Bijlage

Trends en Uitdagingen voor de Landelijke Eenheid

Een schets van benodigde capaciteiten

Prof. dr. Arjen Boin
Prof. dr. Beatrice de Graaf

Universiteit Utrecht

CRISIS plan

COLOFON

Titel: Trends en Uitdagingen voor de Landelijke Eenheid: een schets van benodigde capaciteiten

Auteurs : Arjen Boin & Beatrice de Graaf

Utrecht, Leiden 11 januari 2022

De auteurs bedanken Myrthe van Groningen, Lena Harding, Bjarne von Lampe, Werner Overdijk en Henry Shields voor hun hulp in het tot stand komen van dit rapport.

Inhoudsopgave

I. Opzet en aanpak

De auteurs zijn gevraagd na te denken over de uitdagingen zoals die voortvloeien uit trends en (mogelijke) trendbreuken in vier 'dreigingsdomeinen': terrorisme, ondermijning, cyber, en publieke ordeverstoringen. Zij hebben de recente literatuur op elk van die domeinen (met behulp van een assistent) bestudeerd. Daarnaast hebben zij verschillende experts geïnterviewd om de opgedane bevindingen te toetsen en te verrijken (een overzicht van de respondenten is opgenomen in de bijlage).

Dit rapport identificeert de uitdagingen die binnen de Nationale Politie waarschijnlijk bij de Landelijke Eenheid (LE) zouden 'landen'. De vier dreigingsdomeinen worden gekenmerkt door het grootschalige en grensoverschrijdende karakter van de consequenties die uit deze dreigingen kunnen voortvloeien. Dat wil niet zeggen dat deze uitdagingen niet ook voor de politie in algemene zin, of voor heel andere (publieke) organisaties, van belang kunnen zijn. Het is aan de Commissie om te bepalen welke door ons aangereikte suggesties relevant zijn voor de LE.

Voor ieder domein hebben we in eerste instantie de dominante en extrapoleerbare trends in kaart gebracht: trends worden hier gedefinieerd als ontwikkelingen en patronen die we kunnen vaststellen vanuit het verleden en die voor het heden en de nabije toekomst nog relevant zijn. Daarnaast is bezien welke mogelijke *game changers* in de literatuur worden geïdentificeerd. Game changers zeggen iets over de toekomst: het zijn gebeurtenissen of ontwikkelingen die het potentieel hebben nieuwe uitdagingen in het dreigingsdomein te creëren. Wij bespreken de game changers die consequenties voor de werkwijze van de Landelijke Eenheid kunnen hebben.

We bezien vervolgens welke organisatorische capaciteiten benodigd zijn om met de verschillende uitdagingen effectief om te gaan (we kijken niet of de Landelijke Eenheid op dit moment met die uitdagingen *kan* omgaan; we bezien alleen welke capaciteiten aanwezig moeten zijn om toekomstbestendig te zijn). Onder capaciteiten verstaan we de benodigde structuren, processen en middelen die een organisatie in staat stelt aan de gestelde doelen te voldoen.

We organiseren onze inzichten rond een aantal categorieën van capaciteiten die in het algemeen in een organisatie – wellicht in meer of mindere mate – aanwezig moeten zijn. De vraag die wij niet beantwoorden is of de LE over deze capaciteiten moet beschikken. De Commissie kan adviseren dat sommige van deze capaciteiten misschien wel bij andere organisaties (of organisatieonderdelen van de Nationale Politie) thuis horen. We organiseren onze discussie rond de volgende typen capaciteiten:

Preventie: welke capaciteiten zijn nodig om de dreiging uit te sluiten of te minimaliseren?

Intelligence en analyse: welke capaciteiten zijn nodig om de dreiging tijdig te herkennen en te benoemen? Wat is nodig om de aard, dynamiek en gevolgen van de dreiging in kaart te brengen en goed te begrijpen?

Strategie- en besluitvorming: welke capaciteiten zijn nodig om een effectieve en legitieme strategie te formuleren?

Operationele capaciteit: welke middelen en welk type menskracht zijn nodig om de ingezette strategie op succesvolle wijze te implementeren? Hoe moeten ze worden aangestuurd?

Coördinatie: welke capaciteiten zijn nodig om partners te betrekken (horizontale coördinatie) en de uitvoering binnen de organisatie (verticale coördinatie) goed af te stemmen?

Communicatie: welke capaciteiten zijn nodig om helder en met autoriteit over de dreiging met de buitenwereld te communiceren?

Het rapport is als volgt opgebouwd. We bespreken de trends, *game changers* en daaruit voortvloeiende eisen aan de Landelijke Eenheid per dreiging (paragraaf 2 t/m 5). In paragraaf 6 bezien wat de gemene deler is van de organisatiecapaciteiten die benodigd zijn voor het omgaan met de dreigingen van de toekomst. In de slotparagraaf reflecteren we op de uitdagingen voor de leiders die in de toekomst gestalte moeten geven aan deze capaciteiten. De ontwikkeling en aansturing van deze capaciteiten stellen eisen aan het leiderschap binnen de Landelijke Eenheid. Die proberen wij te benoemen.

Dit deelrapport is nadrukkelijk geen analyse van de bestaande capaciteiten in de Landelijke Eenheid en/of de leiders die vandaag of gisteren aan het hoofd van de Landelijke Eenheid stonden. Wij formuleren een houtkoolschets van benodigde capaciteiten die de Commissie Schneiders mogelijk kan gebruiken om concrete aanbevelingen te formuleren.

II. Ondermijning

Inleiding

De term ondermijning wordt veel gebruikt in beleidsstukken, politieke debatten en mediadiscussies. Het is echter niet altijd duidelijk waar precies op wordt gedoeld. De term wordt op heel veel verschillende manieren gedefinieerd en begrepen (Boutellier et al., 2020).[1]

De Landelijke Eenheid spreekt van ondermijning wanneer sprake is van het 'verzwakken, misbruiken en ontwrichten van maatschappelijke structuren'. Dit is, zo mag worden opgemerkt, een rijkelijk vage en veelomvattende definitie. De definitie maakt bijvoorbeeld niet duidelijk wie nu precies bezig is met ondermijning. In de Nederlandse discussie lijkt de definitie te zijn verengd tot de georganiseerde misdaad. De internationale literatuur besteedt juist steeds meer aandacht aan het *verzwakken* en *ontwrichten* van democratie of 'the rule of law' (door bijvoorbeeld propaganda, misinformatie op social media en interventies van buitenlandse diensten) (European Commission, 2016; Bennett & Livingston, 2018; Haciyakupoglu et al., 2018; Ricard & Medeiros, 2020; Henschke et al., 2020; van Kessel et al., 2021).

Trends

Zelfs in de meest beperkte definitie is duidelijk dat analysten ondermijning zien als een 'creeping crisis': een gestaag accumelerende dreiging die gemakkelijk tot een grootschalige crisis kan uitgroeien (Boin et al., 2020, 2021). Volgens sommige respondenten is de situatie in Nederland nu al 'volledig uit de hand gelopen' (zie ook Saviano, 2021). Recente onderzoeken laten inderdaad zien dat ondermijning breed aanwezig is in onze samenleving (zie bijvoorbeeld Noordanus, 2020, Paulissen, 2019; Tops & Tromp, 2017; Schuurman et al., 2021; cf. Bullough, 2019). De recente moorden op de advocaat Derek Wiersum en misdaadverslaggever Peter R. de Vries kunnen worden gezien als de meest recente, en wellicht meest alarmerende indicatoren van de toenemende crisisdreiging.

Uit de recente literatuur destilleren we een aantal verontrustende en goed gedocumenteerde trends:

Normalisering van drugsgebruik: Het *Christine F.* Beeld van de geïsoleerde en aan lager wal geraakte drugsgebruiker ligt ver achter ons. Recreatief drugsgebruik (vooral cannabis) lijkt steeds normaler te worden, al lijkt het gebruik niet te groeien (Pennay and Measham, 2016; European Monitoring Center for Drugs and Drug Addiction [EMCDDA], 2019; Patton, 2018; Karlsson et al., 2019; Alves et al., 2021; cf. Dickinson and Jacques, 2021).

Grof geweld in de publieke ruimte: Het aantal liquidaties is de afgelopen jaren schrikbarend hoog (Vugts, 2017; Schuurman et al., 2021; Voeten, 2021). De daders lijken jonger te zijn en schuwen het gebruik van geweld niet, zelfs wanneer de objecten van het geweld zich in de openbare ruimte (omgeven door

[1] Interessant is dat de term in het Engels geen gelijkwaardig equivalent lijkt te hebben.

andere mensen) bewegen (Burgers, 2021; De Korte & Kleemans, 2021; Kraak, 2021). Ook het aantal bedreigingen neemt toe (Schuurman et al., 2021).

Het witwassen van crimineel geld is geen nieuw fenomeen: Maar de enorme bedragen die met drugscriminaliteit worden verworven maken het witwassen van dat geld steeds belangrijker voor criminelen. Ze kunnen al dat geld niet contant besteden. Hun rijkdom stelt criminelen in staat professionals in te huren die hen ten dienste staan met allerlei financiële constructies (Europol, n.d, 2021; Levi & Soudijn, 2020; Levi, 2021; Noordanus, 2020; Bullough, 2019; Wainwright, 2016; Tops & Tromp, 2017). Veel criminaliteit en witwaspraktijken lopen via legale bedrijven (Europol, 2021; Tops & Tromp, 2017). Drugscriminelen raken steeds beter in het scheren langs de randen van de wet (Bullough, 2019). De bedragen die jaarlijks worden witgewassen kunnen niet precies worden vastgesteld. Experts zijn het er over eens dat het elk jaar om meer geld gaat (United Nations Office on Drugs and Crime, n.d; Tops & Tromp, 2017, 2020).

Internationalisering drugshandel en geldstromen: De drugshandel is steeds meer geïnternationaliseerd en Nederlandse drugscriminelen weten hier goed gebruik van te maken (Madarie & Kruisbergen, 2020; Voeten, 2021; Noordanus, 2020; Tops & Tromp, 2017). Omgekeerd vinden internationale drugscriminelen gemakkelijk hun weg naar Nederland. Dit betekent dat een wijdverbreid internationaal financieringsnetwerk is ontstaan. Dit netwerk onttrekt zich goeddeels aan het zicht van nationale autoriteiten (Levi, 2021).

Darkweb als handelsplaats: Een extreme vorm van internationalisering is de verplaatsing van de drugshandel naar de cyberwereld (Goosdeel & Wainwright, 2017; Blanco & Cohen, 2017; Kruisbergen et al., 2019; Horton-Eddison et al., 2021; Roks et al., 2021). Fysieke markten waar criminelen elkaar ontmoeten maken plaatsen voor cybertranscties die zich in belangrijke mate onttrekken aan het blikveld van autoriteiten (Bijlenga & Kleemans, 2018; Kruisbergen et al., 2019). Hierdoor ontstaat een efficiënte markt die zich niet laat reguleren via de bestaande toezichtsinstrumenten (Blanco & Cohen, 2017; Bijlenga & Kleemans, 2018). Die markt wordt weer verbreed met aanbod van allerhande criminele diensten (*crime as service*), variërend van wapen- en mensenhandel tot geweldsdiensten.

Steeds weer nieuwe designer drugs: De ontwikkeling van nieuwe drugs wordt door criminelen als een scheikundige uitdaging gezien. Als een wettelijk verbod op een bepaalde drug de chemische eigenschappen van de drug specificeert, is slechts een kleine wijziging in de chemische structuur nodig om het verbod te omzeilen (Noordanus, 2020). De expertise neemt toe en het wordt steeds gemakkelijker om semi-legale drugs te ontwikkelen (Baumeister et al., 2015; European Monitoring Center for Drugs and Drug Addiction, 2020; Zwartsen, 2020; ter Laak, 2021).

Navenante criminaliteit: De professionaliteit van drugscriminelen maakt hen tot belangrijke (en vaardige) spelers in andere vormen van criminaliteit zoals milieudelicten en mensenhandel. Dit vergroot weer de reikwijdte en verwevenheid van drugsorganisaties (Shelly, 2012; Di Cataldo & Mastrorocco, 2020; van Uhm & Nijman, 2020; Achilli & Sanchez, 2021; Tops & Tromp, 2017).

Inzet van lokale gangs en motorclubs: Drugsbendes hebben geen moeite met het uitbesteden van geweldstaken aan ontkoppelde groepen zoals lokale jeugdcriminelen of een motorclub. Dit biedt drugsorganisaties grote voordelen. Ze disassocieren zich van grof geweld en hoeven geen leger van soldaten in dienst te houden. Deze uitbesteding lijkt met regelmaat plaats te hebben (Robinson et al., 2019; Roks et al., 2021; Trejo & Ley, 2020; Blokland et al., 2020; van Deuren et al., 2021; Ruitenberg, 2020).

Lokale impact: Drugscriminelen tasten de fundamenten van een gezonde maatschappij aan. De inzet van scholieren (als dealers) legt de bijl aan de school als maatschappelijk institutie. Het omkopen van beambten op lokaal niveau erodeert de integriteit van het openbaar bestuur (Buscaglia & van Dijk, 2003; Di Cataldo & Mastrorocco, 2020). De infiltratie in politie-eenheden ondermijnt het vertrouwen van de burger (traditioneel een bastion van legitimiteit in Nederland) maar ook de effectiviteit van de opsporing (Buscaglia & van Dijk, 2003; Smith et al., 2020; Europol, 2021; Noordanus, 2020; Bruinsma et al.; Tops & Tromp, 2017; Wijk & Lenders; Ferwerda et al.). De intimidatie van lokale gezagsdragers is een groeiend probleem (Di Cataldo & Mastrorocco, 2020; Europol, 2021). Ook de intimidatie door drugscriminelen van bedrijven is problematisch (Ganau & Rodriguez, 2018; Fourie et al., 2021).

Game changers

De literatuur beschrijft verschillende ontwikkelingen die de rol van potentiële *game changer* kunnen vervullen (in positieve dan wel negatieve zin). De volgende ontwikkelingen kunnen de strijd tegen ondermijning (nog veel) moeilijker maken:

Criminelen winnen de technologische competitie van misdaadbestrijders: De grote criminelen blijken vaak creatief met nieuwe technologische mogelijkheden om te gaan. Natuurlijk krijgen politie-eenheden ook nieuwe mogelijkheden om drugscriminelen en hun transacties in beeld te brengen en te verstoren. Als het criminelen lukt om domeinen in cyberspace af te bakenen en te controleren, zetten zij hun bestrijders op grote achterstand.

