Soft-cyber politieoperaties

Digitale beïnvloedingsoperaties bij de politie en lessen voor de krijgsmacht

Jim van Zon en Peter Pijpers*

De politie behoort tot de overheidsorganisaties die soft-cyberoperaties, ook wel beïnvloedingsoperaties genoemd, uitvoeren. Defensie behoort daar niet toe: in vredestijd is de krijgsmacht niet gerechtigd op te treden in de informatieomgeving. Dit artikel gaat in op de bestrijding van online criminaliteit door de Nationale Politie. Wat houden de cyberoperaties van de politie in, en welke lessen zijn er voor de krijgsmacht?

* Kapitein Jim van Zon is werkzaam als reservist bij 519 Squadron als Executive Officer; brigade-generaal prof. dr. Peter Pijpers is hoogleraar cyberoperaties aan de Faculteit Militaire Wetenschappen van de Nederlandse Defensie Academie.

De Nederlandse politie is zeer actief in het cyberdomein, ook met beïnvloedingsoperaties. Dergelijke operaties leveren veel ervaring op. Ervaring die ook interessant kan zijn voor de krijgsmacht.

De afgelopen jaren stonden er geregeld artikelen in de *Militaire Spectator* over (componenten van) beïnvloedingsoperaties via cyberspace, ook wel soft-cyberoperaties genoemd.[1] Recent verscheen ook de *Defensie Cyberstrategie 2025*[2] waarin Defensie de permanente proactieve inzet tegen

1 Zie: Peter Schrijver en Paul Ducheine, 'Cyber-Enabled Influence Operations. The case of the Belarusian Cyber Partisans', *Militaire Spectator* 192 (2023) (6) 284-295; Willemijn A. Bos en Peter B.M.J. Pijpers, 'Cyberoperaties in de gray zone. Juridische overwegingen omtrent de rol voor de krijgsmacht', Militaire Spectator 190 (2021) (10) 508-521; Adelbert Bronkhorst en Frans Osinga 'Een nieuwe Militaire Revolutie? Technologische trends, Oekraïne en de toekomst van oorlog. Deel 2: 2014-2022: Een nieuwe koude oorlog, een nieuwe RMA (?)' *Militaire Spectator* 194 (2025) jubileumeditie 20-35.

2 Ministerie van Defensie, 'Defensie Cyberstrategie 2025' (2025), zie: https://www.defensie.nl/actueel/nieuws/2025/10/03/defensie-vergroot-slagkracht-in-cyberdomein.

CREDIT: FOTO ANP

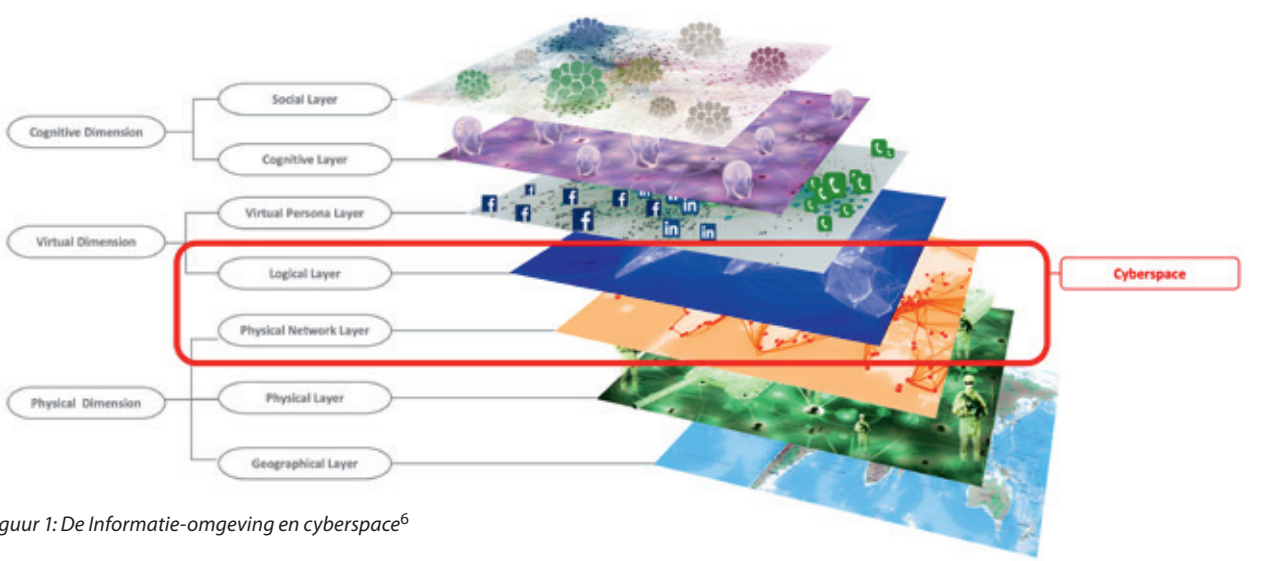
agressieve cyberactoren ambieert,[3] en de synergie met publieke en private partijen, en bondgenoten. Opvallend is de afwezigheid van beïnvloedingsoperaties via cyberspace. De reden hiervoor kan zijn het gebrek aan mandaat en operationele mogelijkheden voor de krijgsmacht om soft-cyberoperaties uit te voeren. Buiten de krijgsmacht zijn er diverse overheidsorganisaties die deze operaties, passend in het raamwerk van soft-cyber, wel uitvoeren. Een van die organisaties is de politie, een partner in de publieke sector.
Dit artikel gaat in op de bestrijding van online criminaliteit door de Nationale Politie. Dit geeft niet alleen inzicht in deze cyberoperaties, maar ook in ervaringen en mogelijke kansen voor de krijgsmacht.

