25 Tanner Wagner, *Escalation of Threats in the Middle East*, CyberPeace Institute, 6 november 2023. Zie: https://cyberpeaceinstitute.org/news/escalation-of-threats-middle-east.

FOTO X.COM, CYB3R DRAG0NZ TEAM

Een hack-and-leak-operatie en website defacement ineen, geclaimd door het pro-Palestijnse Cyb3r Drag0nz Team. Het doelwit was een civiel object: BrainIT, een bedrijf dat escape rooms exploiteert. De hackers claimen gegevens van 40.000 klanten te hebben gelekt

werden ruim 500 defacementoperaties uitgevoerd tegen Israëlische websites.[26]

Een ander type cyberaanvallen betreft hack-and-leak-operaties. Daarbij steelt de aanvaller geclassificeerde of anderszins gevoelige informatie om die vervolgens te publiceren. Meerdere pro-Palestijnse activistische hackers claimden dat zij geclassificeerde defensie-informatie hadden buitgemaakt door militaire systemen en kritieke infrastructuur te hacken. Deze beweringen zijn lastig te verifiëren, aangezien geen van de slachtoffers dergelijke aanvallen meldde. Bovendien leken de gelekte gegevens te zijn 'hergebruikt'; afkomstig van eerdere cyberaanvallen en onterecht gepresenteerd als nieuw.[27]

Beide partijen gebruiken daarnaast social engineering-technieken om mensen te manipuleren (vijandelijke strijders in het bijzonder) en zo informatie te ontfutselen over vijandelijke troepenlocaties, -bewegingen, aanvalsplannen of andere relevante informatie. Met een techniek die bekend staat als catphishing of honey trapping doen hackers zich bijvoorbeeld voor als een aantrekkelijke jongedame, om zo initieel contact te leggen en vervolgens heimelijk inlichtingen te vergaren via tekst-, spraak- en/of videoberichten. Op basis van online verkregen informatie kan een gerichte kinetische aanval volgen.

De pro-Palestijnse cyberaanvallen lijken niet bewust afgestemd op Hamas' kinetische acties op 7 oktober. In 2022 ging Ruslands grootschalige grondoffensief tegen Oekraïne gepaard met destructieve 'wiperware' cyberaanvallen; kwaadaardige software, bedoeld om data en

26 Darkowl, 'Hacktivist Groups Use Defacements in the Israel Hamas Conflict', 26 oktober 2023. Zie: https://www.darkowl.com/blog-content/hacktivist-groups-use-defacements-in-the-israel-hamas-conflict/.

27 Omree Wechsler, 'The Cyberwarfare Front of the Israel-Gaza War', *The National Interest*, 5 november 2023. Zie: https://nationalinterest.org/feature/cyberwarfare-front-israel-gaza-war-207163.

Opvallend in dit conflict is het sterk toegenomen gebruik van zogeheten n-day vulnerabilities

computers van de slachtoffers blijvend te vernietigen.[28] Die Russische cyberaanvallen werden voorbereid en uitgevoerd in de weken voor, tijdens en vlak na de invasie. In het Hamas-Israëlconflict verschenen de eerste cyberaanvallen pas na het publiekelijk bekend worden van Hamas' fysieke aanval. Wel werden ook hier nieuwe varianten van destructieve wiperware ingezet, en ontdekt.[29]

Opvallend in dit conflict is het sterk toegenomen gebruik van zogeheten n-day vulnerabilities als manier om een computersysteem of netwerk ongeautoriseerd binnen te dringen.[30] Bepaalde statelijke of staatsgesteunde aanvallers houden bijvoorbeeld scherp in de gaten wanneer een fabrikant (zoals Microsoft) nieuw gevonden kwetsbaarheden en bijbehorende oplossingen (patches) openbaar maakt. Door zeer snel de gepubliceerde kwetsbaarheden én de bijbehorende patches te analyseren, kan een aanvaller manieren ontwikkelen om die gevonden kwetsbaarheid te misbruiken en nog niet-gepatchte computers aan te vallen. Diverse anti-Israëlische groepen gebruiken deze aanvalsmethode en wisselen hierover onderling informatie uit.[31]

Pro-Hamas hackers bestookten voornamelijk Israëlische kranten- en mediawebsites. De grondstrijd werd vergezeld door cyberoorlogvoering die voornamelijk was gericht tegen websites die in die hectische periode snel cruciale informatie aan vooral de burgerbevolking konden verstrekken. Naast de media waren in mindere mate ook de softwareindustrie, de financiële sector, regeringswebsites en verschillende ziekenhuizen het doelwit van gerichte cyberaanvallen.[32]

Aan Palestijnse zijde was de financiële sector het voornaamste getroffen doelwit (76 procent van alle DDoS-aanvallen). De internetsector werd eveneens getroffen, maar Palestijnse media daarentegen vrijwel niet. Het feit dat veel meer cyberaanvallen waren gericht tegen Israëlische dan Palestijnse doelwitten, is waarschijnlijk een logisch gevolg van Israëls verregaande digitalisatie, waardoor het land automatisch een groter aanvalsoppervlak biedt.