Uitfaseren van cash en introductie van nieuwe betalingsmiddelen: De *war on cash* is in volle gang (Prasad, 2021). Het wordt steeds moeilijker om al dat contante geld (straathandel) wit te wassen. De rappe introductie van allerlei digitale betalingsmiddelen biedt criminelen grote kansen om hun financiële huishouding (nog verder) aan het zicht van opsporingsautoriteiten te onttrekken.

Liquidaties als statussymbool: Geweld tegen concurrenten, afvalligen en overtreders van eigen regels is in Nederland relatief beperkt geweest (maar we noteren een opwaartse trend). Dit zou kunnen veranderen als het symbolisch gebruik van geweld breed wordt geaccepteerd in criminele kringen (Wainwright, 2016). Als drugkartels de behoefte gaan voelen de grenzen van hun domeinen af te perken, is het expliciete en publieke gebruik van grof geweld (bijvoorbeeld onthoofdingen) een beproefd middel (zie bijvoorbeeld de ervaringen in Mexico, Trejo & Ley, 2018). Het zou een enorme impact op de publieke perceptie hebben, zoveel is wel duidelijk. Het kan ook een intimiderende werking op gezagsdragers, beambten en gezichtsbepalende figuren hebben.

Een plotselinge en structurele afname van het vertrouwen in politiek en overheid creëert mogelijkheden voor criminele organisatie om zich als een bron van alternatief gezag te manifesteren: De afname van legitimiteit maakt de overheid ineffectief, waardoor het vertrouwen verder daalt. Het is een verschijnsel van aller tijden (Brosius et al., 2018; European Union Agency for Fundamental Rights, 2020). In veel landen is het vertrouwen in de overheid laag (Brezzi et al., 2020; Prats et al., 2021; Pew Research Center, 2021). Hetzelfde zien we volgens Tops & Tromp (2017) al in sommige Nederlandse wijken. De COVID-19 crisis heeft het vertrouwen in de politiek en politieke gezagsdragers geen goed gedaan.

De infiltratie en overname van publieke instituties: Criminele organisaties kunnen zich besluitvormingsbevoegdheden van publieke instituties toeëignenen, direct of indirect, door infiltratie, omkoping en co-financiering van projecten. Lange-termijn infiltratie in politie en andere bestuurlijke instituten is een bekende methode. Het kopen van invloed in politieke partijen is niet onmogelijk. Dergelijke infiltratie vergroot de invloedssfeer van criminelen en ondermijnt de bestrijding van drugsbendes.

Technische revoluties: De ontwikkeling van drones en vliegende taxi's is in een vergevorderd stadium (MIT Technology Review, 2021; McKinsey & Company, 2021). Dit geldt ook voor 3D-printen en surveillancetechnologieën (Chase & La Porte, 2017; Hornick, n.d; de Korte & Kleemans, 2021; Sherman, 2020; Fussell, 2021). Politieorganisaties maken graag gebruik van nieuwe technologieën. Dat geldt ook voor criminelen, met dien verstande dat zij zich niet aan legale of ethische randvoorwaarden hoeven te storen. Een gerichte investering in nieuwe technologieën geeft criminelen een aanzienlijke voorsprong in de technorace. Het stelt hen in staat nieuwe verdienmodellen te ontwikkelen.

Benodigde capaciteiten

De strijd tegen criminele ondermijning van de gevestigde orde vraagt een enorme inspanning van de politie. Een eerste schets van de benodigde capaciteiten geeft een goed idee van de eisen die we aan de toekomstige politieorganisatie moeten stellen.

Preventie:

De vraag is of de politie capaciteiten kan ontwikkelen die ondermijning tot beheersbare proporties terugbrengen. De experts die wij spraken tonen zich pessimistisch (zie ook Blanco & Cohen, 2017; Gelles et al., 2019; Vermeer et al., 2020). De inkapseling van deze dreiging vraagt om te beginnen dat kwetsbare/target groepen bewust worden gemaakt dat zij de criminaliteit in worden gezogen. Alternatieve loopbaanpaden moeten worden aangeboden, maar dat is geen taak voor de politie. De politie kan wel meewerken aan campagnes die zijn gericht op het verminderen van de aantrekkingskracht van de georganiseerde criminaliteit. Het drugsgebruik moet worden ontmoedigd. Daarnaast ligt het voor de hand om het vestigingsklimaat voor criminele bendes onaangenamer te maken. Ook kan de strafmaat worden verhoogd, zoals sommige experts bepleiten.

Effectieve preventie lijkt echter vooral heel moeilijk en in eerste instantie een maatschappelijke opdracht. De rol voor de politie in deze moeilijk haalbare

ambitie is beperkt. De hamvraag is of de politie moet inzetten op het ontwikkelen of onderhouden van preventiecapaciteiten. Het is goed denkbaar dat deze capaciteiten beter bij andere organisaties worden belegd.

Intelligence en analyse:

Het is cruciaal dat de politie capaciteiten ontwikkelt en verbetert die hen in staat stelt de bronnen van ondermijning in beeld te brengen, werkwijze van criminelen te begrijpen en te monitoren (in *real time*). Dit is een kerntaak van de politie in de misdaadbestrijding. Het monitoren en begrijpen van processen rond ondermijning vergt structurele aandacht voor een verscheidenheid van domeinen en ontwikkelingen:

- De politie kan niet zonder een duidelijk beeld van de reikwijdte, bemensing, werkwijze en kracht van de Nederlandse drugsindustrie (inclusief hennepteelt). Naast klassiek opsporingsonderzoek vraagt dit om een bijna wetenschappelijk aanpak waarin de politie een combinatie van antropologische en journalistieke vaardigheden moet aanwenden om exploratief onderzoek te verrichten, waarbij ontwikkelde veronderstellingen als hypotheses voor verder onderzoek (data-analyse) worden ingezet. Dit werk is te belangrijk en te gevaarlijk om aan wetenschappers en journalisten over te laten. De politie moet de kennisvergaring en –analyse naar een nieuw niveau tillen om ondermijning goed in beeld te krijgen.
- Het is cruciaal dat de 'vruchtbare bodem' voor ondermijning in kaart wordt gebracht. Het gaat dan om een kwetsbaarheidsanalyse van lokale gemeenschappen en de instituties waarop zij leunen. Zonder dergelijke kennis is het onmogelijk grip te krijgen op het veelkoppig monster dat ondermijning is. Een combinatie van data-analyse en interdisciplinair wetenschappelijk onderzoek (sociologisch, bestuurskundig, juridisch) is nodig, maar het is niet nodig dat de politie dit zelf in huis haalt. Wel is een structurele relatie met onderzoeksinstituten nodig die deze kennis ontwikkelen en beschikbaar maken.
- De politie heeft 'early warning' mechanismen nodig die tijdige interventies mogelijk maken. Dat vereist een set van indicatoren die duiden op indringing van de bovenwereld door criminelen. Die indicatoren geven richting aan systematische dataverzameling. Deze informatieverzameling moet binnen de kaders van privacywetgeving worden ontwikkeld en uitgevoerd.
- De politie moet op de hoogte zijn van de laatste technologische ontwikkelingen (drones, soft intelligence, financial intelligence etc.).
- Ook moet de politie weten hoe witwassers te werk gaan, uit welke financiële bronnen politieke partijen putten, de weg kennen op het dark web, 'institutional voids' kunnen herkennen, en weten hoe outlaw motorgangs functioneren.

De behoefte aan informatie is enorm en het potentiële aanbod van relevante informatie nog veel groter. De beschikbare capaciteiten zijn per definitie beperkt. De inzet van dergelijke middelen wordt verder begrensd door privacywetgeving en ethische overwegingen. Dit betekent dat slimme keuzen moeten worden

gemaakt. De politie heeft daarom een adequate beleidstheorie nodig die de informatie-inzameling en-analyse stuurt. De kernvraag die moet worden beantwoord: Welke kennis hebben we nodig om onze doeleinden te kunnen bereiken? Hoe kan die informatie worden vergaard en wie kan dat het beste doen? De antwoorden op deze vragen vormen een beleidstheorie die helpt te bepalen welke capaciteitskeuzen gemaakt moeten worden.

Strategie- en besluitvorming:

De politie kan alleen grip krijgen op ondermijning met een scherpe definitie van het fenomeen die een duidelijke afbakening van de dreiging mogelijk maakt. In de literatuur worden veel verschillende strategieën geformuleerd, variërend van criminelen 'pesten' tot zeer ambitieuze pogingen gericht op het ontmantelen van drugskartels. Het gevaar van opportunisme en 'zwabberbeleid' ligt op de loer, terwijl juist een lange-termijn visie nodig is om alle benodigde capaciteiten te ontwikkelen. Dit betekent niet dat een strategie voor de eeuwigheid moet worden ontwikkeld. Integendeel, de bestrijding van ondermijning vereist de capaciteit om experimentele interventies in te zetten en te monitoren, zonder dat die de overkoepelende strategie ondermijnen. De strategie moet ook ruimte bieden voor de inzet van nieuwe technologieën, die na gebleken succes wellicht om een aanpassing van de strategie vragen. De benodigde capaciteit is dus strategievorming waarbij de lange-termijn visie ruimte biedt voor adaptaties die op de korte termijn kunnen worden doorgevoerd. Voor dogmatische benaderingen is geen plaats.

Operationele capaciteit:

De strijd tegen ondermijning vergt een groep professionals die over een grote verscheidenheid van hoogwaardige competenties moeten beschikken. Het betreft een combinatie van analytische vaardigheden, professionele kennis (juridisch, bedrijfsmatig, financieel, sociologisch, bestuurskundig, politicologisch, antropologisch), en netwerkmanagement (inclusief diplomatieke en communicatieve vaardigheden). In zekere zin lijken de vereiste capaciteiten meer op die van een inlichtingendienst dan van een traditionele politieorganisatie. Daarnaast zijn bepaalde interventiecapaciteiten nodig die betrekking hebben op o.a. financiële stromen, de aankoop van vastgoed en bedrijven, en handelingen in cyberspace.

Coördinatie:

De Landelijke Eenheid kan nooit beschikken over alle specialismen die nodig zijn om ondermijning tegen te gaan. Het speelveld is simpelweg te groot: van wijk tot internationaal belastingparadijs; van transportsector tot diplomatie. De kritieke capaciteit is het leggen en onderhouden van vruchtbare verbindingen. De verbinding met wijkteams is belangrijk, omdat daar de ondermijning direct voelbaar is. De verbinding met regionale recherche en internationale organisaties moet solide zijn. Maar de Landelijke Eenheid moet ook over politiegrenzen heen kunnen werken: met technologische organisaties, beleidsorganisaties, de financiële wereld, de belastingdienst, de lijst is lang. En ook hier geldt: van lokaal tot internationaal. De overkoepelende capaciteit ligt besloten in het idee van een hub waar cruciale informatie samenkomt en nieuwe strategieën en bijbehorende

allianties worden gesmeed. Coördinatie in dit dreigingsdomein is dus meer een kwestie van gefaciliteerde samenwerking dan verticale aansturing.

Communicatie:

De strijd tegen ondermijning is meer dan alleen opsporing en strafrechtelijke vervolging. Deze traditionele instrumenten van de staat zijn te beperkt, zo zeggen experts (Omand, 2018; van Hoboken en Ó Fathaigh, 2021; Europol, 2021). Burgers moeten meedoen, evenals bedrijven. Lokale bestuurders moeten hun rol pakken, evenals nationale politici. Alles begint met het herkennen en helder benoemen van het probleem. Dit alles vergt communicatie die is gericht op het veranderen van diepgewortelde assumpties (‘het valt toch allemaal wel mee’) en op het veranderen van gedrag. Dit vereist communicatie van het hoogste niveau. Ook hier is nadrukkelijk de vraag aan de orde of de LE dergelijke communicatie ter hand zou moeten nemen.

III. Openbare orde

Inleiding

Nederland heeft een rijke geschiedenis op het gebied van openbare orde verstoringen: de rellen in de jaren '60 (het Lieverdje), massale betogingen, de krakers-, kronings- en scholierenrellen, eindeloos veel voetbalvandalisme, de belaging van de Tweede Kamer na de moord op Pim Fortuyn; Project X in Haren, en, meer recentelijk, de Schilderswijkrellen, protesterende boeren, de *Black Lives Matter* demo in Amsterdam, de avondklokrellen en de gewelddadige rellen recentelijk in Rotterdam – de lijst is lang.

Het bewaken van de openbare orde is een traditionele kerntaak van overheid en politie. Door de jaren heen hebben bestuur, openbaar ministerie en politie veel kennis en expertise opgedaan. Zij beschikken over bewezen strategieën en treden doorgaans effectief op tegen mogelijke verstoringen van de openbare orde. Hoewel het aantal demonstraties is toegenomen en de burger mondiger is geworden door de jaren heen, blijft de veiligheid van de burger vrijwel altijd en overal gegarandeerd.

In Nederland lijkt de situatie vrij stabiel, ook volgens de experts. Het aantal aangemelde demonstraties neemt al jaren toe, maar het aantal problematische demonstraties lijkt niet significant toegenomen (maar betrouwbare cijfers ontbreken). Vooral internationaal nemen we zorgwekkende ontwikkelingen en gebeurtenissen waar (Giugni & Grasso, 2019; Portos, 2021; Bojar et al., 2021). Denk aan de dagenlange rellen in Londen, de gewelddadige BLM-rellen in grote steden, het plat leggen van het openbare leven in Frankrijk (Gilets Jaunes), en de bestorming van het Capitool in de Verenigde Staten. Het wakkert de vrees aan dat ons in Nederland nog een en ander te wachten staat.

Laten we eens kijken wat de onderliggende trends zijn, hier en in andere landen. We bedenken ook of er potentiële *game changers* op de radar zijn waar te nemen.