Eerst lichten wij soft-cyber binnen de krijgsmacht toe en beschrijven we de stand van zaken. Vervolgens benoemen we de taakstelling en visie vanuit de politie, waarna het thema 'brede bestrijding' aan bod komt in relatie tot cybercrime. Tot slot zetten we diverse politieoperaties uiteen die relevant zijn voor de krijgsmacht.

Soft-cyber theoretisch kader

Soft-cyberactiviteiten kennen twee elementen, 'soft' en 'cyber'. Cyberspace, als eerste, is een onderdeel van de informatieomgeving. Dit is feitelijk de omgeving waarin we leven, en waar we informatie (data, inlichtingen) uit halen of kunnen 'injecteren' (denk aan een nieuwsbericht, propaganda of reclame).[4] Met de opkomst van cyberspace is deze informatieomgeving uitgebreid; niet alleen zijn er drie lagen bijgekomen (de fysieke netwerklaag van computers, de software (*code*) en onze virtuele personages op sociale media-accounts (de *content*)). Cyberspace is daarnaast toegankelijk en beschikbaar voor een veel breder publiek dan enkel staten. Filters of tussenpersonen zoals overheid, een krant of andere traditionele media zijn verdwenen, met alle gevolgen van dien – cyberspace en internet zorgen voor een grote mate van democratisering, maar tegelijkertijd vallen nuancering en onderbouwing bij berichtgeving weg.[5]

3 De Cyberstrategie zegt hierover: 'Defensie wil haar cyberslagkracht op een doorslaggevende wijze in kunnen zetten, zowel in de huidige 'grijze zone' tussen oorlog en vrede als in het scenario van gewapend conflict. Hiervoor introduceert Defensie een nieuwe koers: een permanente proactieve cyberinzet om meer offensief tegendruk te geven'. Zie hiervoor ook de boekbespreking van Sebastian Reyn en Alexander Claver van *Cyber Persistent Theory* van Michael P. Fischerkeller, Emily O. Goldman en Richard J. Harknett, *Militaire Spectator* 193 (2024) (12) 738-739.
4 Marije Timmer en Paul A.L. Ducheine, 'Conceptual Manoeuvring', Militaire Spectator 192 (2023) (11) 542-555.
5 Thomas Zeitzoff, 'How Social Media Is Changing Conflict' (2017) 61 Journal of Conflict Resolution 1970.
6 Figuur is gemaakt door Jelle van Haaster, zie ook: Jelle van Haaster, 'On Cyber: The Utility of Military Cyber Operations During Armed Conflict' (2018) 173 (noot 898).



Figuur 1: De Informatie-omgeving en cyberspace[6]

Recent verscheen de *Defensie Cyberstrategie 2025*, waarin Defensie de permanente proactieve inzet tegen agressieve cyberactoren ambieert

'Soft' refereert aan de term *soft power*. Nye beschrijft dat als 'a nation's capacity to sway others without resorting to coercive measures'.[7] Soft power komt tot uiting door *agenda setting*,[8] de aantrekkelijkheid van samenwerken (alliantievorming) en overtuigen op basis van waarden (in plaats van dwang). Soft power beïnvloedt de perceptie van vijandelijke (en neutrale) actoren door gebruik te maken van narratieven en frames, of zoals Winder stelt: 'soft power is (…) a storytelling competition'.[9] Indien staten deze narratieven inzetten als strategisch instrument ontstaan er concurrerende regio's of coalities van staten die hun eigen waarden niet naast die van andere zetten maar erboven, en daarmee tegelijk alternatieve narratieven in diskrediet brengen.

Soft-cyber operaties staat tegenover hard-cyber operaties. Hoewel ze allebei vormen van militair gebruik van cyberspace zijn, richten hard-cyberoperaties zich op de lagen *in* cyberspace – de computers, de code of de content. Bij een hard-cyberoperatie raken de lagen – met name de data (code) – in cyberspace beschadigd, waardoor ook een computer niet meer functioneert. Staten gebruiken daarvoor digitale 'wapens' zoals *malware* of de eenvoudige *distributed denial-of-service* (DDoS) aanval om de vertrouwelijkheid, integriteit of beschikbaarheid van de virtuele of fysieke netwerklagen in cyberspace te saboteren.
Recente voorbeelden zijn de *ransomware*-aanvallen die data gijzelen, en de *wiperwares* die Rusland in Oekraïne inzette.[10]

Soft-cyber (beïnvloedings-)operaties richten zich niet op doelen in cyberspace, maar gebruiken cyberspace als een vector om de cognitie van individuen of groepen te bereiken. De soft-cyberoperatie heeft tot doel het overtuigen of manipuleren om het gedrag op bewuste of onbewuste wijzen te beïnvloeden. Manipulatieve beïnvloedingsoperaties maken gebruik van het beperkte rationele vermogen van het brein. Door een tekort aan tijd of een overschot (of tekort) informatie valt het menselijk brein terug op *biases* en heuristieken, ofwel mentale snelkoppelingen om situaties intuïtief aan te kunnen (denk aan vluchtgedrag), in plaats van een weloverwogen rationele besluitvorming. Biases, zoals de conformiteitsbias of de autoriteitsbias, vormen het kennisdomein van de cognitieve psychologie dat sinds de Tweede Wereldoorlog een enorme vlucht genomen heeft in politieke redevoeringen en in de reclamewereld. Maar ook tijdens conflicten en in oorlog is deze vorm van beïnvloeding en misleiding niet ongewoon. De 'wapens' zijn in dit geval niet de code, maar het zijn woorden en beelden (content). Woorden richten niet direct schade aan, maar kunnen in een specifieke context polariserend zijn en tweedracht in een samenleving zaaien.