Een stabiele internetverbinding was in Gaza al geen zekerheid, maar sinds de IDF de strook binnenviel, is de connectiviteit nog verder teruggelopen. Dit komt deels door fysieke schade van kinetische aanvallen op communicatienetwerken en internetdiensten, en deels door voortdurende uitval van elektriciteit. Aangezien de Palestijnse internet-infrastructuur nauwelijks *mobiele* internetdiensten kent, heeft schade aan het vaste netwerk ook direct gevolgen voor allerlei civiele diensten (waaronder medische). Op 17 januari 2024 werd een vrijwel volledige telecommunicatie black-out in de Gazastrook geconstateerd die zes dagen duurde.

Computers en computerprogramma's spelen overigens op nog een andere wijze een rol in dit conflict. De IDF gebruikt voor target selection

28 K.L Arnold en S. van Dorst, 'Wiperware: een nieuw cyberwapen voor de militaire toolbox?', *Militaire Spectator* 192 (2023) (11). Zie: https://militairespectator.nl/artikelen/wiperware-een-nieuw-cyberwapen-voor-de-militaire-toolbox.

29 Trustwave, 'Overview of the cyber warfare used in Israel-Hamas war', 5 december 2023. Zie: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyberwarfare-used-in-israel-hamas-war/.

30 De term n-day vulnerability is gebaseerd op een zero-day vulnerability: een kwetsbaarheid in een software (of hardware) product die kan worden uitgebuit vóórdat de maker van het product die kwetsbaarheid heeft verholpen. N-day vulnerabilities zijn kwetsbaarheden waarvoor (sinds een n-aantal dagen) oplossingen (patches) beschikbaar zijn. Echter, zolang een computersysteem niet tijdig wordt gepatcht, blijft het systeem kwetsbaar voor een cyberaanval. Door snel de gepubliceerde kwetsbaarheid én de bijbehorende patch te analyseren en te vergelijken, kan een aanvaller een manier ontwikkelen om die gevonden kwetsbaarheid te misbruiken om niet-gepatchte computers aan te vallen.

31 Israel National Cyber Directorate (INCD), 'Iron Swords' War in Cyber Sphere: Insights, Recommendations and Mitigations', 7 januari 2024, V1.0, 8.

32 'Health Ministry disconnects the remote connection of several hospitals following cyber attack', *Jerusalem Post*, 21 oktober 2023. Zie: https://www.jpost.com/breaking-news/article-769508.

onder meer kunstmatige intelligentie. Met computerprogramma's als *Where's Daddy*, *Lavender* en *The Gospel* identificeert en lokaliseert het leger uit te schakelen Hamas-strijders. Omdat dit evenwel besluitvormingsondersteunende programma's zijn en geen cyberoorlogvoering betreft, vallen deze programma's buiten de scope van dit artikel.

Digitale beïnvloeding

Toen Hamas-strijders op 7 oktober de aanval openden op Israël werden hun acties live gestreamd door strijders zelf en mediapersoneel dat met hen optrok. Beelden van gruwelijkheden, waaronder executies, werden live uitgezonden en verspreid via sociale media.[33] Dit past in een strategie waarbij cyberspace wordt benut voor psychologische oorlogsvoering en informatieoperaties. Publiciteit is dan ook een essentiële component voor het succes van een terroristische actie. Hamas heeft op ongekende schaal digitale middelen ingezet om dat schokeffect te bereiken.[34]

Ook Israël voert actief psychologische (beïnvloedings)operaties uit. De Influence Unit van de IDF plaatst verhalen in de pers om bewust de perceptie van de oorlog te sturen; niet alleen de publieke opinie, maar ook de tegenstander. Techbedrijven ontwikkelden digitale middelen om te meten hoe de publieke opinie reageert op de berichtgevingen van het leger.[35]

Op tactisch en operationeel niveau gaat dit conflict voornamelijk om raketten en kogels, en het daaruit voortvloeiende menselijk leed en zichtbare schade. Op strategisch niveau gaat de strijd evenwel om het beïnvloeden (manipuleren) van de bevolking; de perceptie van de publieke opinie en het politieke besluitvormingsproces. De te beïnvloeden doelgroep (targeted audience) bestaat niet alleen uit de eigen bevolking en de eigen politiek leiders, maar ook uit aanhangers, steunverleners en geldschieters buiten de regio; en politiek leiders wereldwijd. Voor beide strijdende partijen lijkt internationale steun het Centre of Gravity te zijn.[36] De (perceptie van) aantallen burgerslachtoffers zijn daarbij een luguber middel. Naast het verspreiden van 'zuivere feiten' hieromtrent spelen ook leugens, onjuistheden en regelrechte desinformatie een belangrijke rol bij de beeld- en meningsvorming. Dat dit gebeurt in een oorlog is niet nieuw, maar dankzij cyberspace (in dit geval de mogelijkheid dat 'ieder individu' zelf tekst, foto's en videobeelden kan maken, hergebruiken, vervalsen en online verspreiden) gaat dit tegenwoordig makkelijker, sneller, anoniemer, goedkoper en vooral heimelijker dan voorheen.