Trends

Polarisatie: Politicologen en sociologen hechten veel waarde aan een samenleving waarin mensen elkaar de ruimte laten hun leven in te vullen zoals zij dat willen. De bekende Amerikaanse politicoloog Robert Putnam trok in 2000 aan de bel met zijn boek *Bowling Alone*. Amerikaanse burgers raken onthecht van elkaar en de samenleving, zo waarschuwde hij.

Na de gebeurtenissen van 11 september 2001 is de polarisatie in de Verenigde Staten alleen maar toegenomen. De langdurige financiële crisis en de voortwoekerende COVID-19 crisis hebben deze trend vrijwel overal versterkt (Dikeç, 2018; Döring, 2020; Bartusevicius et al., 2021). De klimaatscrisis maakt veel los bij jongeren (Richardson, 2020). Polarisatie wordt aangewakkerd door groepen als Antifa en Proud Boys (en de vele varianten van deze groepen, zie bijvoorbeeld Lieber [2020] over de AfD). Ook in Nederland bestaan groepen die polarisatie voorstaan [NCTV Dreigingsbeeld]. Het vertrouwen in politieke instituties daalt gestaag (Busemeyer et al., 2021; Heinze et al., 2021; Engbersen et al., 2021; National Intelligence Council, 2021; Calvet & Di Nella, 2020; Peeples,

2020; Barker et al., 2021, Nassauer, 2021; Bartusevicius et al., 2021). Politiegeweld tijdens demonstraties leidt dan weer tot verdere daling in het vertrouwen (Shek, 2020; Heisler et al., 2020).

Disinformatie op social media: De manier waarop mensen nieuws tot zich nemen en informatie verzamelen is radicaal veranderd in de afgelopen twee decennia. Via computer en telefoon verbinden mensen zich met een grote hoeveelheid social media. Veel mensen hebben hun eigen informatiestructuren gecreëerd. Zij nemen dagelijks kennis van grote hoeveelheden informatie die hen razendsnel bereikt (Lim & Bouffanais, 2019; Ting, 2020; Helberger, 2020; Rebrenina et al., 2021). Helaas bereikt hen ook veel informatie die niet geverifieerd is en die experts onder de categorie 'disinformatie' scharen (Zuckerman, 2019). Geruchten, complottheoriën, leugens en verdraaiingen, en inaccurate berichtgeving verdringen de geverifieerde nieuwsgaring die vroeger bepaalde wat de burger van de wereld wist of kon weten. De gemiddelde burger kan zich nu veel beter informeren, maar raakt ook steeds sneller het zicht op de werkelijkheid kwijt. Informatie wordt op waarde geschat door naar de afzender te kijken: als die vertrouwd wordt, zal het wel waar zijn. Deze nieuwe, vrijwel ongereguleerde informatieomgeving biedt ongekende mogelijkheden voor de moedwillige informatie van geruchten en complottheorieën die maatschappelijke polarisatie aanscherpen.

Mobiliserend en faciliterend vermogen van social media: Het is makkelijker geworden om een demonstratie te organiseren (Rhingold, 2006; Lim & Bouffanais, 2019; Rebrina et al., 2021). Oproepen via social media bereiken veel mensen. Het is ook makkelijker geworden om de organisatie van een demonstratie buiten het zichtveld van meekijkende autoriteiten te houden (Ting, 2020). Ook kunnen deelnemers makkelijk handige tips vinden en delen ('hoe maak ik een Molotov cocktail?'). Tijdens een demonstratie kan het collectieve gedrag van demonstranten makkelijk worden (bij)gestuurd met behulp van social media (Poell & Van Dijck, 2018; Rebrina et al., 2021). Demonstranten kunnen zichzelf organiseren via social media. Dit alles zorgt ervoor dat autoriteiten gemakkelijk verrast kunnen worden door de plaats, het moment, de schaal en de dynamiek van een demonstratie. Daarnaast kunnen groepen social media gebruiken om in *real time* gebeurtenissen te framen: korte, suggestieve filmpjes worden gepost met als doel woede aan te wakkeren en te kanaliseren (Adam-Troian et al., 2020a; Rebrina et al., 2021).

Van scherm naar straat-praktijken: Aansluitend bij het vorige punt kan worden vastgesteld dat de social media niet alleen leidt tot snelle mobilisering, maar dat social media praktijken ook letterlijk op straat worden overgenomen. Realtime rellen worden via social media verspreid, beelden worden gedeeld, geliked, tiktok-achtige challenges worden verstuurd, waardoor de rellen soms bijna een 'game-achtige' situatie voor jongeren lijken te worden. Het leidt tot instant, flashmob-gedrag en relschoppen op straat, opboksen tegen elkaar door etalages in te schoppen voor meer likes bijvoorbeeld, concurreren met groepen elders, waarna de groep demonstranten ook zo weer uiteen valt. Ook beelden van rellen in het buitenland worden op die manier gedeeld. Rellen kunnen voortkomen uit hybride situaties, waarbij jongeren (of ouderen, zie de arrestatie van een 60-

jarige vrouw in Utrecht, (https://www.nu.nl/utrecht/6113445/vrouw-60-uit-utrecht-aangehouden-voor-oproep-om-te-rellen-in-de-stad.html) thuis oproepen tot rellen uitzetten, beelden verspreiden, die dan spontaan door groepen op straat worden opgepikt, inclusief bijbehorende hashtags.

Decentralisatie van sociale netwerken: De actiegerichtheid van mensen wordt in toenemende mate gekanaliseerd los van bestaande maatschappelijke en politieke structuren (Kilcullen, 2013; Lefebvre, 2019; Mendonca & Bustamante, 2020; Roth, 2018). Waar demonstraties nog niet zo heel lang geleden werden georganiseerd of gefaciliteerd door vakbonden, NGO's, en politieke partijen is vandaag meer sprake van losse, ad hoc verbanden van mensen die elkaar via social media hebben gevonden (zie ook punt hierboven). Allerlei groepjes, niet direct ideologisch verbonden, weten elkaar snel te vinden (de ene groep maakt opportunistisch gebruik van het initiatief van een ander). Demonstraties nemen het karakter aan van *leaderless movements* (Poell & Van Dijck, 2018): het is dus niet altijd duidelijk wie de 'eigenaar' van de demonstratie is (en wie kan worden aangesproken door autoriteiten).

Toename bereidheid geweld te gebruiken: De misdaadcijfers gaan in veel landen al jarenlang omlaag. Dit geldt ook voor het gebruik van geweld (CBS, 2018; Aarten en Liem, 2021). Tegelijkertijd lijkt een relatief kleine groep mensen juist meer bereid om geweld in de openbare ruimte te gebruiken (Burgers, 2021). Bij protesten in Rotterdam (19 november 2021) werden politie en ME geconfronteerd met gemaskerde demonstranten die probeerden veiligheidspersoneel te raken (met mortiervuurwerk bijvoorbeeld), en dat ook te livestreamen. Dat dwong de politie ertoe met scherp en gericht terug te schieten. Die verharding kan leiden tot rellen met een nog groter vuurwapen-, verwondings- en radicaliseringsgevaar.

Ook het gebruik van politiek gemotiveerd geweld lijkt te stijgen. Zo steeg politiek gemotiveerd geweld in Duitsland met 47.9% tussen 2011 en 2020 (en met 68.5% sinds 2001) (BKA, n.d.).

Georganiseerd geweld in de openbare ruimte: De opkomst van motorclubs die geweld in de openbare ruimte niet schuwen baart al jarenlang zorgen. In Zweden vechten leden van dergelijke clubs hun vetes op gewelddadige wijze uit in de openbare ruimte (Rostani & Mondani, 2019). Ook in Nederland was al eerder sprake van het uitvechten van vetes tussen motorclubs in de openbare ruimte (No Surrender vs Harley's Angels in Amsterdam (2013); HA vs Bandidos in Sittard (2014); HA vs Monguls in Rotterdam (2016)). Verder zien we ook andere groepen waar het gebruik van geweld gemeengoed is (denk aan hooligans). Wanneer georganiseerde misdaad banden aanlegt met groepen die snel in staat zijn om zich gewelddadig te organiseren kan zij een intimiderende werking hebben op de openbare ruimte. Dit komt voor zover bekend nauwelijks voor in Nederland (motorgangs en hooligans weten elkaar in sommige steden goed te vinden). Een dergelijke relatie komt in andere landen met enige regelmaat voor (Kilcullen, 2013).

Militarisering politie: De politie krijgt in veel landen de beschikbaarheid over verbeterde uitrusting en een verbreding van het geweldsspectrum (Doumani &

Dakwar, 2020; Gaffney et al., 2020); Pearl et al., 2021). In de Verenigde Staten kunnen we spreken van de militarisering van de politie. Ook in Nederland wordt het geweldsinstrumentarium stapje voor stapje uitgebreid (pepperspray, stroomstootwapens, meer kogels, waterkanonnen). De militarisering kan, zo vrezen sommige experts, geweldsescalatie in de hand werken.

Game changers

Gebruik van vuurwapens tijdens demonstraties: In Nederland spelen geen vuurwapens geen rol tijdens demonstraties. We zien echter wel een toename van wapenbezit. We zien ook een toename van grof geweld in het criminele circuit. Wanneer meer en meer mensen gemakkelijk toegang tot een vuurwapen hebben, kan het een kwestie van tijd zijn voordat mensen hun wapen gebruiken tegen politieagenten. Dat zou een heftige schok teweeg brengen en gevolgen kunnen hebben voor de bejegeningsstrategie van de politie (nu voornamelijk gericht op communicatie).

Politieke inzet van stoottroepen: Wanneer een band ontstaat tussen politieke bewegingen en groepen die geweld niet schuwen, ontstaat een ernstig risico voor geregisseerd straatgeweld. De geschiedenisboeken bieden voorbeelden ten over, die teruggaan tot het Romeinse Rijk. Vandaag de dag zijn er voldoende landen waar gebruik wordt gemaakt van gewelddadige milities. Nederland kent dit verschijnsel niet. Elke ontwikkeling in die richting moet worden aangemerkt als gevaarlijk (Miller, 2021).

Plotselinge en dramatische delegitimering van bevoegd gezag: Als het bestuur van een land of een stad plotseling wordt geconfronteerd met een diepe vertrouwenscrisis, die de relatie tussen burger en staat op de proef stelt, dan ligt het gevaar van spontaan geweld op de loer (Boin et al., 2020). Een dergelijke situatie komt zelden voor (de Amsterdamse kroningsrellen en de belegering van het parlement na de moord op Fortuyn komen nog het dichtstbij). Als burgers het vertrouwen in de staat verliezen en verontwaardigd zijn over het disfunctioneren van publieke instituties, dan zou dit kunnen leiden tot langdurige protesten die in meerdere plaatsen gebeuren (Dikeç, 2018).

Internationale interferentie: Inmenging in binnenlandse aangelegenheden wordt doorgaans niet door een staat getolereerd. In recente jaren is het echter steeds makkelijker geworden voor vijandig gezinde mogendheden om burgers te bestoken met disinformatie via social media, soms gebruikmakend van informatie die via hacks is verkregen. De Zweedse overheid kreeg hier onlangs nog mee te maken (en heeft onlangs een Psychological Defence Agency opgericht). De Verenigde Staten en Israël zijn al enige tijd object van buitenlandse inmenging. Het doel is burgers tegen elkaar op te zetten en hun vertrouwen in publieke instituties te ondermijnen. In de VS zijn gevallen bekend waarbij buitenlandse inmenging direct aanzette tot confrontatie tussen groepen. In Nederland is dit voor zover bekend nog niet gebeurd. Als het gebeurt, mogen we gerust spreken van een *game changer*.

Benodigde capaciteiten

De Nederlandse politie heeft ruime ervaring met openbare ordeverstoringen. Het gaat ze doorgaans goed af. We nemen nieuwe ontwikkelingen waar en zien enkele potentiële *game changers*, maar de verwachting is niet dat radicaal nieuwe capaciteiten nodig zijn op afzienbare termijn. Hieronder bezien we welke organisatiecapaciteiten nodig zijn:

Preventie:

Het is onmogelijk om elke verstoring van de openbare orde te voorkomen. Een goede kennispositie is elementair. Wie gaat iets organiseren? Werken ze samen met politie en bestuur? Hoe kan het gedrag van onwilligen (denk aan hooligans) worden ingeperkt en gekanaliseerd? Het zijn capaciteiten die over tijd worden opgebouwd. De nieuwe ontwikkelingen stellen nieuwe uitdagingen (nieuwe actoren, nieuwe geweldspatronen). Dat maakt een investering in de 'slimheid' een permanente noodzaak (zie volgend punt). Daarnaast is het belangrijk dat kleine gemeenten, waar geen capaciteit bestaat om al heel vroeg in het proces gewelddadige demonstraties in de kiem te smoren, proactief worden ondersteund.

Intelligence en analyse:

Er zijn eigenlijk drie typen kennis en vaardigheden die in de toekomst meer gewicht zullen krijgen: 1) kennis van maatschappelijke verschuivingen, legitimiteit en vertrouwen (politicologische en sociologische kennis); 2) diepe kennis en beheersing van social media processen (beeldvorming en framing); en 3) kennis van veranderende geweldsdynamiek. Het gaat, met andere woorden, om kennis van de processen die tot gewelddadige escalatie leiden. De politie kan niet zonder een goed gevoel voor maatschappelijke ontwikkelingen en mogelijke gevolgen. Zonder deze kennis groeit de kans op onaangename verrassingen. Dit is niet een kwestie van meer academisch geschoolde mensen aannemen. Het is waarschijnlijk beter om structurele samenwerking met sociale wetenschappers en criminologen op te tuigen. Ook structurele samenwerking met communicatiewetenschappers zal vruchten afwerpen (de ontwikkelen rond social media en gedrag op social media zijn nauwelijks te volgen). Wat nodig is: een slimme organisatie, slimmer worden door omgaan met andere slimme organisaties. Daarnaast blijft een constante investering in de eigen analisten van groot belang. Dit zorgt ervoor dat zij *in real time* het ontstaan en de escalatie van gewelddadige openbare ordeverstoringen kunnen volgen. Het blijft belangrijk om deze analyses snel bij de juiste besluitvormers te krijgen.