Kennis van cognitieve psychologie in combinatie met de opkomst van cyberspace zorgt voor een toegenomen bruikbaarheid van beïnvloedingsoperaties – waaronder desinformatie operaties. De oorzaak van het neerstorten van MH17 in 2014 ging gepaard met grootschalige misleidende berichtgeving. Daarnaast vinden bij verkiezingen veelvuldig digitale desinformatie-

7 Joseph S. Nye, 'Soft Power. The Evolution of a Concept', *Journal of Political Power* 14 (2021) 196.
8 Het gaat om het beïnvloeden van de politieke agenda, en daarmee zorgen dat deze thema's publieke aandacht krijgen. Zie ook Maxwell E. McCombs en Donald L. Shaw 'The Agenda-Setting Function of Mass Media', *The Public Opinion Quarterly* 36 (1972) 2.
9 Robert Winder *Soft Power. The New Great Game* (New York, Little, Brown Book Group, 2020).
10 Kraesten L. Arnold en Sander van Dorst, 'Wiperware: een nieuw cyberwapen voor de militaire toolbox?' *Militaire Spectator* 192 (2023) (11) 512-525.

operaties plaats, en ook rondom de oorlog in Oekraïne zijn soft-cyberoperaties een geliefd instrument.[11]

Soft-cyber binnen Defensie – de problematische gereedstelling

Hoewel menige krijgsmacht actief is in de informatieomgeving en in cyberspace,[12] is de inzet van de Nederlandse krijgsmacht in de informatieomgeving geen vanzelfsprekendheid.[13] De doelomschrijving van de krijgsmacht geeft weliswaar aan dat de krijgsmacht de vitale belangen te allen tijde en overal dient te beschermen, maar de wettelijke kaders leggen de krijgsmacht aanzienlijke beperkingen op. In vredestijd is de krijgsmacht niet in staat op te treden in de informatieomgeving, enkel de MIVD (wier capaciteit niet ongelimiteerd is) kan dat doen. Beperkingen die opponenten zoals China of Rusland, die Nederland in vredestijd aanvallen via cyberspace, niet hebben.[14]

De Militaire Inlichtingen- en Veiligheidsdienst maakt weliswaar deel uit van Defensie, maar is geen onderdeel van de krijgsmacht. De MIVD ressorteert onder de Secretaris-Generaal en niet onder de Commandant der Strijdkrachten. De beide inlichtingendiensten MIVD en AIVD vallen daarnaast onder een specifiek juridisch regime, de Wet op de Inlichtingen- en Veiligheidsdiensten (Wiv 2017).

De reden dat de krijgsmacht niet kan optreden is gekoppeld aan de privacywetgeving vanuit de EU, de zogeheten Algemene Verordening Gegevensbescherming (AVG).[15] Deze AVG is een waardevolle wet die directe rechtskracht heeft in Nederland en daarom ook de soevereine gebieden waar de EU geen rechtsmacht heeft – zoals Buitenlandse Zaken en Defensie – buiten beschouwing laat. De idee achter de AVG is dat men enkel op grond van vooropgestelde wettelijke bepalingen van privacyregels mag afwijken. De EU-lidstaten moeten dus zelf een wet maken waarin ze het inperken van de privacyregels vastleggen voor onder meer de krijgsmacht.

Nederland heeft er echter voor gekozen om de AVG in zijn geheel ook voor krijgsmacht toepasbaar te verklaren, via de zogenoemde Uitvoeringswet AVG ((U)AVG).[16] Alleen de Wiv 2017 vormt hier een uitzondering op, omdat daar al een wettelijk privacyregime in is opgenomen.

En dat was wellicht niet helemaal doordacht. Het gevolg van de (U)AVG is dat de krijgsmacht in vredestijd – dus zonder een specifiek mandaat – vrijwel geen enkele handeling op het internet mag verrichten waar persoonsgegevens aan verbonden zijn. Waar de MIVD een inlichtingenanalyse mag doen, kan de krijgsmacht dat niet. Gevolg is dat waar de krijgsmacht zich wel gereed kan stellen voor de conflicten in de fysieke omgeving,[17] zij dit voor de virtuele omgeving niet kan.[18] Naast krijgsmacht en inlichtingendiensten heeft ook de politie belang bij het optreden in de informatieomgeving. De politie heeft weliswaar een andere set aan mandaten waar ook de KMar gebruik van kan maken, maar treedt daarnaast ook pro-actiever op in de informatie omgeving.

11 Kraesten L. Arnold e.a., 'Assessing the Dogs of Cyberwar. Reflections on the Dynamics of Operations in Cyberspace during the Russo-Ukrainian War', in: Maarten Rothman, Lonneke Peperkamp en Sebastiaan Rietjens (red.), *Reflections on the Russian-Ukrainian War* (Leiden, Leiden University Press, 2024)

12 Pieter Zhao, 'Chinese Political Warfare. A Strategic Tautology? The Three Warfares and the Centrality of Political Warfare within Chinese Strategy' [2023] The Strategy Bridge

13 Paul A.L. Ducheine, Peter B.M.J Pijpers en Marten C. Zwanenburg, '*Tanden voor de leeuw. Een voor haar doel en op haar taak berekende krijgsmacht in de informatie-omgeving*', NLDA War Studies Research Centre (2024), zie: https://open.overheid.nl/documenten/e8d9cd92-fe6e-4a6f-a27b-9673649c2643/file.