Hoe kunnen beïnvloedingsoperaties een rol spelen in het creëren van effecten zoals het veranderen van een mening, besluit en gedrag? Met een bepaalde intentie voor ogen, kiest een partij een strategisch narratief. Die overkoepelende verhaallijn wordt vervolgens geoperationaliseerd; opgesplitst in kleinere verhalen (frames). Framing heeft als doel het beoogde doelpubliek aan te zetten tot vooraf bepaalde beslissingen en acties die overeenkomen met wat de actor achter die beïnvloedingsoperatie wenst. Vooral sterk contrasterende waarden, normen en opvattingen zijn bij uitstek geschikt om tweespalt te creëren, of in stand te houden;[37] een ideaal concept in een gewapend conflict.

Volgens de 'gebruikelijke' verhaallijnen benadrukt de IDF het eigen gebruik van precisiewapens en het gebruik van burgers als menselijk schild door Hamas. Laatstgenoemde accentueert graag de menselijke ellende vanwege onophou-

33 N.n 'Hamas Attack on Israel: AP Photographer who accompanied terrorists wins award for clicking Shani Louk's half-naked body', *Organiser*, 29 maart 2024. Zie: https://organiser.org/2024/03/29/229969/world/hamas-attack-on-israel-ap-photographer-who-accompanied-terrorists-wins-award-for- clicking-shani-louks-half-naked-body/.

34 Veronica Neifakh, '4 Stages of Hamas' Psychological Warfare', *The Media Line*, 29 mei 2024. Zie: https://themedialine.org/top-stories/4-stages-of-hamas-psychological-warfare/.

35 Eric Cortellessa en Vera Bergengruen, 'Inside the Israel-hamas Information War', *Time Magazine*, 22 december 2023. Zie: https://time.com/6549544/israel-and-hamas-the-media-war/.

36 Het Centre of Gravity (zwaartepunt) is een militair concept dat verwijst naar de primaire bron waaraan een krijgsmacht zijn kracht ontleent om de strijd te kunnen voortzetten. De term is geïntroduceerd door Carl C. von Clausewitz in zijn werk *Vom Kriege (On War)*. Zie bijvoorbeeld M.E. Howard en P. Paret (red.), *On War* (Princeton University Press, 2008).

37 B.M.J. Pijpers en P.A.L. Ducheine, 'Influence Operations in Cyberspace – How They Really Work', Amsterdam Law School Research Paper No. 2020-61, Amsterdam Center for International Law No. 2020-31, 24 september 2020. Zie: https://ssrn.com/abstract=3698642.

delijke Israëlische aanvallen op Palestijnse burgers. Beelden die wreedheden en massale sterfgevallen tonen, worden evenwel vaak verspreid zonder de nodige context, waardoor het bijna onmogelijk is hun oorsprong te verifiëren. Aanhangers van beide zijden ge- of misbruiken moderne technologie en tonen, creëren, wijzigen en delen audio- en video-materiaal dat hun beweringen, frame en narratief moet ondersteunen.

Een dramatisch voorbeeld hiervan is de explosie nabij het Al-Ahli ziekenhuis waarbij naar verluidt honderden doden en gewonden vielen onder Palestijnse vluchtelingen die daar een veilig toevluchtsoord zochten. Hamas beschuldigde Israël en Israël beschuldigde Hamas.[38] Aanhangers van beide kanten brachten hun standpunten – en vermeend 'bewijsmateriaal' – via socialemediaplatforms naar voren om de publieke opinie en politieke beslissingen te beïnvloeden, waarbij ze dankbaar gebruikmaakten van de moeilijkheid om die bewijzen te weerleggen. Een vervalst bericht of gemanipuleerd beeld is, met dank aan kunstmatige intelligentie, tegenwoordig snel te maken. Bewijzen dat iets wel/niet authentiek is (factchecken), kost veel meer tijd. Dat dit uiteindelijk toch mogelijk is, bleek een maand na de explosie.[39]

Het gebruik van (sociale) media om de perceptie en besluitvorming van conflicten te beïnvloeden is geen noviteit, maar door dit conflict heeft deze vorm van digitale oorlogvoering wel een ongeëvenaard niveau bereikt in omvang en intensiteit. Dat geldt niet alleen voor real-time gegevens, maar ook voor bewust gemanipuleerde informatie. Met kunstmatige intelligentie gemaakte beelden hebben het potentieel om het vertrouwen van het publiek in *alle* verspreide informatie te ondermijnen. Wetende dat audio, video- en ander beeldmateriaal kan worden vervaardigd met computersoftware, kan zelfs authentiek materiaal al snel worden bestempeld als 'fake'. Het resultaat is een virtueel slagveld waar online polarisatie nieuw geweld kan aanwakkeren.[40]