Strategie- en besluitvorming:

Twee typen strategische discussie zullen in de toekomst nodig blijken. Een belangrijke discussie betreft bejegening. De Nederlandse politie is, met recht, trots op de bejegeningsstrategie die het over de jaren heeft ontwikkeld. De vraag is of die strategie aanpassing behoeft als georganiseerd geweld in de openbare ruimte significant toeneemt. Een andere belangrijke discussie betreft 'timing': op welk moment grijpt de politie in? Meer kennis zal meer interventiemogelijkheden genereren. De verleiding zal groot zijn om een *precautionary approach* te volgen, maar zo'n benadering staat als snel op gespannen voet met rechtsstatelijke

principes. Dit vergt intense deliberatie die tot een duidelijke visie leidt. Het moge duidelijk zijn dat de politie dergelijke discussies met relevante partners dient te voeren. Een duidelijke positiebepaling is dan wel nodig.

Operationele capaciteit:

De geschetste uitdagingen vragen niet alleen om meer mensen en meer technische middelen (die zijn natuurlijk altijd welkom, denk bijvoorbeeld aan inzet van drones, big data, robotica, mixed reality), maar vooral om een investering in kennis. Die kennis hoeft niet altijd in huis te worden gehaald. Slimme allianties met slimme organisaties bieden veel meer mogelijkheden (waaronder ook het ophalen van lessen die in andere landen zijn opgedaan). Daarnaast zal het nodig zijn om snel bijstand te organiseren in gevallen van plotseling oplaaiend geweld (of geweld dat op meerdere plaatsen tegelijk plaatsheeft). De organisatie van bijstand op heel korte termijn kan gevolgen hebben voor de verticale gezagsrelaties binnen de politie.

Coördinatie:

De samenwerking op het gebied van openbare orde verloopt volgens gebaande paden. Goed functionerende arrangementen moeten worden onderhouden, maar er moet ruimte worden gemaakt voor nieuwe arrangementen die de snelheid van bijstand kunnen verhogen (in het licht van de toenemende onzekerheid). De vraag is of de huidige bestuurlijke arrangementen het mogelijk maken om op heel korte termijn bijstand te kunnen organiseren.

Communicatie:

Nieuwe dreigingen zullen een nieuwe verhaal vragen. Toen voetbalvandalisme groteske vormen begon aan te nemen, worstelde de politie met het formuleren van een verhaal (Wat is de rol van de politie? Hoe gaan we om met hooligans?). Als de politie wordt verrast door plotseling escalerend geweld in de openbare ruimte, heeft de politie vaak moeite om uit te leggen hoe dat zo is gekomen. De politie zal hard moeten werken om het publieke vertrouwen (traditioneel hoog in Nederland) te blijven verdienen. Frisse communicatiestrategieën zullen nodig zijn als de politie in unieke en heel onaangename situaties terecht komt.

IV. **Terrorisme**

Inleiding

Terrorisme is in Nederland sinds 2004 een officieel misdrijf, maar is al veel langer onderwerp van beleid en bestuur. In de publieke en politieke discussie is het inmiddels een veelbesproken thema en heeft het betrekking op het plegen of dreigen van geweld met een terroristisch oogmerk. Zo'n oogmerk omvat, aldus de Nationaal Coördinator Terrorisme en Veiligheid (NCTV) het willen ontwrichten van de samenleving, het angst aanjagen van (delen van) de bevolking, dan wel het willen afdwingen van een politieke reactie van uit de overheid. Volgens experts gaat het terroristen om de drie 'R's' – 'revenge, renown, reaction' (Richardson, 2006), waarbij daar (soms) ook een vierde 'r' van radicale verlossing aan toe kan worden gevoegd die meer op de radicale geloofs- of levensbeschouwelijke overtuiging doelt van het zich willen opofferen om anderen (of zichzelf) te bevrijden van onrecht en te verlossen van tekort of onderdrukking (De Graaf, 2021a; Van den Bos, 2019).

Bij terrorisme gaat het om vraag en aanbod. Er moet een meer of minder gearticuleerde vraag zijn van jongeren op zoek naar houvast, identiteit, of gewoon avontuur en spanning. Toch kan zelfs de meest individuele 'lone operator' niet worden losgezien van het aanbod van een terroristische ideologie of levensbeschouwing (online of offline), van een beweging, organisatie of basis die in die ideologie, de middelen, en soms zelfs ook de fondsen voorziet. Terrorisme komt en gaat in golven van verschillende intensiteit, en verandert ook steeds van ideologische/religieuze/politieke inhoud (Rapoport, 2022).

Trends

De aard van de terroristische dreiging is veel fluïder geworden: De afgelopen vijf jaar is de speler met de meeste aantrekkingskracht op het toneel van wereldwijd terrorisme behoorlijk onderuit gehaald. Het 'Kalifaat' als bestaand grondgebied met een de facto bestuur, slagvaardige internationale organisatie en bijbehorend kapitaal bestaat in de vorm zoals deze van 2014 tot 2017 functioneerde, niet meer. Daardoor is het aantal jihadistische aanslagen en internationale plots afgenomen, ook al worden nog regelmatig 'lone operators' aangehouden en zelfs een enkele samenzwering ontdekt en voorkomen (in Eindhoven vonden in september 2021 arrestaties plaats van een groep mannen die verdacht werden van het voorbereiden van een terroristische aanslag).

Alhoewel de NCTV en Europol de dreiging van jihadistisch terrorisme nog steeds volgens het hoogste niveau inschatten, is de dreiging van extreemrechts extremisme en terrorisme verhoudingsgewijs sneller gegroeid. De aantallen blijven nog achter bij de numerieke dreiging die van jihadisten uitgaat, maar de NCTV spreekt in zijn laatste Dreigingsbeeld Terrorisme Nederland (DTN) van ca. 300 zeer jonge jongens (12-20 jaar) die vatbaar zijn voor rechtsextremistisch gedachtengoed (NCTV, 2021b). Daarnaast is er de afgelopen twee jaar (2020-2021) sprake van *aan de coronacrisis gerelateerde radicalisering*, denk aan de avondklokrellen in januari 2021, bedreigingen van gezagsdragers (Rutte, De Jonge, Kaag), en leden van het RIVM, aanslagen op GGD-teststraten en andere vormen van dreigementen via telegramkanalen en social media. Dit soort nieuwe,

minder ideologisch gearticuleerde dreigingen, poppen heel snel op, zijn soms ook weer heel snel voorbij, maar zijn in hun vluchtigheid zeer lastig in kaart te brengen – een respondent noemde de brandstichting bij zendmasten als voorbeeld.

Wat opvalt aan deze groep radicaliserende personen is dat het een *zeer hybride groep* is: Het zijn soms zeer jonge mannen, minderjarig nog. Maar tegelijkertijd zijn er ook vrouwen van boven de vijftig opgepakt. De lockdownmaatregelen hebben de fysieke organisatie van radicaliserende personen bemoeilijkt, maar online content vindt juist steeds meer verspreiding, voornamelijk vanuit de Verenigde Staten (voor wat extreemrechts betreft) (Davies et al., 2021).

De trend is dat *social mediapraktijken aard en vorm van radicalisering en terrorisme vrijwel volledig bepalen*: De beeldtaal van 'memes', de poging contact op te nemen via games, maakt het heel moeilijk de bronnen van verspreiding van radicaal gedachtengoed aan te wijzen. Bovendien lopen offline en online naadloos in elkaar over; hashtags op Twitter, Telegram, Facebook en YouTube zien we op straat in spandoeken en in dreigpost terug. Ook de rol van 'influencers' op social media neemt toe: als die ineens complottheorieën gaan omarmen, neemt de verspreiding daarvan onevenredig toe.

Bovenstaande trend werkt ook *vermenging van extremistisch en terroristisch gedachtengoed* in de hand: de terroristische dreiging is niet meer helder aan één organisatorische bron, of zelfs aan één ideologie of religieuze stroming toe te schrijven. Er vindt een 'knip- en plak'-radicalisering plaats van allerlei complottheorieën (5G, hagedissen, corona, Great Reset), die aan bestaande extreemrechtse overtuigingen worden gekoppeld, aan antisemitisme of juist islamofobe ideeën, en zo een heel ongrijpbare en grillige vorm aan kunnen nemen. Extreemrechts wordt aan milieuactivisme gekoppeld (ecofascisme), maar ook aan anti-vaxxcomplotten.

Hetzelfde geldt voor de *snelheid waarmee radicalisering* zich voltrekt: Instant-radicalisering, of 'dark conversion' is het fenomeen dat mensen niet eerst meer eindeloos teksten bestuderen, of in een fysieke omgeving en organisatie worden gerekruteerd en geschoold, maar dat ze op basis soms van enkele filmpjes in een oogwenk de sprong nemen in het radicale diepe. Jonge mensen, maar ook ouderen (denk aan de 53-jarige Dieuwke P.) kunnen een vorm van extreem en militant martelaarschap omarmen en zich gaan richten tegen de overheid in wie ze 'het beest' zien waartegen ze in geweer moeten komen (De Graaf, 2021b). Dat kan van de één op de andere dag gaan, als er een platform is ('Bataafse Republiek' bijvoorbeeld) dat hen die mogelijkheid biedt.

Steeds vaker wordt een *correlatie tussen radicalisering en ggz-problematiek* vastgesteld (niet: persoonlijkheidsstoornissen!). De 'normaliteitshypothese' is een lastig fenomeen: hebben veroordeelde terroristen vaker last van persoonlijkheidsstoornissen dan niet-gedetineerden? Die vraag is vooralsnog ontkennend beantwoord (Thijssen, 2021). Maar in het proces van radicalisering rond lockdown en corona lijkt wel sprake te zijn van een correlatie met sociale kwetsbaarheden en depressie. Recent onderzoek toont die correlatie ook aan voor jihadisme en extremisme (Moonshot, 2020; Alberda et al., 2020; Alberda et al., 2021). Let wel: vastgestelde correlaties in onderzoek zeggen dus nog niets over aangetoonde en gecontroleerde diagnoses over pathologieën of

persoonlijkheidsaandoeningen. Het gaat hier over een mogelijke correlatie met kwetsbaarheden en depressie/eenzaamheid.

De zeer recente trend van afname van vertrouwen 'in de politiek' en verzet tegen anti-Covid-maatregelen (lockdown, 2G-regel) schept een voedingsbodem voor verdere verspreiding van complottheorieën, anti-overheidssentimenten en activiteiten en radicalisering: Daarbij is er volgens een respondent een 'continuüm van online oproepen tot protest, bedreiging, daadwerkelijke gewelddadige acties en voorbereidingen tot aanslagen', wat het lastig maakt de dreiging precies te omschrijven.

Game changers

Het staat buiten kijf dat voor de komende periode de verdere *continuering, intensivering of juist afname van lockdown- en anticoronamaatregelen* een direct effect heeft op de voedingsbodem voor radicalisering, in het bijzonder corona-gerelateerde radicalisering en bedreigingen van bijvoorbeeld OMT-leden.

Daarnaast hebben ook *significante ontwikkelingen elders, in het bijzonder in de VS*, gevolgen voor de mobilisatie van bijvoorbeeld anti-vaxx- en extreemrechtse radicalisering: Denk aan het onderzoek naar de Capitoolrellen, de mogelijke hernieuwde campagne van Donald Trump dan wel de toename van extreemrechts 'vigilantism' in de Verenigde Staten (vrijspraak van Kyle Rittenhouse). Organisaties als The Base en Atomwaffen Division met (online) bases in de VS hebben directe uitstraling en uitwerking op jongeren in Nederland (NCTV 2021b).

Ook *ontwikkelingen in het Midden-Oosten/Azië/Afrika* kunnen opnieuw uitstraling hebben op radicaliserende jongeren in Nederland: zal IS erin slagen opnieuw ergens een territoriale basis in te richten? Zullen vergelijkbare groepen in Afghanistan, of in Afrika oproepen plaatsen aan jongeren elders om zich te voegen in de strijd of in eigen land aanslagen te plegen? Vooralsnog is IS te gefragmenteerd, maar in Afghanistan probeert ze weer voet aan de grond te krijgen (Larres & Hof, 2022).

Datzelfde geldt voor het *effect van topontmoetingen op de internationale klimaatbeweging*: De recente COP26 wordt door organisaties als Extinction Rebellion als een mislukking gezien (Thunberg, 2021). Wordt de klimaatbeweging in haar heroverwegingen gekaapt of opgezweept door meer actiebeluste groepen, leiden teleurstellingen en gevoelens van 'klimaatschuld' tot frustratie en verharding? Ook anti-vaxx'ers en 'ecofascisten' lijken ingang te zoeken in de klimaatbeweging.

Aangezien huidige patronen van radicalisering sterk van social media afhankelijk zijn, is de *rol van het vernieuwde Facebook/Meta en de wijze waarop de tech-giganten werk gaan maken van detectie en identificatie* van radicalisering en hatecrime op hun platforms van doorslaggevend belang: Hoe gaan we in de toekomst om met anonimiteit (in Australië is een wet in de maak die anonimiteit en trolgedrag aan banden moet leggen)? Zullen techbedrijven meer zelfreinigende interventies plegen?

Een andere gamechanger relateert aan de *speelruimte van de overheid op social media* de komende jaren: Zal de AVG monitoren en surveillance verder aan banden leggen? Of wordt er, bijvoorbeeld naar aanleiding van recente onthullingen

over het gebrek aan rechtsgrond bij de NCTV (en Landmacht), alsmede over onderzoeksmethodes van particuliere onderzoeksbureaus een nieuwe discussie gevoerd over interventiemogelijkheden in de online wereld? De gemeente Utrecht heeft onlangs voor het eerst een online opruier een online gebiedsverbod opgelegd. Als dat standhoudt, betekent het een vergroting van de interventiemogelijkheid van de overheid (Algemeen Dagblad, 2021).

De laatste jaren is – met succes – geïnvesteerd in sleutelfiguren en in lokale verbanden ten behoeve van tijdige detectie en preventie van radicalisering: Door de langdurige formatie, ophef rond affaires (Toeslagenaffaire bijvoorbeeld), de lockdown, maar ook door bovengenoemde onthullingen is in de samenleving het vertrouwen in de lokale en/of landelijke overheid afgenomen. In de strijd tegen radicalisering is juist steun en vertrouwen vanuit de groepen (te denken valt aan moskeebesturen) hard nodig. Zullen koepels en gemeenschappen van moslims, maar ook orthodoxe christenen, de overheid blijven steunen als ze zich verder in de hoek gezet voelen?