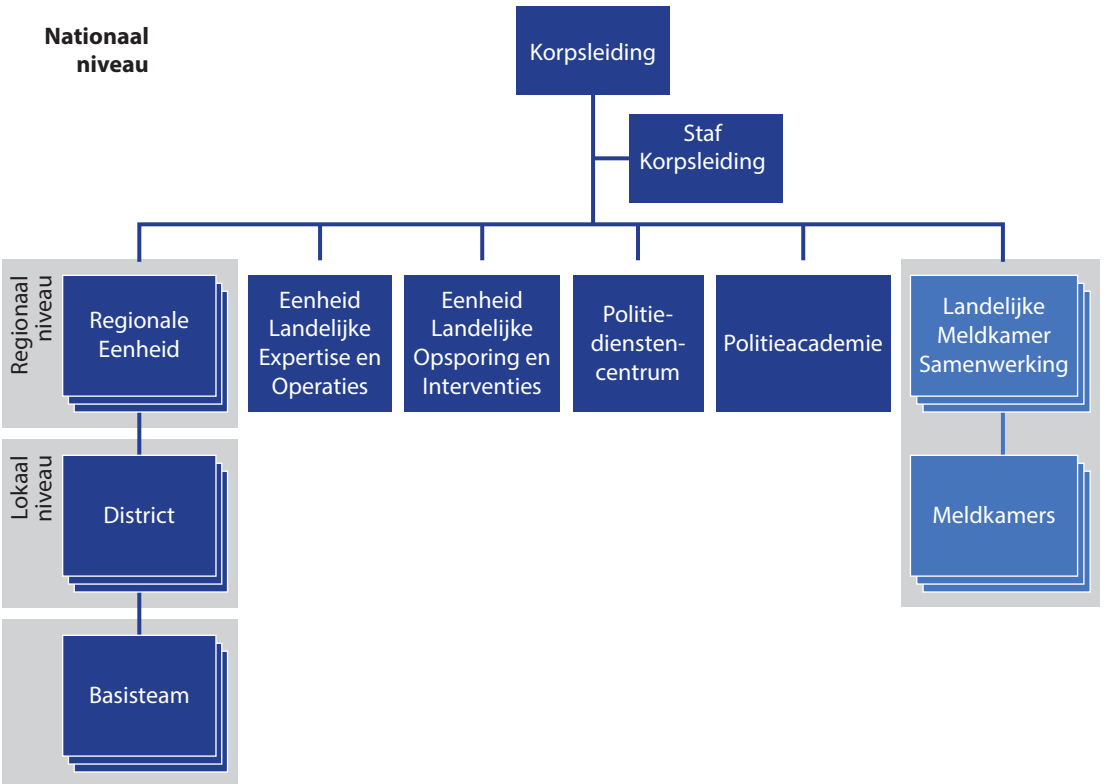
14 NCTV, AIVD, MIVD, 'Dreigingsbeeld Statelijke Actoren (DBSA) (2025), zie: https://www.nctv.nl/documenten/2025/07/17/dreigingsbeeld-statelijke-actoren-2025.

15 Verordening 2016/679, te vinden op: https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679.

16 Uitvoeringswet Algemene Verordening Gegevensbescherming, te vinden op: https://wetten.overheid.nl/BWBR0040940/2021-07-01.

17 Op grond van het Algemeen Organisatie Besluit Defensie (2021). Zie ook: Paul A.L. Ducheine, Peter B.M.J. Pijpers en Eric H. Pouw, 'Information Manoeuvre and the Netherlands Armed Forces. Legal Challenges Ahead', in: Peter Pijpers, Robert Beeres en Mark Voskuijl (red.), *Towards a Data-Driven Military* (Leiden, Leiden University Press, 2023).

18 De Wet op de Gereedstelling Defensie zal hier enige verlichting in brengen, zie meer hierover: https://www.defensie.nl/actueel/nieuws/2025/06/06/nieuw-wetsvoorstel-voor-versnelde-gereedheid-defensie.



Figuur 2: Organogram Nederlandse politie[21]

De politie

'De politie heeft tot taak in ondergeschiktheid aan het bevoegd gezag en in overeenstemming met de geldende rechtsregels te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven'.[19] Dit artikel 3 Politiewet 2012, vormt de basis van het handelen van de politie met het Openbaar Ministerie of de burgemeester als bevoegd gezag. De politie werkt lokaal (in een basisteam) meestal aangiftegedreven. Regionaal of landelijk zijn onderzoeken vaker gericht op fenomenen.[20] In fenomeenonderzoeken staat de *modus operandi* (criminele werkwijze) centraal en kijkt de politie welke handelingsopties het meest effectief zijn om misdaad te bestrijden binnen het gestelde juridisch kader.

In beleid- en visiedocumentatie staat uitgebreid beschreven hoe de politie te werk moet gaan. De huidige korpschef, Janny Knol, beschrijft hierbij onder meer de volgende focuspunten:

- focus op digitaal: *het internet heeft een politiefunctie nodig*;[22]
- effectieve interventies: brede bestrijding;[23]
- meebewegen met ontwikkelingen in onze omgeving.[24]

19 Politiewet 2012 artikel 3, zie: https://wetten.overheid.nl/BWBR0031788/2025-07-01.
20 Politie, 'Werken bij de Politie als cybercrimespecialist', zie: https://kombijde.politie.nl/blog/it/cybercrimespecialist.
21 Politie.nl, 'organogram Nederlandse politie', zie: https://www.politie.nl/informatie/organogram-nederlandse-politie.html.
22 Politie.nl 'Nieuwe korpschef Janny Knol: 'Zorgen dat de politie midden in de samenleving blijft staan' (2024), zie: https://www.politie.nl/nieuws/2024/februari/29/00-nieuwe-korpschef-janny-knol-zorgen-dat-de-politie-midden-in-de-samenleving-blijft-staan.html.
23 Politie, 'Stevig Stevig staan in deze tijd: Strategische agenda politie 2025-2030 (2024), zie: https://www.politie.nl/binaries/content/assets/politie/onderwerpen/publicaties/2025/748ab5cf-6e4d-41ca-b8a1-d9d141a2f916.pdf.
24 Idem.

Brede bestrijding van (online) criminaliteit

Voordat we het politieoptreden in het cyberdomein nader uiteenzetten, vraagt het begrip 'brede bestrijding' nadere duiding. Brede bestrijding van cybercrime draait niet alleen om *opsporing en vervolging*, maar ook om het beperken van criminaliteit (*verstoring*) en het voorkomen van dader- en slachtofferschap (*preventie*).[25] Dit zijn de drie categorieën interventies waar de politie gebruik van kan maken, om ze vervolgens toe te passen in de modus operandi van cybercrime.