Soms komen cyberaanvallen en digitale beïnvloedingsoperaties samen. Hackergroep *CyberAv3ngers* claimde een cyberaanval op een Israëlische energiecentrale en deelde foto's van de vermeende hack met daarbij een Palestijnse vlag en politieke boodschappen. Daarmee suggereerden de aanvallers dat deze computeraanval was uitgevoerd ter ondersteuning van de Palestijnse zaak. De gegevens waren echter afkomstig van een eerdere cyberaanval (2022); destijds uitgevoerd door een andere hackergroep en voor een ander doel.[41]

Meer dan twee strijdende partijen

Eind oktober 2023 waren 116 hackergroepen actief betrokken bij de cyberoorlogvoering tussen Hamas en Israël. Het merendeel (90) daarvan was pro-Palestijns, opereerde voornamelijk vanuit Azië en het Midden-Oosten en had aantoonbare religieuze motieven.[42] Opvallend is dat ook enkele beruchte pro-Russische hackergroepen zich achter Hamas zaak leken te scharen. Zij opereerden althans tegen Israël.[43] Dat land vond 23 hackergroepen aan zijn zijde. Drie hackergroepen bestempelden zichzelf als onpartijdig. Zij bestookten beide vechtende partijen.[44] Tegen het einde van 2023 steeg het aantal betrokken hackerscollectieven naar 133; het merendeel pro-Hamas.

38 Todd C. Helmus en William Marcellino, 'Lies, Misinformation Play Key Role in Israel-Hamas Fight', Rand Corporation, 31 oktober 2023. Zie: https://www.rand.org/blog/2023/10/lies-misinformation-play-key-role-in-israel-hamas-fight.html.

39 Amerikaanse en Franse inlichtingendiensten alsook onafhankelijke factcheckers van Associated Press kwamen tot de conclusie dat de explosie (waarschijnlijk) is veroorzaakt door een afgedwaalde raket, afgevuurd vanuit Gaza. Bron: Michael Biesecker, 'New AP analysis of last month's deadly Gaza hospital explosion rules out widely cited video', 22 november 2023. Zie https://apnews.com/article/israel-palestinians-hamas-war-hospital-rocket-gaza-e0fa550faa4678f024797b72132452e3.

40 P.W. Singer en Emerson T. Brooking, 'Gaza and the Future of Information Warfare. The Digital Front of the Israel-Hamas Conflict Is a Preview of Fights to Come', *Foreign Affairs*, 5 december 2023. Zie: https://www.foreignaffairs.com/middle-east/gaza-and-future-information-warfare.

41 N.n., 'A hack in hand is worth two in the bush', *Kaspersky SecureList*, 16 oktober 2023. Zie: https://securelist.com/a-hack-in-hand-is-worth-two-in-the-bush/110794/.

42 M. Sahariya, 'The Evolving Landscape of Cyber Warfare in the Israel-Palestine: A Comprehensive Analysis', *Falconfeeds*, 18 oktober 2023. Zie: https://falconfeeds.io/blog/post/the-evolving-landscape-of-cyber-warfare-in-the-israelpalestine-conflict-a-comprehensive-analysis–356011.

43 Tanner Wagner, 'Escalation of Threats in the Middle East', CyberPeace Institute, 6 november 2023. Zie: https://cyberpeaceinstitute.org/news/escalation-of-threats-middle-east.

44 Jurgita Lapienytė, 'Hacktivists in Palestine and Israel after SCADA and other industrial control systems', *Cybernews*, 15 november 2023. Zie: https://cybernews.com/cyber-war/palestine-israel-scada-under-attack/.

FOTO U.S. CYBER COMMAND

Het U.S. Cyber Command is 'always in the fight'. Meerdere partijen houden zich op in de 'regionale cyberspace' in het Midden-Oosten, en van het U.S. Cyber Command is bekend dat het, sinds het oplaaien van het recente conflict, Israël actief steunt

Verschillende activistische hackergroepen benutten online communicatieplatforms, zoals Telegram, om medestanders te mobiliseren, specifieke doelwitten aan te wijzen en de kwetsbaarheden daarin te openbaren, alsook kwaadaardige softwareprogramma's te delen, waarmee anderen vervolgens cyberaanvallen kunnen uitvoeren.[45] In een poging de dreiging van dergelijke vijandige hackergroepen te neutraliseren, infiltreerde het Israëlische cybersecuritybedrijf Radware heimelijk in verscheidene (online) communities van Telegram. Medewerkers van het bedrijf deden zich voor als sympathisanten die zich wilden mengen in de strijd tegen Israël. Aldus verkreeg het bedrijf inzicht in aanvalsmethoden en technieken van deze hackers, en de rationale achter hun doelkeuzes. Door de kwaadaardige software te analyseren, konden potentiële slachtoffers tijdig worden voorzien van tegenmaatregelen.[46]