Benodigde capaciteiten

Preventie:

De persoonsgebonden aanpak is een beproefd en een robuust instrument gebleken. De fenomeenanalyse, in het bijzonder gericht op preventie van online radicalisering blijft evenwel een enorme uitdaging. Er is veel meer kennis van radicale platforms en radicale groepen nodig. De politie moet meer investeren in kennis en inzicht omtrent zogeheten 'van-scherm-naar-straat'-processen (Bakker et al., 2021). Is dit modernisering van de ouderwetse 'van-pamflet-naar-straat' beweging, of is er echt een kwalitatieve en kwantitatieve (want zeer versnelde) ontwikkeling aan de gang? Dat laatste wordt inmiddels door onderzoekers wel geconstateerd. Dat is tegelijk een zeer problematische uitdaging in het licht van de AVG-discussies en obstakels voor de autoriteiten om social media accounts van burgers te mogen monitoren.

Detectie en intelligence:

Zie hierboven. Hoe mogen de autoriteiten, in het bijzonder de Landelijke Eenheid omgaan met open source intelligence en het monitoren van social media accounts van burgers? Hoe wordt er naar accountability en transparantie gestreefd? Een stap kan zijn dat de politie ook haar eigen schaduw monitort, met andere woorden, in kaart kan brengen wat de gevolgen van eigen interventies zijn (actie-reactie-radicalisering). Verder geldt dat Nederland vaak netto-ontvanger (in tegenstelling tot veroorzaker of bron van terroristische groepen) van ontwikkelingen in het buitenland is. Bij detectie kan worden binnengehaald en gemonitord wat er in Duitsland, België, het Verenigd Koninkrijk en de Verenigde Staten aan radicalisering gaande is. Veel daarvan zal zich ook in Nederland (gaan) voordoen.

Tegelijkertijd vindt alle radicalisering, hoe individueel en gefragmenteerd ook, ergens, op een lokaal adres, plaats. Is er genoeg continuïteit van operationeel experts ter plekke, die ook langer dan een paar jaar in een wijk gestationeerd zijn, en die hun informatie en interpretatie aan de LE kunnen doorgeven? Nu lijken de portefeuillehouders en operationeel experts wel heel snel te wisselen, zo vindt er

geen kennisopbouw plaats. Daar is winst te behalen. In het bijzonder ook op het vlak van samenwerking met AIVD.

Analyse:

Hoe ziet terrorisme er de komende vijf jaar uit? Er dient meer oog te zijn voor diverse, en ook razendsnel veranderende en fluïde vormen van religieuze, ideologische, ongearticuleerde anti-overheidsradicalisering. Ook analyse van trends in omringende landen is zeer relevant. Daarnaast wordt radicalisering vaak getriggerd door concrete (vermeende) 'onrechtservaringen' (Della Porta, 1995; Van den Bos, 2019). Politieoptreden kan zo'n trigger zijn. Ook hiervoor geldt: in de analyse samenwerken met goed ingevoerde medewerkers van veiligheidshuizen, veiligheidsmedewerkers van de gemeente en operationeel experts is essentieel. Zij weten wat op lokaal niveau de triggers kunnen zijn.

De LE is er voor landelijke operationele taken, maar ook voor ondersteuning en samenwerking met regionale eenheden, in het bijzonder ook met het oog op analyse. Omdat er regionaal sneller ad hoc wordt opgetreden – en dus wordt afgeschaald wanneer het gaat om een sterk conjuncturele dreiging als terrorisme en radicalisering – is het zaak dat er binnen het leiderschap van de LE oog is voor continuering en doorgaande investering in de analysecapaciteiten op dit dreigingsdomein. Dat betekent dat er geïnvesteerd moet worden in specialisten op verschillende vormen van radicalisering. Dat er oog is voor ontwikkelingen in het buitenland, dat er vaker wellicht ook aan uitwisseling van analisten (landelijk-regionaal, nationaal-internationaal) wordt gedaan.

Het is ook zaak te onderkennen dat de hybride, fluïde aard van de dreiging samenhangt met de ontwikkelingen van social mediapraktijken in de samenleving. De politie kan zich niet afschotten, maar zou hier nauwer en sneller met onderzoekers aan hbo's en universiteiten moeten samenwerken, waar het gaat om vroegtijdige detectie, signalering, verzamelen van intelligence en – in het bijzonder- analyseren van nieuwe trends en disruptors. Om blinde vlekken en tunnelvisie te vermijden – iets dat op dit zeer gepolariseerde en gepolitiseerde dossier vaak voorkomt – is het te overwegen dat de LE net als het Ministerie van Defensie bij de analyse ook aan Red Teaming gaan doen, en tegendenkers vanuit de eigen gelederen en/of van buiten uitnodigt.

Daarbij staat voorop dat het opleidingsniveau van de analisten van de LE gelijke tred dient te houden met het verhoogde opleidingsniveau en de digitale geletterdheid van de 'agents of disruption' in de samenleving.

Strategie- en besluitvorming:

Met het oog op de strategie voor de lange termijn is het zaak dat de politie, de NCTV en de veiligheidsdiensten zich niet vastleggen op de dreiging van gisteren. Openheid en definiëring van de dreiging in al zijn vloeibare, grillige, zeer dynamische en veelzijdige vormen zijn essentieel. De strategie moet niet alleen op jihadisme en rechtsextremisme zijn gericht, maar ook op nieuwe, diffuse, 'irrationele' ideologieën of samenzweringstheorieën die eveneens tot radicalisering

kunnen leiden. Daarnaast is aandacht nodig voor de rechtsstatelijke en mensenrechtelijke componenten. Uitvoering wordt vaak aan de rechter overgelaten, of aan de burgemeester terwijl zowel de magistraten, lokale bestuurders als bewindspersonenen meer van de discretionaire bevoegdheden gebruik kunnen maken (denk aan het ontnemen van staatsburgerschap). Ook in de toekenning van de strafmaat bepaalt elke rechter welke voorwaarden worden toegepast. Met het oog op recidive en re-integratie is het belangrijk hier een gestroomlijnde afstemming en strategie op toe te passen.

Operationele capaciteit:

Terrorisme is een fenomeen met grote impact en een lage waarschijnlijkheid. Plaatselijk wordt er snel afgeschaald als de dreiging als minder urgent wordt gezien (ten opzichte van drugscriminaliteit bijvoorbeeld). De LE moet investeren in blijvende operationele capaciteit, niet alleen met het oog op arrestaties, maar ook in het aansturen, afstemmen van detectie en analyse. Zijn er plaatselijk genoeg 'eyes and ears' aanwezig, is er continuïteit in de omgang met de netwerken waar de politie het van moet hebben in preventie en detectie?

Coördinatie:

Met het oog op de huidige trend van corona-gerelateerde en complotgedreven radicalisering is het zaak de correlatie met depressie, eenzaamheid en geestelijke gezondheid ook institutioneel te beleggen. Coördinatie tussen instanties in het veiligheidsdomein en die in het sociale domein, geestelijke gezondheidszorg, onderwijs, jongerenwerk is essentieel en kan beter – een taak die wellicht eerder voor de NCTV is weggelegd, maar waar ook de LE een rol in kan spelen gezien haar uitvoerende karakter. Uit recent onderzoek in Arnhem blijkt dat scholen vaak terughoudend zijn in het melden van radicaliseringsincidenten bij de gemeente en de politie. Lokale wijkagenten, operationele experts kunnen in samenwerking met de LE een cruciale rol spelen in het coördineren van persoonsgebonden aanpak en preventieve fenomeenanalyse. Hiervoor zou ook een netwerk van analisten kunnen worden opgeleid dat bijvoorbeeld de ronde doet langs diverse organisaties in de veiligheidsketen (zie ook het hoofdstuk over de cyberdreiging), zoals door een respondent werd voorgesteld. Dat verhoogt de bekendheid met elkaar, vergroot de kracht van het veiligheidsnetwerk, en stroomlijnt het bewustzijn rond de aard van de dreiging bij de verschillende partners.

Communicatie:

Communicatie op dit domein is landelijk bij NCTV belegd. Maar hoe moet de politie communiceren over nieuwe trends? Met welke doelgroepen of gemeenschappen zou de politie moeten communiceren? Kan politie met marginale minderheden en (geloofs-)gemeenschappen in gesprek blijven? Kunnen er operationele experts meerdere jaren in een gebied en op het thema van radicalisering geplaatst blijven, zodat de kennis en het vertrouwensnetwerk op niveau blijven? Te vaak worden vertrouwde gezichten verplaatst, wordt er gereorganiseerd en gereshuffeld waardoor de communicatie het met steeds weer nieuwe gezichten moet doen. Dat werkt in dit domein niet vertrouwenwekkend, zeker niet in relatie met de essentiële maatschappelijke partners. In de communicatie met het buitenland en aanverwante organisaties valt eveneens terreinwinst te behalen.

V. Cybersecurity

Inleiding

'Computergerelateerde' misdaad werd al in de jaren negentig van de vorige eeuw als een probleem gezien. Formeel staat de cyberdreiging pas sinds 2011 op de nationale agenda toen de Nationale Cyber Security Strategie werd gepubliceerd. Het jaar daarop werd de Cyber Security Raad en een Nationaal Cyber Security Centrum (NCSC) opgericht, met als doel samen met relevante partijen in het private en publieke domein – waaronder de politie - bijeen te brengen en gezamenlijk uitvoering te geven aan de nationale veiligheidsstrategie.

Onder cyber crime verstaan we het fenomeen dat een computersysteem wordt aangevallen of misbruikt voor criminele activiteiten (CCV, 2019). Dat kunnen in brede zin alle strafbare activiteiten zijn waarbij iemand een informatiesysteem of computer gebruikt (diefstal en vervalsing van betaalpassen, het vergaren van kennis (spionage), oplichting, afpersing, kinderporno, racisme en belediging). Het kan ook cybercriminaliteit in enge zin zijn, waarbij informatiesystemen en computers niet het middel zijn maar het doel: cybersabotage, spamaanvallen, DDoS-aanvallen, virussen verspreiden. Digitale veiligheid is de uitkomst van 'het geheel aan maatregelen om schade door verstoring, uitval of misbruik van ICT te voorkomen en, indien er toch schade is ontstaan, het te herstellen' (NCTV, 2020).[2]

Het NCSC werkt nauw samen met de NCTV, de Joint Sigint Cyber Unit (JSCU) (van AIVD en MIVD gezamenlijk), regionale eenheden alsmede het Team High Tech Crime (THTC) van de politie en het ministerie van Defensie. Onder cyberdreigingen worden immers ook spionagepogingen en (staatsgestuurde) buitenlandse hacks verstaan. In 2018 publiceerde het ministerie van Buitenlandse Zaken de Integrated International Security Strategy 2018-2022 waar cyberdreiging als één van de grootste dreigingen voor Nederland werd beschouwd, inclusief de combinatie met hybride en 'cyberwarfare'.

Nederland scoort niet het hoogst op de landen die in de frontlinie van cyberaanvallen staan (Romaniuk & Manjikian, 2021). De digitale weerbaarheid is volgens de officiële rapporten, bijvoorbeeld het CBSB, hoog[3], en het JSCU heeft in 2018 met succes een poging tot cyberspionage gestopt en verijdeld. Tegelijkertijd laten de Diginotar-affaire, succesvolle ransomware-aanvallen op ziekenhuizen en universiteiten, alsmede op het MKB en particulieren zien dat de cyberdreiging reëel is. Hoofdofficier Michiel Zwinkels, binnen het OM portefeuillehouder cybercrime zei hierover in 2021: 'Hoewel het Cyber Security Beeld Nederland beschrijft dat er in Nederland tot nu nog geen aanval op een

[2] In het CSBN 2021 is de definitie uitvoeriger geformuleerd. Cybersecurity is: 'het geheel aan maatregelen om (relevante) risico's tot een aanvaardbaar niveau te reduceren. De maatregelen kunnen zijn gericht op het voorkomen van cyberincidenten en wanneer cyberincidenten zich hebben voorgedaan deze te ontdekken, schade te beperken en herstel eenvoudiger te maken. Wat een aanvaardbaar niveau is, is de uitkomst van een risicoafweging' (NCTV, 2021a).

[3] Aldus de officiële verslagen; onlangs liet evenwel vertrekkend minister van Defensie Henk Kamp zich veel negatiever over de stand van de weerbaarheid uit, zie *NRC Handelsblad*, 3 januari 2022.

vitaal proces heeft plaatsgevonden, betekent dat niet dat er géén cruciale processen zijn verstoord' (Politie.nl, 2021).

Trends

De *cyberdreiging is in toenemende mate grenzeloos en dynamisch*: Cybercrime surft mee op de razendsnelle ontwikkelingen in het digitale domein. Onder het motto 'crime as a service' (zie ook p. 5) zijn er steeds meer actoren, partners in de cybercrime-keten die vanuit de hele wereld opereren. Anders dan bij traditionele criminaliteit en klassieke veiligheidsdreigingen is bij deze dreiging de afstand tot slachtoffer en dader heel groot. Eén dader kan bovendien duizenden slachtoffers maken. Dat maakt preventie en detectie zo complex, zeker omdat preventie en opsporing institutioneel nog zo lokaal zijn opgehangen (denk aan de lokale driehoek).

Nederland is in verhouding tot andere landen *digitaal zeer goed verbonden en ontsloten*: Nederland ziet zichzelf als een *early adopter* van nieuwe technologie en de bijbehorende instanties en reguleringsmechanismen, en heeft als ambitie de '*Digital Gateway'* van Europa te zijn, met de haven van Rotterdam, Schiphol en de Amsterdam Internet Exchange als wereldwijde knooppunten van goederen, verkeer en vooral data en systemen. Maar liefst 95 procent van de Nederlandse huishoudens is op snel internet aangesloten, 4G is vrijwel overal uitgerold en de digitale geletterdheid is hoog. Bovendien zijn al die voorzieningen de afgelopen twee jaar door het thuiswerken en online vergaderen nog verder uitgebreid. Dat betekent ook dat de kwetsbaarheid voor cyberaanvallen hoog is en groeit (omdat particulieren die thuisweken vaak minder goed beveiligen dan bedrijven).