Een (gesimplificeerde) modus operandi bestaat uit drie onderdelen: slachtoffers, infrastructuur en daders.[26] Slachtoffers en daders zijn vaak (rechts)personen. De infrastructuur omvat een faciliterende laag zoals een digitaal geautomatiseerd werk –bijvoorbeeld een internetserver in beheer van een bedrijf. Hoe dit precies in zijn werk gaat wordt beschreven in de praktijkvoorbeelden.

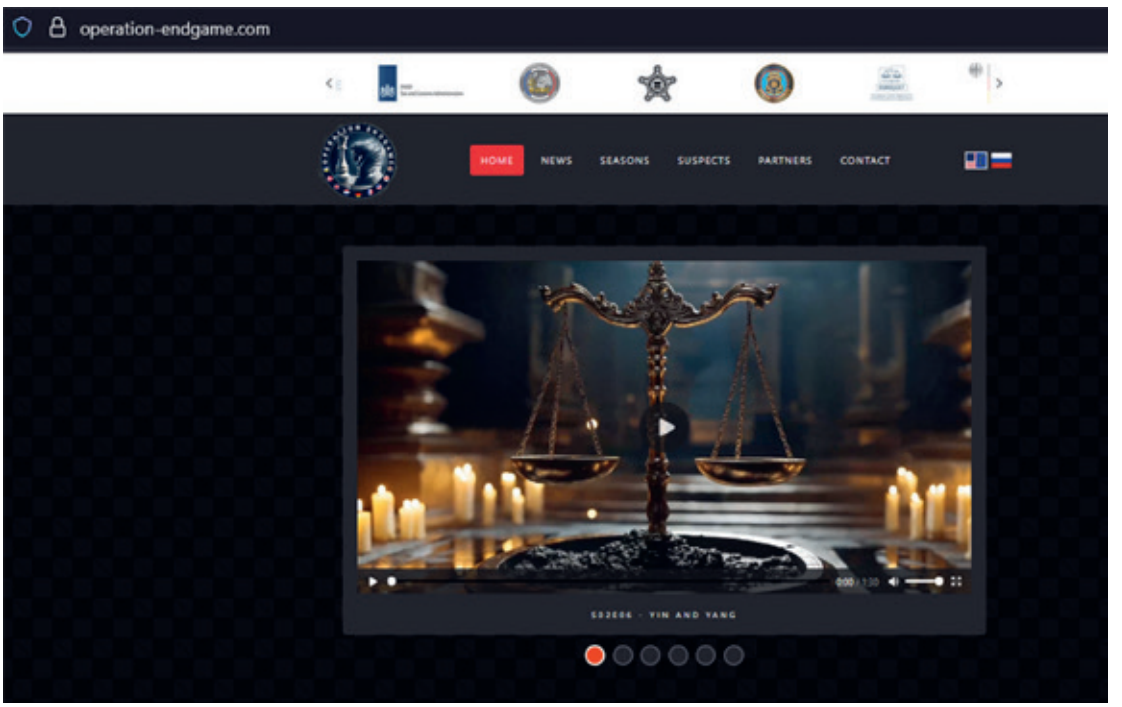
De politie maakt geen categorisch onderscheid binnen cyber vergelijkbaar met hard- en soft-cyber. Vergelijkbaar met soft-cyber werkt de politie met het beïnvloeden van gedrag, de focus van dit artikel. Dit valt vaak te verantwoorden binnen artikel 3 Politiewet. Soms zijn dergelijke interventies wel onderdeel van een groter onderzoek met een ander juridisch kader met additionele bevoegdheden. Voorbeelden vergelijkbaar met hard-cyber binnen de politie (waar wij niet nader op ingaan) zijn onder meer inbeslagname, het ontoegankelijk maken, het vorderen van gegevens, het bevriezen van data, het laten verwijderen van data of het vernietigen van hardware. Voor al deze opties volstaat

25 Politie en Openbaar Ministerie, 'Cybercrime beeld Nederland 2024', te vinden op: https://www.politie.nl/binaries/content/assets/politie/nieuws/2024/juni/4983dcc5-96df-4a2c-8d76-1f6fe2cab4fa.pdf.

26 Idem, zie ook: https://fts.politie.nl/cybercrimebeeld/.

27 Politie.nl 'Internationale politiediensten pakken met Operation Endgame door in bestrijding ransomware' (2025), zie: https://www.politie.nl/nieuws/2025/mei/22/11-internationale-politiediensten-pakken-met-operation-endgame-door-in-bestrijding-ransomware.html.

Figuur 3: Splash page Operation Endgame[27]



Figuur 4: Website operation-endgame.com

artikel 3 Politiewet niet, maar zijn additionele bevoegdheden benodigd.

Praktijkvoorbeelden

Operation Endgame

Operation Endgame is een van de bekendste internationale acties tegen botnets, ofwel netwerken van met malware geïnfecteerde computers. Wat botnets zo gevaarlijk maakt, is dat de geïnfecteerde malware als het ware de deur opent voor andere vormen van cybercrime. Operation Endgame bestaat niet alleen uit opsporingsinterventies, maar ook uit gedragsbeïnvloeding. Dit is nodig omdat niet alle verdachten (direct) aangehouden kunnen worden. Daarom is er een speciale website opgezet, specifiek voor de verdachten en geïnteresseerden, onder meer in het Russisch. Het doel van deze website is de verdachten aanspreken, twijfel zaaien in het criminele netwerk en allerlei data blootleggen.

Opvallend aan de website is de communicatiestijl, die overeenkomt met de wijze van communicatie van de cybercriminelen zelf. Bij het openen van de website valt direct de quote ‘Think about (y)our next move’ op. Daarnaast zijn er specifieke opties om te communiceren met de politie – voor de verdachten, maar ook voor tipgevers. Dit is dus een directe beïnvloedingspoging van het gedrag van diegenen die de website zien of te zien krijgen.