Het gezelschap dat zich toelegt op cyberoorlogvoering is behoorlijk divers en dat geldt ook voor het soort cyberaanvallen. Ideologisch gedreven activistische hackers gebruiken veelal vervelende, maar relatief onschadelijke DDoS-aanvallen, hack-and-leak-operaties en defacements, waarmee zij een politieke of religieuze boodschap afgeven. Aangezien de aanvallers doorgaans bewust de publiciteit zoeken om hun actie te claimen, worden dergelijke aanvallen snel ontdekt. Daarnaast zijn ze hierdoor vrij eenvoudig te attribueren aan een specifieke dader. Dit staat in schril contrast met meer substantiële, heimelijke cyberaanvallen, waarbij aanvallers trachten ontdekking van hun identiteit of achterliggende intenties te verhullen. Niet vreemd dus dat een deel van de pro-Palestijnse

45 Steve Emerson, 'An Analysis of the Israel-Palestine Conflict from a Cybersecurity Perspective, October 2023', *Medium*, 5 november 2023. Zie: https://blogs.crushingsecurity.com/an-analysis-of-the-israel-palestine-conflict-from-a-cybersecurity-perspective-october-2023-858c4c20f0ac.

46 Sara Miller, 'Infiltrating Anti-Israel Cyber Attackers To Hunt Their Targets & Tools', *NoCamels*, 23 november 2023. Zie: https://nocamels.com/2023/11/infiltrating-anti-israel-cyber-attackers-to-hunt-their-targets-tools/.

en pro-Israëlische cyberaanvallen niet is geclaimd door de aanvallers.

Hieruit zou je kunnen opmaken dat naast de activistische hackers nog een ander type aanvaller actief is: statelijke of staatsgesteunde actoren (APT's).[47] In het huidige conflict zouden aan Hamas, Hezbollah of Iran gelieerde APT's zich goed kunnen voordoen als activistische hackergroepen en zich met de (cyber)strijd in Gaza kunnen bemoeien om hun identiteit en werkelijke intenties te verhullen.[48] Daarnaast is het echter ook mogelijk dat andere landen zich heimelijk ophouden in de 'regionale cyberspace'. Hetzij om inlichtingen te vergaren, hetzij om een van de strijdende partijen actief te steunen (defensief en/of offensief). Van het U.S. Cyber Command is bekend dat het, sinds het oplaaien van het recente conflict, Israël actief steunt op dit gebied.[49]

Ook de technologisch geavanceerde, pro-Israëlische hackergroep *Predatory Sparrow* is opgedoken in het huidige cyberconflict. Deze actor, waarschijnlijk gelieerd aan de Israëlische overheid, heeft in het verleden naar verluidt verschillende destructieve en spraakmakende cyberaanvallen uitgevoerd in Iran.[50] De groep, vermoedelijk verantwoordelijk voor een cyberaanval op het Iraanse spoorwegennetwerk in 2021, en op een staalfabriek in 2022, beweerde dit keer de website van het Iraanse overheidsnieuwsagentschap ontoegankelijk te hebben gemaakt; op zijn minst tijdelijk.[51] Meerdere Israëlische (tech)bedrijven spannen zich overigens in op zoek naar aanwijzingen over het lot van de Israëlische gijzelaars en hun verblijfplaats.[52] Ook de Israëlische *NSO Group Technologies* is actief op dit gebied.

Het pro-Israëlische hackerscollectief *WeRedEvils* claimde het Iraanse elektriciteitsnet en kernreactoren te hebben gehackt, alsook faciliteiten van de Iraanse Revolutionaire Garde en de Iraanse website *Tasnim News*. Hoewel Iran geen stroomstoringen meldde, deelden de aanvallers een uitgebreide verzameling bestanden inzake de genoemde digitale inbraken. Dezelfde groep zou daarnaast verantwoordelijk zijn voor een cyberaanval op het pro-Hamas Telegram-kanaal *GazaNow*.[53]

Opvallende afwezigen in de eerste dagen van dit cyberconflict waren de notoire hackergroepen van de Iraanse veiligheidsdiensten en de Revolutionaire Garde. De vraag daarbij is of Teheran zich bewust afzijdig hield van dit cyberconflict, of dat zijn cybereenheden simpelweg niet waren voorbereid op de inzet van cyberwapens ter ondersteuning van Hamas' inval. Iraanse operators leken initieel vooral reactief te zijn. Dat wil zeggen, zij gebruikten reeds aanwezige toegang tot systemen van hun slachtoffers, alsook bestaande digitale infrastructuur en middelen. Pas elf dagen na de fysieke inval van Hamas werden twee afzonderlijke cyberaanvallen vanuit Iran waargenomen. Beide gericht tegen Israëlische infrastructuur en met een destructief oogmerk. Deze incidenten hadden weliswaar slechts beperkte (bewezen) effecten, maar de aanvallers trachtten via online beïnvloedingsoperaties het succes en de impact van beide aanvallen uit te vergroten.[54]

47 Een Advanced Persistent Threat (APT) is een dreiging die wordt gevormd door een hackerscollectief met uiteenlopende specialismen. Een dergelijke groep is vaak in staat om ongemerkt een computersysteem of -netwerk binnen te dringen en daar een langere periode ongemerkt te blijven om informatie te verzamelen. De meeste van dit soort groepen betreffen statelijke, staatsgesteunde, of staats-gedoogde (criminele) actoren die tot doel hebben andere regeringen te ondermijnen.