Nederland doet mee in de eerste *lijn van landen die binnen de EU en de NAVO samenwerken op het vlak van digitale veiligheid*: De ambitie daarbij is om aan internationale vrede en veiligheid bij te dragen, door veilige hardware en software te ontwikkelen, mee te denken over het ontwikkelen van weerstand en barrières tegen aanvallen in EU- en NAVO-verband, en de internationale rechtsorde actief te verdedigen tegen cyberaanvallen. Dat betekent ook dat Nederland werkt aan wetgeving om digital fraude, digital diefstal, en hacks beter te kunnen penaliseren en te vervolgen (door strafrecht en strafprocesrecht aan te passen).

Tegelijkertijd zijn de *actoren van cyberonveiligheid ook steeds professioneler* en opereren die ook steeds meer in internationaal verband: De ransomwareketen liet de afgelopen tijd zeer professionele spelers zien, zowel bij het bouwen, plaatsen, weghalen en afpersen van de slachtoffers van de cyberaanvallen. 'Cybercrime as service' floreert, functioneert beter, sneller en internationaler.

Cryptovaluta maken het in het kader van 'follow the money' nog ingewikkelder zo niet vrijwel onmogelijk bij de financiële bronnen van cyberdreigingen te komen.

Tegelijkertijd is '*cyber shame'* nog steeds de trend: bedrijven, particulieren, publieke organisaties vermelden liever niet dan wel dat ze gehackt zijn, dat er ransomware is geplaatst en dat er iets aan de hand is. Mensen en bedrijven doen vaak niet aangifte, of proberen het via particuliere bedrijven op te lossen,

waardoor de overheid en de politie soms te weinig zicht hebben op de omvang van de dreiging.

Cyberdreiging afkomstig van staten, dus als voortvloeisel van interstatelijke, geopolitieke spanningen en klassieke spionage en sabotage is één van de grootste dreigingen op dit domein. Er zijn in Nederland nog geen vitale sectoren geraakt door deze vorm van dreiging. Wel heeft de MIVD informatie-operaties gericht tegen bondgenootschappelijke doelen in Nederland verijdeld. Ook digitale economische spionage is vastgesteld. De EU, en ook Nederland, gaan er in de cyberstrategie vanuit dat die statelijke dreigingen zullen groeien.

De coronacrisis leidt de afgelopen twee jaar ook tot gerichte, 'gethematiseerde' aanvallen, waarbij cyberaanvallen worden uitgevoerd op ziekenhuizen, onderzoeksinstituten, de WHO, het Europees Geneesmiddelenbureau (EMA), of andere instanties, experts, personen. Overlappend met de bovengenoemde coronaradicalisering, maar niet alleen daardoor, was er ook sprake van digitale aanvallen en pogingen (bijvoorbeeld van Vizier op Links, of andere groepen) persoonlijke gegevens van onderzoekers buit te maken. Daarnaast leidden ook phishing-pogingen die inspelen op corona, of andere crisissituaties tot miljoenen aan verliezen voor burgers en economie.

Game changers

In het algemeen is de *overgang naar een datagedreven samenleving* een gamechanger die de komende jaren allerlei vormen van dreiging met zich mee brengt. Of het nu om het internet-der-dingen gaat, om de snelheid waarmee de samenleving zich via social media organiseert en laat mobiliseren, of het nu om grenzeloze en grensoverschrijdende criminele netwerken gaat of om spionage: de transformatie naar zo'n datagedreven wereld zal de komende jaren nog sneller en veelomvattender zijn.

Publiek-private samenwerking kan tot een doorbraak in de strijd tegen cybercrime leiden: Het Openbaar Ministerie werkt aan een landelijk punt voor alle meldingen. Als het bedrijfsleven en particulieren hier daadwerkelijk aan mee gaan doen, leidt dit tot meer informatie en inzicht in de dreiging, en mogelijk tot een betere bestrijding. In de EU is een nieuwe beleidslijn (een EU Network and Information Security (NIS)-directive) in de maak, die mogelijk tot Europese en dus ook Nederlandse meldplicht gaat leiden. In dat geval zullen aangiftebereidheid en meldbereidheid omhoog schieten, en zullen er veel meer onderzoeken voor de politie bij komen (NIS Directive, 2016).[4]

De taskforce Ransomware werkt sinds kort niet alleen meer aan het 'afpakken van het wederrechtelijk voordeel', maar werkt samen met cybercrime teams en andere partners op meerdere actielijnen, om zo de pakkans te verhogen. Politie en OM delen gegevens internationaal, pakken de infrastructuur en servers aan waarop software draait, vervolgen malafide hostingbedrijven, facilitators, verkopers, kortom *het hele systeem rond het uitvoeren van cybercrime wordt systemisch aangepakt*. Dat kan een gamechanger zijn. Onlangs leidde dat al tot de arrestaties van enkele topverkopers van drugs op het darknet, volgens

[4] Er komt een nieuwe versie van deze wet aan.

onderzoekers een 'trendbreuk' (NOS, 2021).[5] Tegelijkertijd neemt daardoor eveneens het aantal onderzoeken en de vraag aan de politie om mee te doen in internationale acties toe.

Herijking van de AVG en vrijheid van meningsuiting: Door de toegenomen cyberdreiging is de discussie over bevoegdheden van overheden, politie en justitie toegenomen om gedrag van burgers en bedrijven op het internet te kunnen monitoren. Vooralsnog geldt een IP-adres als persoonsnummer, en valt daarmee onder de AVG. Mogelijk zal dat veranderen met de NIS 2. Mogen de krijgsmacht, politie en NCTV dan wel gebruik maken van open source intelligence en IP-adressen opvolgen en delen, zonder dat van een strafrechtelijk onderzoek sprake is?

Voor de handhaving is het van belang of er nieuwe wetgeving komt om het digitale domein te reguleren. Mogen burgemeesters *online gebiedsverboden* opleggen aan mensen van wie zij vinden dat die hun meningsvrijheid op het internet misbruiken om de veiligheid van anderen en van de openbare orde (door het oproepen tot rellen) in gevaar te brengen? Als de zeer recent geïnitieerde toepassing van onlinegebiedsverboden stand houdt voor de rechter, zal dat een gamechanger zijn in het handhaven van de veiligheid op het internet (Algemeen Dagblad, 2021).

De *uitbraak van concrete geopolitieke conflicten* zal de cyberdreiging online verhogen en doen overslaan naar het aantasten van offline systemen (Thompson et al., 2021): Te denken valt aan versterkte en verhevigde cyberaanvallen vanuit Rusland of China richting de EU, de VS of het Westen, inclusief Nederland, met het doel Westerse samenlevingen te ontwrichten en verkiezingen te beïnvloeden of te verstoren.

Benodigde capaciteiten

Preventie:

Preventie vereist meldplicht en een verhoogde aangiftebereidheid. Dat betekent weer dat de politie veel meer menskracht nodig heeft om aan die toegenomen aangiftes opvolging te geven. Er zijn in 2019 vier sectorale computercrisisteams ingezet om de zorg, gemeenten, waterschappen, onderwijs en onderzoek te beschermen. Voor samenwerking rond preventie zijn convenanten getekend. Met het oog op de genoemde trends en game changers zullen er veel meer van dit soort teams nodig zijn, en zal er ook voor de opvolging van aangifte, het ophalen van informatie vanuit die aangiftes (met het oog ook op preventie) meer menskracht en denkkracht nodig zijn.

Detectie en intelligence:

Detectie van een cyberaanval duurde in 2020 gemiddeld 56 dagen, waarbij de vertraging vooral te maken had met de late melding door de gedupeerde aan de

[5] 'Waar eerder dit soort operaties zich richten op het oppakken van beheerders van dit soort marktplaatsen en het in beslagnemen van de infrastructuur, zien we dat politiediensten zich nu hebben gericht op het arresteren van de topverkopers' (NOS, 2021).

politie. Basismaatregelen van organisaties bij het verhinderen van computervredebreuk zijn vaak niet op orde. Kunnen overheid, justitie en politie daar een rol in spelen, om daar beter op te handhaven? Zijn AIVD en MIVD niet te veel op monopolisten en commerciële bedrijven als Fox-IT aangewezen? En hebben die bedrijven een meldplicht om inbreuk op de cyberveiligheid te melden? Met de NIS 2 die inmiddels is uitonderhandeld, zal dit veranderen. De vitaalverklaring geldt nu voor 300 objecten en zal dan wellicht naar 15.000 objecten gaan. Dat betekent dat er met de nieuwe wetgeving die eraan komt, veel meer werk bij komt voor de politie om intell over vitale objecten te verzamelen, bij te houden, en op te volgen.

Overheden en internationale organisaties tasten vaak letterlijk in het duister als het gaat om toegang tot informatie op de private sociale media platforms. De EU en de VS hebben Facebook onder druk gezet om end-to-end encryptie niet uit te rollen. Dat kan het beste in internationaal verband worden gedaan. Nederland zou binnen de EU met Duitsland, dat voorop loopt met zijn 'network enforcement law', hier een voortrekkersrol in kunnen spelen. De politie moet nagaan wat haar rol en functie hier is (aangezien de teams van de LE hier met buitenlandse collega's operationeel vorm aan geven), of dat dit iets is voor NCSC en diensten die meer op beleidsmatig en politiek niveau opereren.

Een probleem hier is dat er 'op de markt' ook wordt gewerkt aan cyber threat intelligence (CTI) en dat die ook wordt verkocht en ingezet als asset voor cybersecurity gerelateerde bedrijven en partijen (Oosthoek en Doerr, 2020). Hoe kan de politie hiervan gebruik maken, onder welke voorwaarden werken organisaties als Kaspersky, of open source intelligence gebaseerde groepen als Bellingcat wel of niet samen met nationale overheden, en is dat dan ook te controleren onder de Wet op de Inlichtingen- en Veiligheidsdiensten (WIV) of de politiewet?

Analyse:

Analyse van data op het vlak van cyberdreiging kan verdrinken in een oceaan aan informatie. Want waar gaat het precies over en wie is ervoor verantwoordelijk? (Is cyberdreiging alles waar computers bij betrokken zijn – maar dan is het nauwelijks meer te begrenzen?). 'Er is geen regie', aldus een betrokkene. Cyber is een volstrekt gefragmenteerd domein, waar veel meer afstemming en stroomlijning nodig is. Doen analisten bij de cyberunit van de LE niet hetzelfde wat AIVD, MIVD, NCSC of NCTV doen? En richten ze zich op cybercrime, op het verspreiden van fakenews, phishing en fraude, datadiefstal, of ook op buitenlandse cyberaanvallen?

In het poldermodel van overlappende en horizontale samenwerking is het essentieel dat de analysevragen en analisten zelf samenwerken, maar ook gericht en afgebakend te werk gaan. Het is wellicht wenselijk dat er een duidelijke afbakening aan domeinen en specifieke bedreigingen of dreigingsactoren komt, om de analyse te stroomlijnen. Denk aan de NCTV die verantwoordelijk is voor het Dreigingsbeeld Terrorisme Nederland (DTN); het equivalent, het

Cybersecuritybeeld Nederland (CSBN), moet nog teveel met inschattingen vanuit andere ministeries concurreren, zo lijkt het. Bovendien is het CSBN heel/te breed. Ook zijn er 'veel meer slimme jonge mensen nodig', er zijn sowieso te weinig analisten om alle informatie, bijvoorbeeld over binnenkomende hacks, cybercrime, tijdig en adequaat te kunnen analyseren, aldus een respondent.

In de analyse moet ook rekening gehouden worden met de zich vormende AVG-wetgeving, privacyoverwegingen en toezicht en controle op de nieuwe opsporings- en onderzoeksmethodes. Cybersecurity is als domein onderhevig aan hypersecuritisering (heel veel wordt heel snel als risico gezien, en leidt tot extra inzet van vaak nog niet getoetste veiligheidsmaatregelen en interventies), alsmede aan technificering: steeds minder mensen weten precies wat er gebeurt, waardoor toezicht, accountability en daarmee legitimiteit afneemt – en de kans op afbreuk en onthullingen groot is (Cavelty & Egloff, 2021; De Groene Amsterdammer, 2021). Met de toekomstige meldplicht en mogelijk aanpassing van de AVG voor IP-adressen neemt de noodzaak meteen te investeren in toezicht op analyse en delen hiervan toe. Ook voor de politie.

Strategie- en besluitvorming:

Wie bepaalt wat vitale sectoren zijn die prioriteit krijgen? Welke onderzoeken moet de politie doen? Er is nu capaciteit bij het THTC voor zo'n 20 onderzoeken. In de toekomst zal dit nog nauwer met de andere spelers, in het bijzonder de NCSC moeten worden afgestemd. Met het oog op de nieuwe dreigingen is strategische denkkracht nodig, binnen de politie in den brede. Dat betekent dat er bij de politie, 'vanouds een MBO-organisatie', aldus een respondent, 'een veel hoger niveau van kennis en analyse nodig is bij de strategievormende units'.

Veelvuldig is gewezen op de afhankelijkheid van Nederlandse instellingen en organisaties van buitenlandse producten en diensten (denk aan Citrix, Chinese aanleg van 5G). Kan de strategische continuïteit van maatschappelijke kernprocessen niet beter gegarandeerd worden, ook bij de politie, als er strategisch geïnvesteerd wordt in betere alternatieven, ofwel in eigen land, of minder verspreid over risicovolle landen? Binnen de EU wordt over meer digitale autonomie gesproken, dat zou ook binnen en vanuit de LE beter belegd kunnen worden, om te beginnen in strategie- en besluitvorming (nieuwe investeringen, onderzoek naar alternatieven, samenwerking met andere EU-landen op dit terrein).

Operationele capaciteit:

De WRR stelde in 2019 dat de cybermaatregelen vooral gericht zijn op preventie, maar dat er weinig operationele capaciteiten lijken te zijn voor de fase van ontwrichting. Wat moet de overheid doen als servers worden gehackt of als systemen worden aangevallen door ransomware en in handen komen van buitenlandse dan wel private partijen? Wat doet de NCSC, en wat doen OM en politie? Wie bepaalt welke onderzoeken het meest effectief kunnen worden opgezet? Welke analisten gaan de data van in beslag genomen computersystemen

uitlezen en interpreteren? Wie vormt de liaison met partners in het buitenland? Binnen de politie is de operationele slagkracht ook versnipperd, in regionale eenheden, het THTC etc. De vraag is of die slagkracht verbeterd kan worden door de operationele coördinatie bij de LE samen te brengen, om prioritering en effectief opereren te kunnen waarborgen, of dit toch samen met het NCSC af te stemmen. Sturing op risico vergt meer investering in menskracht en analysekracht, juist om operationeel bij te kunnen blijven.