Daarnaast heeft de politie ervoor gekozen om de namen, foto’s en de modus operandi van de verdachten online te plaatsen. In de wereld van online-cybercrime, met allerlei afschermingsmethoden, is blootstelling een zware interventie. Dit heeft direct effect op de verdachten, hun sociale kring en derden. Ook hindert de politie de criminele modus operandi en persoonlijke leefsfeer van de verdachten. Ze kunnen bijvoorbeeld geen (internet)diensten meer afnemen, omdat deze internationaal zijn gekoppeld. Bovendien heeft het tonen van

verdachten ook effect op andere cybercriminelen.

Deze interventies zijn duidelijk gericht op daders, met als doel preventie en verstoring, én infrastructuur met als doel preventie op basis van kennisdeling en samenwerking.

Criminele carrière in cyber voorkomen

Bij cybercriminelen valt op dat zij vaak een verleden hebben in gaming.[28] Binnen gaming is DDoS een bekend fenomeen. Zo is het vrij gebruikelijk om elkaars server 'plat te gooien', zodat iemand bijvoorbeeld een spel kan winnen of wraak kan nemen tegen andere online gamers.
Doordat gamers op vroege leeftijd al in aanraking kunnen komen met DDoS, is het niet vreemd dat sommigen van hen zich doorontwikkelen tot cybercrimineel. Om dit carrièrepad te voorkomen, waarschuwt de politie potentiële daders door middel van ingekochte Google-advertenties.[29] Wie via Google zoekt op 'DDoS bestellen' vanuit Nederland, ziet vaak een politiewaarschuwing hoog in de zoekresultaten.
Deze politiewaarschuwingen moeten leiden tot gedragsverandering bij (potentiële) daders. Deze interventie is uiteraard niet sluitend, maar vergroot de aanwezigheid van de politie op een plek waar mogelijk gezocht wordt naar strafbare feiten. Daarnaast zorgen deze advertenties voor meer bewustwording. Deze interventie focust dus op daders door middel van preventie.

Publiek Private Samenwerking

Een van de belangrijkste interventies binnen de politie is Publieke Private Samenwerking (PPS). PPS is de gestructureerde interactie tussen de politie (en eventueel een of meerdere overheden) en particulieren met als doel het ontwikkelen en/of uitvoeren van een gezamenlijke strategie voor het realiseren van veiligheidsbeleid.[30]
PPS is voornamelijk effectief voor de categorieën infrastructuur, verstoring en preventie. Hierbij zoekt de politie de samenwerking op met zowel bedrijven als andere (maatschappelijke) organisaties. Op die manier kan de politie deze bedrijven en organisaties wijzen op de verantwoordelijkheden, modus operandi delen en adviseren in maatregelen.

> Soft-cyber (beïnvloedings-)operaties richten zich niet op doelen in cyberspace, maar gebruiken cyberspace als een vector om de cognitie van individuen of groepen te bereiken

In veel onderzoeken is PPS onderdeel van brede bestrijding, zoals in het eerder genoemde Operation Endgame.[31] Daarnaast is er een aantal samenwerkingen tussen de politie en het bedrijfsleven die structureel van aard zijn, zoals het telecomoverlegorgaan COIN en het bancaire overlegorgaan ECTF. Dergelijke samenwerkingen bieden doorlopend interventiekansen binnen de sectoren waarin cybercriminaliteit voorkomt. Verder creëren ze wantrouwen bij criminelen, omdat de kans op (structurele) verstoring én opsporing toeneemt. Ook krijgt het bedrijfsleven meer inzicht door kennisdeling en stijgt de druk om waar nodig zelf actie te ondernemen op basis van verantwoordelijkheid. Zo kunnen organisaties verantwoordelijkheid nemen door aan te sluiten bij initiatieven zoals *nomoreleaks*, een initiatief tegen datalekken.[32]

28 Politie, 'Cybercrimebeeld 2024', zie: https://fts.politie.nl/cybercrimebeeld/.
29 Politie, 'Politie gebruikt Google Ads om cybercrime te bestrijden', zie: https://www.politie.nl/nieuws/2024/februari/29/00-politie-gebruikt-google-ads-om-cybercrime-te-bestrijden.html.
30 Publiek Private Samenwerking, *Tijdschrift voor de Politie*, No.3, 2021 zie: https://www.ppsconstruct.nl/inhoud/uploads/PPS-succesfactoren-tijdschrift-voor-de-politie.pdf.
31 Politie, 'Cybercrimebeeld 2024', zie: https://fts.politie.nl/cybercrimebeeld/.
32 Politie, 'No More Leaks', zie: https://www.politie.nl/onderwerpen/no-more-leaks.html.

Operation Heartblocker
Niet alleen landelijke onderzoeken hebben internationaal impact. Bijna elke maand is er wel een regionale cyberinterventie van de politie in de media.[33] Een van deze acties is Operation Heartblocker, een onderzoek naar de criminele webshop Heartsender.[34] Deze via het clearweb bereikbare webshop verkocht allerlei criminele software, waarmee cybercrime gepleegd kon worden.

In dit onderzoek komen veel slachtoffers naar voren en verwijst de politie door naar slachtoffernotificatietools, zoals *checkjehack*. Hiermee kunnen internetgebruikers hun accounts spiegelen aan een database. Op die manier kunnen ze zien of hun gegevens voorkomen in datasets van gelekte gegevens. Waar nodig adviseert de politie om beveiligingsmaatregelen treffen.

De mediaberichtgeving richt zich ook tot potentiële kopers van dergelijke software. Niet alleen de ontwikkelaars en verkopers van de software in dit onderzoek zijn namelijk strafbaar, maar ook afnemers van deze software. Dit brengt verdere twijfel in de netwerken van criminelen.