48 Tom Hegel en Aleksandar Milenkoski, 'The Israel-Hamas War |Cyber Domain State-Sponsored Activity of Interest', *SentinelOne*, 24 oktober 2023. Zie: https://www.sentinelone.com/labs/the-israel-hamas-war-cyber-domain-state-sponsored-activity-of-interest/.

49 General Timothy D. Haugh, Commander U.S. Cyber Command, 'Posture Statement of Timothy D. Haugh 2024', 12 april 2024. See: https://www.cybercom.mil/Media/News/Article/3739700/posture-statement-of-general-timothy-d-haugh-2024/.

50 Farnaz Fassihi en Ronen Bergman, 'Israel and Iran Broaden Cyberwar to attack Civilian Targets', *The New York Times*, 27 november 2021. Zie: https://archive.ph/30DGG.

51 AJ Vicens, 'Savvy Israel-linked hacking group re-emerges amid Gaza fighting', *CyberScoop*, 10 oktober 2023. Zie: https://cyberscoop.com/predatory-sparrow-israel-gaza-cyber/.

52 David Swan, 'Cyber Intelligence Report 10 – 23 November 2023', CSCIS (Centre for Strategic Cyberspace & International Studies), 23 november 2023. Zie: https://cscis.org/2023/11/24/cyberwarfare-how-russia-hacked-denmark/.

53 David Israel, 'Israeli Hackers Claim They Shut Down Revolutionary Guards' Nuclear Projects', *The Jewish Press*, 24 oktober 2023. Zie: https://www.jewishpress.com/news/middle-east/iran-news/israeli-hackers-claim-they-shut-down-revolutionary-guards-nuclear-projects/2023/10/24/.

54 N.n., 'Reactive and opportunistic: Iran's role in the Israel-Hamas war', *Microsoft Threat Intelligence blog*, 9 november 2023. Zie: https://www.microsoft.com/en-us/security/blog/2023/11/09/microsoft-shares-threat-intelligence-at-cyberwarcon-2023/.

Een van de hackergroepen lijkt sterk verbonden aan de Iraanse APT *Agonizing Serpens*. Deze groep richt zijn kwaadaardige software (malware) voornamelijk op Israëlische doelwitten in uiteenlopende industrieën en verschillende landen.[55] De aanvallers maakten voor hun destructieve cyberwapen gebruik van één oude en drie nieuwe wiperware-versies, om data én computers van hun slachtoffers permanent te vernietigen. Behalve meerdere wiperware-varianten gebruikten de hackers ook stealth en andere technieken om (cyber)verdedigings-maatregelen te omzeilen, ongemerkt te opereren en hun eigen digitale sporen uit te wissen. Hoewel de aanvallen (tijdig) zijn onderkend, toont dit de toegenomen capaciteit van deze aanvallers.

Naarmate het conflict voortduurt, willen Iraanse partijen wellicht een pro-actievere houding aannemen. Echter, het doelkeuzeproces en het verkrijgen van toegang tot specifieke doelwitten vergt doorgaans veel tijd. Om ongemerkt een computernetwerk binnen te dringen en daar gedurende langere tijd ongemerkt te verblijven (bijvoorbeeld om inlichtingen te verzamelen), is specifiek ontwikkelde (tailored to the mission) software nodig. Aangezien die software specifiek wordt afgestemd op een bepaald doelwit, heeft die een beperkte herbruikbaarheid wat betreft inzet tegen willekeurige andere doelwitten. Dit maakt dat specifieke intelligence gathering-software minder geschikt is om snel om te bouwen naar tactisch of operationeel bruikbare cyberwapens die kunnen worden ingezet tegen verschillende doelwitten.

Geopolitiek cyberconflict

Hoewel de naam anders doet vermoeden, is hackerscollectief *Anonymous Sudan* geen onder-afdeling van het activistische hackerscollectief *Anonymous*, en evenmin Sudanees. Het betreft vermoedelijk een groep die nauwe banden onderhoudt met Rusland.[56] Binnen een uur na de initiële raketaanvallen van Hamas op Israël voerde de groep samen met hackers van *AnonGhost* cyberaanvallen uit. Ze claimden daarbij Israëls Iron Dome-luchtverdedigings-systeem te hebben gecompromitteerd, evenals Israëls RedAlert-raketwaarschuwings-programma; een app die voornamelijk burgers voorziet van real-time gegevens over inkomende raketten.[57] Een van de gevolgen was dat gebruikers van de RedAlert-app valse berichten ontvingen over nucleaire wapens. De makers van de RedAlert-app werden gelijktijdig bestookt met DDoS-aanvallen, waardoor de producent voor langere tijd online onbereikbaar was. Een andere pro-Russische hackergroep (*KillNet*) richtte zich, uit wraak voor Israëls steun aan Oekraïne, op Israëlische overheidswebsites en financiële instellingen.[58]