Coördinatie:

Cyberveiligheid is nog meer dan de strijd tegen terrorisme een aangelegenheid van horizontale samenwerking. Er is een NCSC, maar ook Defensie, politie, AIVD/MIVD, en Buitenlandse Zaken hebben hun eigen cyberunits. Er is overleg gaande om binnen het NCSC een soort 'groot oog' te creëren: door binnen het NCSC de informatiestromen samen te brengen en zo het delen van informatie en coördineren van samenwerking nog sneller te laten lopen. Cyberveiligheid is gebaat bij snel opereren. Daarom is wellicht een joint cyber command nodig, zoals ook in andere landen is ingericht. Een respondent vond dat het NCSC bij AZ ondergebracht zou kunnen worden. Dan kan de politie ook sneller met juiste informatie (ook vanuit het buitenland) gevoed worden. Het is nog maar de vraag of dat echt tot snellere informatiedeling met de politie zal delen. Er zijn wellicht betere oplossingen denkbaar (bijvoorbeeld een joint cyber command). Bij cyber ligt de oplossing nooit lokaal, maar altijd buiten het eigen veiligheidsdomein (bij programmeurs in de VS of China bijvoorbeeld).

Nog meer dan bij andere dreigingen zijn cybercrime en cybersabotage/spionage een type dreiging dat wordt uitgevoerd door teams van zeer kundige criminele experts. Het risico is ongekend hoog. Leiderschap vergt dan ook coördinatie op risico, en niet op basis van reeds gepleegde aanvallen. Er is in Nederland veel kennis belegd, maar bij uiteenlopende organisaties. De LE zou een coördinerende rol kunnen spelen bij het inrichten van meer teams van hoogopgeleide specialisten, experts voor preventie, detectie, maar ook bij ontwrichting. Het trainingsprogramma van het NCSC zou in samenwerking met LE kunnen worden uitgebreid.

Coördinatie op cybersecurity vergt ook besluitvaardigheid om het domein af te bakenen. Is er meer sturing en coördinatie nodig om de samenwerking met private organisaties en bedrijven vorm te geven, lekken te dichten bij ontwrichting en te helpen bij het overschakelen, zoeken en investeren naar alternatieven en het creëren van digitale autonomie, en meer onafhankelijkheid van bestaande digitale diensten die in de VS of in China zijn belegd?

[6] Of moet de LE dat juist niet allemaal doen, en moeten er ook coördinerende taken bij de regionale eenheden worden belegd? Volgens een respondent is het ook zaak om draagvlak te houden onder alle eenheden van de politie, en 'niet alle leuke, grote onderzoeken en besluiten aan de LE over te laten'.

Communicatie:

Het is al genoemd, maar deze dreiging leidt onder een tekort aan drama en publieke aandacht, mede veroorzaakt door de genoemde cyberschaamte. Maar ook omdat cybercrime vaak 'heel saai' is (Collier et al., 2020). Nederland doet niet graag aan 'cyber attributie' (Egloff, 2020; Goel & Nussbaum, 2021). Het CSBN is minder bekend dan het DTN, wellicht ook omdat cybersecuritybeeld heel veel zaken bevat. Te denken valt aan sectorale communicatie, of communicatie langs verschillende lijnen: digitale fraude in de burgermaatschappij, phishing, ransomware jegens bedrijven, publieke instellingen, en gerichte waarschuwingen tegen dual use dan wel te grote afhankelijkheid van ICT systemen. Communicatie zou met advisering verbonden kunnen worden, om de weerbaarheid tegen de cyberdreiging te verhogen. De politie is regionaal heel actief in voorlichting en informatievoorziening, bijvoorbeeld naar scholen toe. Voor eensluidende communicatie naar verschillende sectoren is evenwel meer coördinatie nodig.

[6] Zoals het CSBN 2021 stelt: 'De meest kansrijke oplossing ligt dan ook in het structureel laten stijgen van de kosten voor de criminelen ten opzichte van de baten van ransomware. Dit kan alleen als politie, het NCSC en OM samen met publieke en private partners en (potentiële) slachtoffers een vuist maken door proactief samen te werken en daarbij gericht informatie en inzichten te delen' (NCTV, 2021a, 31).

VI. Algemene analyse

Wanneer we de vier dreigingen in samenhang bekijken, en daarbij de trends in ogenschouw nemen, is het duidelijk dat de Landelijke Eenheid voor een bijzondere uitdaging staat in de aankomende jaren. Stuk voor stuk vormen de dreigingen een direct gevaar voor het collectief welzijn en de maatschappelijke weerbaarheid van onze samenleving. De Landelijke Eenheid dient als een bastion te functioneren in de strijd tegen deze dreigingen. Het is echt alle hens aan dek.

De Landelijke Eenheid wordt met dreigingen geconfontreerd die grensoverschrijdend van aard zijn, en veelal 'datagedreven'. Dit betekent dat de dreigingen zich niet netjes aan geografische grenzen of bureaucratische scheidslijnen houden. Deze dreigingen strekken zich uit over sectoren, langs bestuurlijke grenzen, en tot verre oorden. De bureaucratische afbakening van de Landelijke Eenheid als onderdeel van de Nationale Politie beperkt de LE in reikwijdte en slagkracht – en verkeert daarom altijd in een nadelige positie ten opzichte van een dreiging die zich van grenzen niets aantrekt en meesurft op de allerlaatste ontwikkelingen in de (digitale) wereld.

Het bestrijden van grensoverschrijdende problemen is een nachtmerrie voor het openbaar bestuur dat haar kracht juist ontleent aan het vaststellen van, en het bewegen binnen, bureaucratische grenzen. Het is altijd moeilijk om de juiste informatie te vergaren en te interpreteren; samenwerking met anderen is noodzakelijk maar kan nooit echt worden afgedwongen. De kans op falen in moeilijke dossiers voedt de politiek-bestuurlijke reflex om geen expliciete verantwoordelijkheid te nemen.

Het is, met andere woorden, een hele uitdaging om de dreigingen die wij hier beschrijven het hoofd te bieden. Het is ook het beeld dat respondenten bij ons doen neerdalen. We zijn niet succesvol, we winnen de strijd niet en de dreigingen worden alleen maar groter en moeilijker.

Drie bevindingen springen in het oog:

Ten eerste is geen sprake meer van een 'koude fase', een fase van rust waarin een dreiging rustig in kaart kan worden gebracht en op effectieve interventies kan worden gebroed. De dreigingen zijn voortdurend aanwezig, in beweging, en tasten ons land aan. Preventie lijkt nauwelijks nog een serieuze optie. Nodig is een proactieve en prospectieve manier van werken.

Ten tweede lijkt het steeds moeilijker om zicht te houden op deze dreigingen. Het is ongelooflijk moeilijk om de juiste informatie te vergaren en vervolgens te interpreteren, alleen al omdat die informatie uit zoveel domeinen afkomstig is. De politie moet zich natuurlijk ook aan allerlei beperkende condities houden, die zijn geformuleerd om de politie tegen zichzelf te beschermen (en de burger tegen de politie). Bovendien ontbreekt het aan menskracht en structurele financiering (in tegenstelling tot de doelgebonden financiering waar de LE vaak mee werkt).

Ten derde is de vraag of de traditionele, bureaucratische organisatievorm zich nog wel goed verhoudt tot de aard van uitdagingen waarvoor de LE zich in de toekomst gesteld zal zien. In zo'n vorm zijn de verantwoordelijkheden keurig

afgebakend, zowel verticaal als horizontaal. Maar het creëert een enorme behoefte aan coördinatie. Dit maakt een organisatie traag en reactief.

Wat is nodig om de hier beschreven dreigingen effectief tegemoet te treden? Op basis van de deelanalyses (per dreiging) komen we tot de volgende gewenste capaciteiten:

Analytische capaciteit: de juiste informatie verzamelen, analyseren, en die analyses vertalen in begrijpelijke inzichten die zich lenen voor concrete interventies. Elke dreiging die wij hebben onderzocht vereist in eerste instantie het vermogen om de aard, dynamiek en (mogelijke) gevolgen van die dreiging in kaart te brengen. Dit is een ongelooflijk moeilijke opgave, die allerlei vormen van theoretische en praktische kennis alsook methoden van analyse vereist. De dreigingen zijn veelal datagedreven. De bestrijding ervan moet dus ook een beroep doen op nieuwe vormen van analyse ('big data') en slimme technologieën, en die tegelijkertijd verbinden aan klassieke methoden (kennis van de straat). Deze dreigingen vereisen een 'slimme' organisatie, zoals een van onze respondenten het uitdrukte. Klassieke vaardigheden blijven belangrijk, maar een constante 'update' van die vaardigheden is cruciaal. Dit vraagt om een transitie naar een organisatie waar ruimte en waardering is voor denkkracht.

Vooruit kijken: trends en game changers. Het gaat niet alleen om het begrijpen van oorzaken en het in kaart brengen van de stand van zaken. Wat ook nodig is een idee van de richting waarheen en het tempo waarop een dreiging zich ontwikkelt. Traditionele concepties van lineariteit moeten worden gecomplementeerd door een begrip van exponentiële groei, tipping points, *creeping crises* en incubatie, kansberekening en *worst case scenario's*. Dit is een nieuwe manier van kijken. Het 'vooruit denken' vereist structurele inbedding in de verzameling en analyse van informatie. Financiering van deze capaciteitsuitbreiding is dan gewenst; wellicht op het niveau van de LE, wellicht ook verdeeld over regionale eenheden.

Een interdisciplinaire 'mindset': Een verscheidenheid aan bronnen van kennis vereist een brede variëteit aan analytische perspectieven. Onze analyse van de vier dreigingen laat geen twijfel bestaan dat traditionele perspectieven op opsporing verrijkt moeten worden met technologisch, juridische, financiële, historische, politicologische, bestuurskundige, sociologische, culturele, psychologische en antropologische perspectieven. En dan zien we ongetwijfeld nog een aantal perspectieven over het hoofd. Het is onmogelijk en onwenselijk om een politieorganisatie om te toveren in een universiteit. Wel kan de politie een veel sterkere band met de wereld van onderzoek ontwikkelen.

Het begint met een vanzelfsprekend respect met betrekking tot het idee van interdisciplinariteit. Dat betekent dat de cultuur van erkenning en waardering niet alleen aan grote aanhoudingen of opsporingssuccessen wordt gekoppeld, maar dat ook waardering wordt uitgesproken voor processen van interdisciplinaire uitwisseling, 'informatieveredeling' en data-analyses.

Vertrouwd met social media: Sociale platforms genereren een schier oneindige bron van kennis en informatie die kan worden benut voor lange-termijn onderzoek en *real-team intelligence*. Sociale platforms bieden allerlei innovatieve vormen van communicatie waar vrijwel iedereen gebruik van maakt. Ze vormen het voornaamste domein van disinformatie, complottheorieën en wilde geruchten. Social media vormen een virtuele wereld die steeds meer vermengd is geraakt met de echte wereld. Dit vergt een organisatie die deze wereld tot in de haarvaten begrijpt (zoals vroeger de wijk op een voetstuk werd geplaatst).

Over grenzen heen werken: De dreigingen die wij onderzochten zijn zonder uitzondering grensoverschrijdend van aard. We doelen niet alleen op een internationale dimensie (die in elk van de vier dreigingen is te ontwaren), maar ook op een intersectorale dimensie (meerdere sectoren zijn betrokken) en een *multi-level* dimensie (van lokaal tot internationaal). Dit levert een driedimensionaal werkveld op waarin moet worden genavigeerd om informatie en kennis te verzamelen; het is een wereld met een smörgåsbord van verantwoordelijkheden die moet worden doorsneden om iets gedaan te krijgen. Dit vereist een organisatie die banden onderhoudt met lokale ondernemers en internationaal-opererende onderzoekers, met banken en spionnen, met de lokale carnavalsvereniging en internationale organisaties.

In de haarvaten van de samenleving: Het is de traditionele slogan van de politie: wij weten wat speelt door onze aanwezigheid op straat. Al het gepraat over nieuwe domeinen die ver en wijd strekken mag niet afleiden van het belang deze kernvaardigheid te onderhouden en te versterken. Het blijft een conditie voor effectiviteit en legitimiteit.

Borgen van ervaring en kennis: Een organisatie die zo breed opereert verzamelt een rijkdom aan kennis en ervaring. Die rijkdom zit maar al te vaak in de hoofden van de medewerkers. In een traditionele organisatie wordt die kennis en ervaring bij het koffieapparaat gedeeld; collega's weten in wiens hoofd ze moeten kijken voor deze of gene inzichten. In de moderne organisatie is het van belang dat kennis en ervaring op meer doelmatige wijze worden ontsloten. Makkelijker gezegd dan gedaan, dus dit vereist een fundamentele bezinning op de kennis en ervaring die als onmisbaar moet worden gekwalificeerd – voor zowel de korte als de lange termijn.

Nieuwe vormen van interventie: Wat te doen met cyberdreigingen? Hoe te sturen op nieuwe risico's? Hoe om te gaan met 'coronaprotesten'? Nieuwe interventies moeten worden bedacht en ontdekt. Experimenten moeten hand in hand gaan met een respect voor traditionele beperkingen die voortvloeien uit het recht, sociale conventies, internationale verdragen en politieke oekazes. Dat vraagt om een combinatie van kennis, creativiteit en integriteit.

Netwerk navigatie: De politie functioneert in meerdere netwerken. Dat is geen nieuws. Maar de netwerken worden complexer, veelzijdiger en dynamischer. Een plek in een netwerk moet worden verdiend. Samenwerkingen brengen ook risico's

met zich mee. Kennis van partners – hun preferenties, beperkingen en werkwijzen – moet paraat zijn.