Dergelijke specifieke communicatie komt vaker voor binnen de politie, met een bewuste afweging welke gegevens wel of niet worden gepubliceerd. Inzicht geven in de criminele modus operandi is een mogelijkheid, maar inzicht geven in politieoptreden is een hele andere invalshoek. Dit laatste is bijvoorbeeld te zien in een recentelijk gepubliceerd politie.nl-persbericht over een politie-inval.[35] Dit bericht beschrijft uitvoerig hoe de politie te werk is gegaan tijdens een huiszoeking bij een cybercrimineel. Met opvallend veel detail worden de directe gevolgen van crimineel handelen beschreven. Het artikel beschrijft niet alleen de gevolgen voor de verdachte zelf, maar ook voor de ouders van de verdachte. Dit is dan ook weer een voorbeeld voor andere ouders; een waarschuwing om beter te controleren wat hun thuiswonende kinderen online uitvoeren. Daderpreventie gaat namelijk niet alleen om de persoon zelf, maar ook om het netwerk van mensen om die persoon heen.

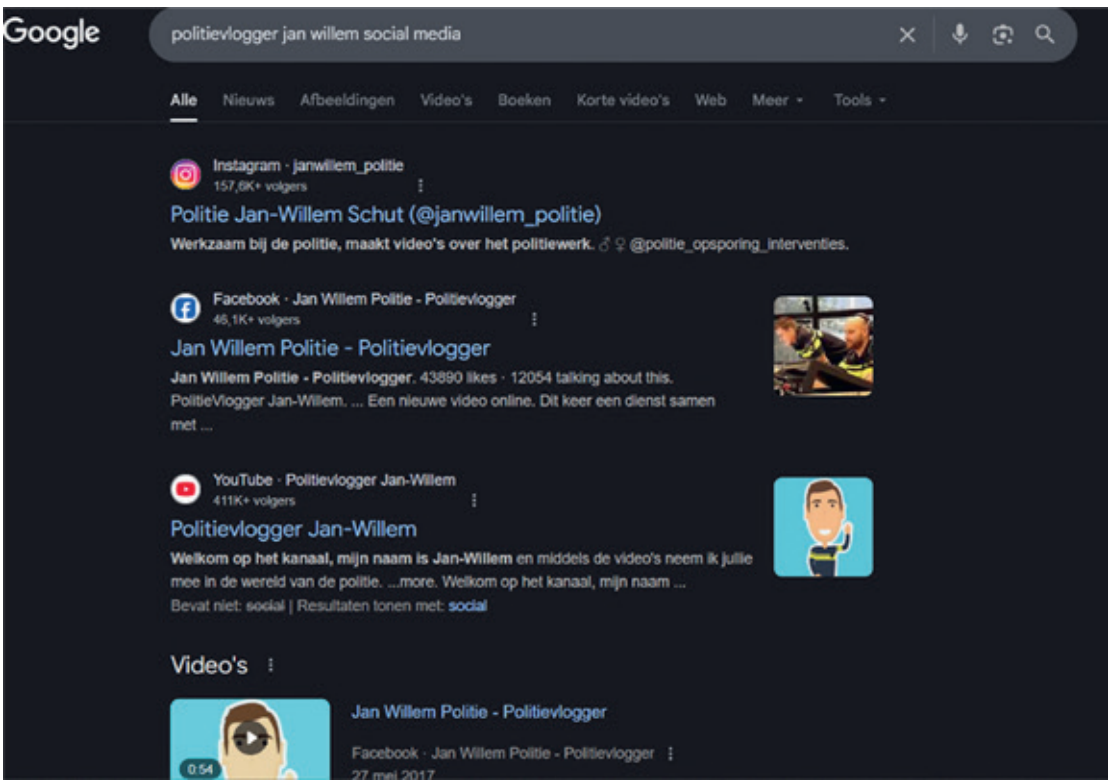
In Operation Heartblocker gaat de focus uit naar slachtoffers en preventie. In het persbericht over de politie-inval gaat de focus uit naar daders en preventie. Uiteraard blijft het de vraag of deze berichtgeving ook daadwerkelijk de desbetreffende doelgroep bereikt.

Slachtofferpreventie via Meta-advertenties
De politie acteert niet alleen gericht op daders, maar ook op slachtoffers. Zo heeft de politie MKB'ers uitgebreid gewezen op een specifieke oplichtingsvorm die vaak voorkomt: hacking via Facebook.[36] Opvallend aan deze criminele modus operandi is dat het instellen van tweefactorauthenticatie deze oplichtingsvorm voorkomt. Dit is een relatief gemakkelijke gedragsverandering om te bewerkstelligen.

Samen met Platform Veilig Ondernemen (tevens PPS-interventie) heeft de politie een campagne gelanceerd, specifiek gericht op kleine ondernemers op Facebook en Instagram. De advertenties zijn afkomstig van een regionaal politieaccount met daarin een waarschuwing voor deze vorm van hacking.[37] Op deze manier creëert de politie meer bewustzijn bij deze slachtofferdoelgroep. Daarnaast krijgen potentiële slachtoffers instructies om tweefactorauthenticatie aan te zetten. Deze interventie focust dus op slachtoffers met als doel preventie.

Lokale beïnvloeding
Waar eerdere voorbeelden zich voornamelijk focussen op klassieke mediaberichtgeving, is wellicht de grootste beïnvloedingstactiek van de

33 Zie: https://www.google.com/search?q=politie+actie+cybercrime.
34 Politie, 'Verstoringsactie deelt klap uit aan crimineel cybernetwerk HeartSender', zie: https://www.politie.nl/nieuws/2025/januari/27/09-verstoringsactie-deelt-klap-uit-aan-crimineel-cybernetwerk-heartsender.html.
35 Politie, 'Ineens van je bed gelicht…', zie: https://www.politie.nl/nieuws/2025/september/1/ineens-van-je-bed-gelicht%E2%80%A6.html.
36 'Ondernemers zoals Maik in grote problemen door Facebook-hacks: 'Twee ton omzetverlies'', zie: https://www.rtl.nl/nieuws/onderzoek/artikel/5506912/facebookhacks-treffen-ondernemers.
37 PVO, 'Voorkom fraude op Meta: stel 2FA in op Facebook', zie: https://pvo-nl.nl/nieuws/voorkom-fraude-op-meta-stel-2fa-in-op-facebook/.