In tegenstelling tot het kinetisch gevecht dat zich beperkt tot een specifieke geografische regio, vindt de conflict-gerelateerde cyber-oorlogsvoering ook elders plaats. Aanvallers en slachtoffers bevinden zich (ver) buiten de conflictzone. Meerdere hackergroepen richtten hun pijlen op derde landen (zoals de VS, India en Frankrijk), voornamelijk als reactie op de steun van die landen aan Israël. Hackergroep *CyberAv3ngers,* gelieerd aan de Iraanse Revolutionaire Garde, viel meerdere (civiele) Industriële Controle Systemen (ICS) aan; systemen die veelal onderdeel zijn van de vitale infrastructuur van een land. *CyberAv3ngers* claimde tevens, deels terecht, deels gefingeerd, cyberaanvallen op verscheidene Israëlische industriële sectoren (water, energie, scheepvaart en logistiek). Diezelfde groep viel bovendien drinkwatervoor-zienings- en waterzuiveringsinstallaties aan in meerdere Amerikaanse staten. De aanvaller legitimeerde die aanvallen met de quote 'Every Equipment "Made in Israel" is Cyber Av3ngers Legal Target!'[59] Een korte zoekslag op internet leert overigens dat het specifiek aangevallen

55 Or Chechik, Tom Fakterman, Daniel Frank en Assaf Dahan, 'Agonizing Serpens (Aka Agrius) Targeting the Israeli Higher Education and Tech Sectors', *Palo Alto Unit 42*, 6 november 2023. Zie: https://unit42.paloaltonetworks.com/agonizing-serpens-targets-israeli-tech-higher-ed-sectors/.

56 Vilius Petkauskas, 'Anonymous Sudan: neither anonymous nor Sudanese', *Cybernews*, 23 june 2023. Zie: https://cybernews.com/editorial/anonymous-sudan-explained/.

57 M. Sahariya, 'The Evolving Landscape of Cyber Warfare in the Israel-Palestine'.

58 Ryan Gallagher en Jordan Robertson, 'Cyberattacks Targeting Israel Are Rising After Hamas Assault', *Time Magazine,* 10 oktober 1023. Zie: https://time.com/6322175/israel-hamas-cyberattacks-hackers/.

59 Zie: https://twitter.com/CyberAveng3rs/status/1728743948246569469.

Israëlische computeronderdeel voorkomt in nog eens 1800 apparaten wereldwijd;[60] alle dus potentieel doelwit.

Volgens het Israëlische Nationale Cyberdirectoraat (INCD) hebben meer dan vijftien, aan Iran en Hezbollah gelieerde, statelijke en staatsgesteunde hackergroepen cyberaanvallen uitgevoerd op Israëls vitale diensten en infrastructuur. Het INCD constateerde dat tegenstanders ook verscheidene doelgroepen (waaronder anti-Israëlische activisten) aanspoorden om cyberaanvallen op Israël uit te voeren door hen te voorzien van specifieke doelwitten alsook de benodigde middelen voor bijvoorbeeld DDoS-aanvallen; ook te gebruiken zonder technische kennis.[61] Het aantal cyberaanvallen op Israël is sinds 7 oktober verdrievoudigd, mede doordat Iran en zijn proxies (waaronder Hezbollah) hun inspanningen coördineerden. Dat de aanvallen weinig schade aanrichtten, dankt Israël naar eigen zeggen aan zijn proactieve cyberdefensie. Deze aanpak ontleende het land aan de bevindingen in de cyberoorlogvoering tussen Rusland en Oekraïne. De aldaar geleerde lessen betreffen voornamelijk een intensieve samenwerking met industriële en internationale partners, het delen van cyberdreigingsinformatie en voorzorgsmaatregelen tegen dreigende cyberaanvallen.[62]

Ook pro-Israëlische hackers opereren over de grens. Vermoedelijk in reactie op de Iraanse bemoeienis met het conflict voerde hackergroep *Predatory Sparrow* een cyberaanval uit op Iraanse benzinestations waardoor zo'n 70 procent daarvan (tijdelijk) niet meer werkte.[63] Iran kreeg twee jaar eerder een soortgelijke cyberaanval op de brandstofvoorziening te verduren; destijds vermoedelijk uitgevoerd door hackers vanuit Israël en de VS.

Het Gaza-conflict lijkt daarmee onderdeel van een grotere machtsstrijd om invloed in het Midden-Oosten en het streven naar een multipolaire wereld met meerdere machtsblokken. Daarbij spelen ook andere dan rechtstreeks betrokken partijen een rol, zoals China[64] en Rusland.[65]

Conclusie

Sinds 2009 maken Hamas en Israël gebruik van sociale media om hun strijd ook online uit te vechten. Tot 2014 beperkte de cyberoorlog zich voornamelijk tot digitale beïnvloeding (soft cyberoperaties). Vanaf dat jaar richtten aanhangers van beide zijdes zich ook op het hacken van computers (hard cyberoperaties), al richtten die cyberaanvallen (voor zover momenteel te achterhalen) slechts beperkte, herstelbare schade aan. Hamas bleek zich de afgelopen jaren vooral te hebben bekwaamd in cyberspionage om zich voor te bereiden op '7 oktober'. Tot die datum was de Israëlische perceptie dat Hamas, in vergelijking met Rusland of China, geen serieuze cyber- of inlichtingendreiging vormde. Dit was een pijnlijke inschattingsfout. Een sterk gedigitaliseerde staat kan online onconventioneel worden bevochten en ondermijnd zonder daar adequate maatregelen tegenover te kunnen stellen.

In het huidige conflict heeft cyberoorlogvoering door (aanhangers van) beide strijdende partijen, voor zover bekend, nog geen doorslaggevende rol gespeeld. Duidelijk is wel dat de virtuele oorlogvoering ook, of juist, plaatsvindt *buiten* het specifieke gebied waar de grootste fysieke schade wordt aangericht. De meeste aanvallers én slachtoffers van cyberaanvallen bevinden zich juist buiten Gaza.

60 Het aangevallen onderdeel betrof een Programmable Logic Controller (PLC) van het Israëlische bedrijf Unitronics. Een PLC is een microcomputer die industriële machines en processen aanstuurt. Pierluigi Paganini, 'Iranian hacker group Cyber Av3ngers hacked the Municipal Water Authority of Aliquippa in Pennsylvania', *Security Affairs*, 27 november 2023. Zie: https://securityaffairs.com/154818/hacktivism/cyber-av3ngers-hacked-municipal-water-authority-of-aliquippa.html.

61 INCD, 'Iron Swords' War in Cyber Sphere', 5.

62 Wechsler, 'The Cyberwarfare Front of the Israel-Gaza War'.

63 N.n, 'Iran petrol stations hit by cyberattack, oil minister says', *Reuters*, 18 december 2023. Zie: https://www.reuters.com/world/middle-east/software-problem-disrupts-iranian-gas-stations-fars-2023-12-18/.

64 National Contagion Research Institute, 'A Tik-Tok-ing Timebomb: How TikTok's Global Platform Anomalies Align with the Chinese Communist Party's Geostrategic Objectives', *Intelligence Report*, december 2023.

65 Maria Shamrai, 'How Russia uses the Israel-Gaza Crisis in its disinformation campaign against the West', International Centre for Counter-Terrorism (ICCT), 8 december 2023. Zie: https://www.icct.nl/publication/how-russia-uses-israel-gaza-crisis-its-disinformation-campaign-against-west.

FOTO ANP ATEF SAFADI

Israëls luchtverdedigingssysteem Iron Dome in actie. Een hackergroep claimde Iron Dome en de waarschuwingsapp RedAlert te hebben gecompromitteerd

Het hacken van computersystemen speelt een ondersteunende rol in deze strijd. Het beïnvloeden van de publieke opinie en politieke besluitvormers lijkt een cruciale rol te spelen. Dankzij moderne technologie (sociale media in combinatie met kunstmatige intelligentie) kan informatie over de strijd niet alleen eenvoudig worden gemaakt en verspreid, maar ook hergebruikt of ronduit vervalst. Het Centre of Gravity lijkt voor beide strijdende partijen de internationale steun te zijn. Burgerslachtoffers zijn een luguber middel in de strijd om perceptie.

Twee op het eerste gezicht niet-gerelateerde conflicten (Rusland-Oekraïne en Hamas-Israël) zijn in zeker opzicht toch met elkaar verbonden dankzij Iran. Rusland ontvangt wapens (zoals drones) en munitie vanuit dat land en levert in ruil daarvoor digitale capaciteiten, die Iran inzet om de Palestijnse zaak via cyberoorlogvoering te beïnvloeden.

Rusland ontwikkelde meerdere destructieve cyberwapens (wiperware) die het inzette tegen Oekraïne. Gaandeweg konden Russische hackers bestaande wiperware snel modificeren, verbeteren en inzetten tegen nieuwe doelwitten. Als het Gaza-conflict voortduurt, zou ook Iran nieuwe, meer agressieve cyberwapens kunnen ontwikkelen en inzetten tegen Israël of zijn bondgenoten.

Online activisme kan een bruikbare dekmantel vormen. Irans statelijke of staatsgesteunde cybergroepen kunnen cyberaanvallen uitvoeren zonder eenvoudig als dader te worden herkend. Dergelijke cyberaanvallen zullen dit kinetisch reeds geëscaleerde conflict waarschijnlijk niet verder doen verslechteren en evenmin zullen cyberwapens de doorslaggevende factor vormen in de strijd.

Door zich actief te mengen in deze cyberstrijd kunnen andere landen niet alleen een van beide strijdende partijen van dienst zijn, maar bovenal hun eigen geopolitieke strategische doelen nastreven. Als de fysieke strijd rond Gaza eenmaal is geluwd, zal het cyberconflict ongetwijfeld voortduren. Verscheidene landen zullen in een constant (cyber)conflict met elkaar verwikkeld blijven. ■