Figuur 5: Socials overzicht Politievlogger Jan-Willem

politie haar digitale aanwezigheid, voornamelijk op social media. Het overgrote deel van Nederland is actief op een vorm van social media.[38] Maar ook vrijwel elk politiebasisteam heeft zijn eigen socials.[39] Diverse politieagenten zijn zelfs influencer. Ook op TikTok heeft de politie een aantal accounts met honderdduizenden volgers. Dit alles bij elkaar zorgt ervoor dat de politie een groot online-bereik heeft. Daarnaast kan de politie op deze manier doelgroepen bereiken die via standaardcommunicatiemogelijkheden niet bereikbaar zijn.

Het intensief gebruik van dergelijke socials biedt de politie ook kostbare inzichten. Op basis van views is duidelijk zichtbaar welke gemaakte content aanslaat bij volgers. Content met veel actie, bijvoorbeeld een aanhouding door de politie, blijkt bijvoorbeeld veel views te genereren. Dit soort content wordt normaal gesproken door moderatie geblokkeerd of verwijderd. Het tonen van wapens en geweld valt immers onder hevig moderatiebeleid. Doordat dit politieaccounts zijn, en het geweld dus legitiem is, blijft de content online.

De kracht van social media zit voor de politie in het grote bereik. Dit bereik is te vergroten door het taggen van andere politieaccounts en actief samenwerken met influencers (bondgenoten).[40] Met deze communicatie op social media vindt op lokaal niveau slachtoffer- en daderpreventie plaats, met geregeld een landelijk bereik. Voorbeelden hiervan zijn filmpjes van de politie op TikTok – waar een groot deel van de Nederlanders een account heeft – met miljoenen views. Dit is een vorm van online surveillance. Zonder deze aanwezigheid is beïnvloeding met

38 'Socialmedia-onderzoek 2025: flinke daling X, LinkedIn in de lift & actieve 40-plussers', Frankwatching.com, zie: https://www.frankwatching.com/archive/2025/01/25/social-media-onderzoek-2025/.
39 Politie, 'Social media', zie: https://www.politie.nl/contact/social-media.
40 'Gebiedsverbonden' politie als middel tegen polarisatie'', zie: https://www.politieacademie.nl/over-ons/nieuws/gebiedsverbonden-politie-als-middel-tegen-polarisatie.

Vrijwel elk politiebasisteam heeft zijn eigen social media; diverse politieagenten zijn zelfs influencer

als doel het interveniëren tegen criminaliteit onmogelijk.

Lessen voor de krijgsmacht

De krijgsmacht dient de vitale belangen van de staat te beschermen, maar mist in het digitale domein het mandaat om zich gereed te stellen om deze taak in een situatie van conflict uit te voeren. Daarnaast heeft de krijgsmacht rol noch mandaat om de bescherming van de vitale belangen in het digitale domein uit te voeren buiten een gewapend conflict of binnen het Koninkrijk. In een rechtsstaat is dat weliswaar een geruststellende gedachte – de krijgsmacht hoort niet binnen Nederland op te treden, daar is de politie voor – maar het staat haaks op de grenzeloze eigenschappen van (de activiteiten in) cyberspace.

Op welke wijze kan de krijgsmacht leren van de nationale politie, of hoe kunnen beide organisaties samenwerken om invulling te geven aan de synergie tussen publieke partijen in het Nederlandse cyberlandschap? De centrale thema's bij de politie om brede bestrijding te bewerkstellingen komen conceptueel overeen me de theoretische concepten van soft-cyber-operaties, te weten: hoe bereik je effectief een doelgroep via huidige communicatiemethoden, hoe draag je effectief een boodschap over, en hoe beïnvloed je gedrag.

De politie operationaliseert deze beïnvloedingsoperaties ten eerste door zichtbaar te zijn op (social) media, dit ter voorkoming van het verstoren van de eigen operatie (moderatie); als afschrikking; ze binden doelgroepen aan zich; en genereren betrouwbare accounts en bereik. Daarnaast creëert de politie effectieve Publiek Private Samenwerking (PPS), door partners aan te zetten tot actie (een *force multiplier*), en gebruik te maken van de middelen van die partners. Tot slot zet de politie doelgroepgerichte effectieve communicatie in, om zo de juiste boodschap over te brengen aan de juiste doelgroep; en om daarmee een daadwerkelijke gedragsverandering te genereren.

De krijgsmacht gebruikt deze methode nog niet, deels ook vanwege juridische beperkingen, maar dat wil niet zeggen dat zij helemaal niet kan optreden. Naast samenwerking met de inlichtingendiensten of met buitenlandse krijgsmachten kan de krijgsmacht ook gaan samenwerken met (en onder het mandaat van) de politie, vooral in situaties buiten een gewapend conflict, zoals bij nationale inzet. De krijgsmacht geeft daarmee invulling aan de nieuwe Defensie Cyberstrategie, maar is daarmee bovenal effectief om dreigingen tegen te gaan en kan tegelijkertijd haar vaardigheden op peil houden. De krijgsmacht kan zo leren welke content bij welke doelgroep past, welke soorten outlets de doelgroepen hanteren, en op welke wijze zij empathisch kan communiceren (gebruikmaken van de taal van die specifieke doelgroep). Ten slotte valt te overwegen om ook zelf social media-accounts op te zetten en zelfs militaire vloggers aan te moedigen en te professionaliseren, niet voor intern gebruik maar om de krijgsmacht meer bekendheid te geven bij een breder publiek, mogelijk zelfs gericht op de bevolking (en diaspora) van potentiële opponenten. ■