Aanknopingspunten voor leiderschap van de nabije toekomst

Sturen op missie: Traditionele vormen van top-down leiderschap, zo eigen aan de bureaucratische organisatievorm, hebben geen toekomst. Professionals hebben ruimte nodig, maar ook een idee van richting. Een missie-gedreven organisatie biedt de beste kansen. Dat vereist leiders die een doel duidelijk neer kunnen zetten, een effectieve beleidstheorie kunnen helpen ontwikkelen door experimenten te faciliteren en te sanctioneren, en korte-termijn winst kunnen afzetten tegen lange-termijn risico's voor de legitimiteit van de organisatie. Dit betekent niet dat de traditionele politieleider heeft afgedaan. Integendeel. De Nederlandse politie heeft indrukwekkende leiders voortgebracht die aan deze kenmerken voldoen. De kunst is om deze leiders te herkennen en op de juiste plek te krijgen, en te omringen met teamleden die het geheel aan vereiste competenties compleet maken. Geen enkele leider kan over alle benodigde competenties beschikken, leiderschap is een functie van *the density of competences* op het strategische niveau.

Adaptief vermogen: Het traditionele idee van de leider die door principes wordt gedreven, de sterke persoonlijkheid, verhoudt zich slecht met de behoefte aan adaptiviteit. Complexe dreigingen vragen om experimenten. Dat betekent maar al te vaak een aanpassing van de koers, gebaseerd op feedback. Daar hoort twijfel bij, een omarming van ambiguïteit, respect voor tegenspraak. Het organiseren van Red Teaming, niet voor de symboliek maar om blinde vlekken op te sporen en nieuwe oplossingen op tafel te krijgen. Adaptief vermogen vereist wel degelijk een sterke persoonlijkheid, want het is niet eenvoudig terug te komen op uitgedragen commitment.

Absolute toewijding aan het belang van integriteit: Nieuwe vormen van leiderschap kunnen gewenst zijn, maar het traditionele integriteitsprincipe is de poolster van politieleiderschap. De dilemma's die hieruit voortvloeien zijn bekend. Leiderschap kan eenzaam zijn. Maar integriteit binnen de politie is niet onderhandelbaar.

Vertelkunst: Sturen op visie vereist het vermogen om te overtuigen. Binnen de organisatie, maar ook daarbuiten. Niets overtuigt beter dan een goed verhaal. En een goed verhaal moet worden verteld. Met overtuiging en met gevoel voor de leefwereld van het beoogde publiek. Een verhaal dat kan verbinden, een verhaal dat de *agency myth* van de LE als instituut inzichtelijk maakt.

Bewaken van autonomie: Het is makkelijk om als organisatie de weg kwijt te raken in een netwerk dat innige samenwerking vereist. Maar de identiteit van de organisatie moet worden bewaakt, ten opzichte van netwerk-partners maar ook ten opzichte van het hoofdbureau, het departement, de politiek, en de media. Dat is niet louter een kwestie van op de strepen staan. Het vereist een constante uitleg waarom autonomie nodig is: professionals kunnen niet werken in een klimaat van micromanagement. Autonomie gedijt onder een strategisch vaardige leider die het

spel kent, maar het werkt nog beter als anderen die autonomie respecteren en faciliteren.

Met het oog op communicatie over onderzoek, dreiging, uitdagingen zou met de NCTV en de driehoek moeten worden overlegd of de politie hier niet meer de eigen vrije hand kan krijgen, juist om sneller te kunnen reageren in een omgeving van dynamische en fluïde patronen van dreiging.

Fouten toegeven maar staan voor je mensen: Tot slot vergt leiderschap ook voldoende openheid in de eigen organisatie om fouten toe te geven, achter de mensen staan die fouten maken, coverup logica te doorbreken, en hierover ook naar de buitenwereld verantwoording over af te leggen. Met het oog op de enorme werkdruk, de grote dreigingen en het gebrek aan menskracht, is een cultuur nodig van saamhorigheid en collectiviteit, zoals alle respondenten aangeven. Dat betekent dat de politie een boegbeeld heeft, dat er stevig leiderschap is dat voor de eigen mensen gaat staan, dat successen op de hele organisatie laat afstralen (en niet op dat ene sectorhoofd dat in de media kwam), en fouten opvangt. Dat betekent ook dat er erkenning moet komen voor het feit dat de LE een andere soort organisatie is dan de regionale eenheden; de LE heeft geen driehoek waarmee ze structureel optrekt en door wordt gesteund. Om niet overweldigd te raken door de enorme stroom informatie, om niet af te stompen door een cultuur van elkaar vliegen afvangen, is een leiderschap nodig die erkenning en waardering aan professionals geeft, en niet alleen aanhoudingen, concrete resultaten in de opsporing 'beloont', maar ook denkkracht en inventiviteit aanmoedigt.

VII. Interviews/achtergrondgesprekken

Otto Adang, Politie Academie

Robin van Dalen, LE

Michel Kok, Stad Utrecht

Peter Noordanus, LSOAO

Erik van Palland, LE

Theo van der Plas, LE

Jeroen Poelert, LE

Edward van der Torre, LokaleZaken

Hans de Vries, NCSC

VIII. Literatuur

'150 drugs-arrestaties bij internationaal onderzoek darknet' (Oktober 2021). *NOS Nieuws*. https://nos.nl/artikel/2403212-150-drugs-arrestaties-bij-internationaal-onderzoek-darknet.

Aarten, P. G., & Liem, M. C. (2021). 'Unravelling the Homicide Drop: Disaggregating a 25-Year Homicide Trend in the Netherlands'. *European Journal on Criminal Policy and Research*, 1-26. https://doi.org/10.1007/s10610-021-09489-0.

Achilli, L. & Sanchez, G. (2021). 'Introduction – migration, smuggling and the illicit global economy'. *Public Anthropologist,* 3:1, 1-7. European University Institute, Brill. https://doi.org/10.1163/25891715-03010001.

Adam-Troian, J., Çelebi, E., & Mahfud, Y. (2020a). '"Return of the repressed": Exposure to police violence increases protest and self-sacrifice intentions for the Yellow Vests'. *Group Processes & Intergroup Relations*, 23:8, 1171-1186. https://doi.org/10.1177/1368430220920707.

'Advies aan de (in)formateur (17): Jan-Jaap Oerlemans - Geheimhouding of openheid?' (September 2021). *De Groene Amsterdammer.* https://www.groene.nl/artikel/geheimhouding-of-openheid.

Alberda, D., Duits, N. & Kempes, M. (2020). *Doorwerking psychopathologie in terroristische misdrijven*. Den Haag: Ministerie van Justitie en Veiligheid. https://www.nifp.nl/documenten/rapporten/2021/11/30/doorwerking-psychopathologie-in-terroristische-misdrijven.

Alberda, D., Duits, N., Bos, K. van den, Ayanian, A. H. Zick, A. & Kempes, M. (2021). 'The European Database of Terrorist Offenders (EDT): Development, Usability and Options'. *Perspectives on Terrorism,* 15:2, 77-99. https://www.jstor.org/stable/27007297.

Alves, R., Precioso, J., & Becoña, E. (2021). 'Illicit Drug Use among College Students: The Importance of Knowledge about Drugs, Live at Home and Peer Influence'. *Journal of psychoactive drugs*, 53:4, 1-10. https://doi.org/10.1080/02791072.2020.1865592.

Bakker, J., Cornelisse, D., Mohamed, S., Schäfer, M. T., & Veerbeek, J. (2021). *Van scherm naar straat: Hoe sociale media-conversaties protest op straat mobiliseren.* Utrecht: Utrechtse Data School. https://dataschool.nl/wp-content/uploads/sites/272/2021/03/20210318_Van-scherm-naar-straat.pdf.

Barker, K., Baker, M., & Watkins, A. (2021). 'In City After City, Police Mishandled Black Lives Matter Protests'. *The New York Times*, 1-9. https://www.kooriweb.org/foley/news/2000s/2021/march/nyt20mar2021.pdf.

Bartusevicius, H., Bor, A., Jørgensen, F. J., & Petersen, M. B. (2021). 'The psychological burden of the COVID-19 pandemic drives anti-systemic attitudes and political violence'. *Psychological Science,* 32:9, 1391-1403. https://doi.org/10.1177/09567976211031847.

Baumeister, D., Tojo, L. M., & Tracy, D. K. (2015). 'Legal highs: staying on top of the flood of novel psychoactive substances'. *Therapeutic advances in psychopharmacology,* 5:2, 97-132. https://doi.org/10.1177/2045125314559539.

Bennett, W. L., & Livingston, S. (2018). 'The disinformation order: Disruptive communication and the decline of democratic institutions'. *European journal of communication,* 33:2, 122-139. https://doi.org/10.1177/0267323118760317.

Bijlenga, N., & Kleemans, E. R. (2018). 'Criminals seeking ICT-expertise: an exploratory study of Dutch cases'. *European Journal on Criminal Policy and Research,* 24:3, 253-268. https://doi.org/10.1007/s10610-017-9356-z.

Blanco, J.M & Cohen, J. (2017). 'Macro-environmental Factors Driving Organised Crime'. In Larsen, H. L., Blanco, J. M., Pastor R. P., & Yager R. R. (Eds.), *Using Open Data to Detect Organized Crime Threats: Factors Driving Future Crime*, Cham: Springer International Publishing, 137-166.

Blokland, A., Leest, W. van der, & Soudijn, M. (2020). 'Officially registered criminal careers of members of Dutch outlaw motorcycle gangs and their support clubs'. *Deviant Behavior,* 41:11, 1393-1412. https://doi.org/10.1080/01639625.2019.1619422.

Boin, A., Ekengren, M. & Rhinard, M. (2021). 'Hiding in plain sight: Conceptualizing the creeping crisis'. *Risk, Hazards & Crisis in Public Policy*, 11:2, 116-138. https://doi.org/10.1002/rhc3.12193.

Boin, A., Ekengren, M. & Rhinard, M. (Red) (2021). *Understanding the creeping crisis*. London: Palgrave Macmillan.

Boin, A., Linck, R., Duin, M. van, Hendriks, J., Berger, E. & Varst, L. van der (2020). *Versterken van Veerkracht: Naar een gezamenlijke aanpak van ongekende crises*. Arnhem: IFV.

Bojar, A., Gessler, T., Hutter, S., & Kriesi, H. (Eds.) (2021). *Contentious Episodes in the Age of Austerity.* Cambridge: Cambridge University Press.

Bos, Kees van den (2019). *Waarom mensen radicaliseren: hoe waargenomen onrechtvaardigheid radicalisering, extremisme en terrorisme aanwakkert.* Amsterdam: Prometheus.

Boutellier, H., Van Steden, R., Eski, Y. & Boelens, M. (2020). 'Een einde aan ondermijning: Over de opkomst en werking van een nieuwe veiligheidsstrategie'. *Tijdschrift voor Veiligheid*, 19:1, 3-15. https://doi.org/10.5553/TvV/187279482020019001001.

Brezzi, M., González, S., & Prats, M. (2020). 'All you need is trust: Informing the role of government in the Covid-19 context'. *Directorate for Public Governance, OECD.* https://data.oecd.org/gga/trust-in-government.htm.

Brosius, A., Elsas, E. J. van, & Vreese, C. H. de (2018). 'Trust in the European Union: Effects of the information environment'. *European Journal of Communication,* 34:1, 57-73. https://doi.org/10.1177/0267323118810843.

Bruinsma, M.Y., Ceulen, R., & Spapens, A. (2018). *Ondermijning door criminele 'weldoeners': Inventariserend onderzoek*. Den Haag: SDU.

Bullough, O. (2019). *Moneyland*. London: Profile Books.

Bundeskriminalamt [BKA] (Federal Criminal Police Office). (n.d.). Politisch motivierte Kriminalität. https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/PMK/pmk_node.html;jsessionid=50C2089B646C9729D05BB9B731F598A3.live612.

Burgers, J. (Augustus 2021). 'Epidemie van extreem geweld onder jongeren'. *Leidsch Dagblad*, 4.

Buscaglia, E. & Dijk, J. van (2003). 'Controlling organized crime and corruption in the public sector'. *Forum on crime and society,* United Nations Office on Drugs and Crime, 3. https://www.unodc.org/pdf/crime/forum/forum3_Art1.pdf.

Busemeyer, M. R., Diehl, C., Wöhler, T., Wolter, F., Bertogg, A., Strauß, S., & Kulic, N. (2021). 'Vertrauen. Impfzugang. Radikalisierung. Unzufriedenheit.: Wo die Coronakrise die Gesellschaft ungleicher macht'. *Leibniz-Informationzentrum Wirtschaft,* 7, 1-17. https://nbn-resolving.de/urn:nbn:de:bsz:352-2-8gjg8e9k03974.

Calvet, C. C., & Di Nella, D. (2020). 'Contrahegemonías antirrepresivas. Un estudio de caso de la protesta en Barcelona (2011-2015)'. *Politica y Sociedad*, 57:1, 146. https://doi.org/10.5209/poso.60271.

Cavelty, M. D. & Egloff, F. (2021). 'Hyper-Securitization, Everyday Security Practice and Technification: Cyber-Security Logics in Switzerland'. *Swiss Political Science Review,* 27:1, 139-149. https://doi.org/10.1111/spsr.12433.

Centraal Bureau voor de Statistiek (mei 2018). 'Het mysterie van de verdwenen criminaliteit'. https://www.cbs.nl/nl-nl/longread/statistische-trends/2018/het-mysterie-van-de-verdwenen-criminaliteit/1-ontwikkelingen-in-de-criminaliteit.

Chase, R.J. & La Porte, G. (2017). 'The Next Generation of Crime Tools and Challenges: 3D Printing'. *National Institute of Justice.* https://nij.ojp.gov/topics/articles/next-generation-crime-tools-and-challenges-3d-printing.

Collier, B., Clayton, R., Hutchings, A. & Thomas, D. R. (2020). 'Cybercrime is (often) boring: maintaining the infrastructure of cybercrime economies'. *Workshop on the Economics of Information Security*. Cambridge: University of Cambridge. https://doi.org/10.17863/CAM.53769.

'Cyber Security Beeld Nederland: toegenomen dreiging Ransomware' (Juni 2021). *Politie.nl.* https://www.politie.nl/nieuws/2021/juni/28/00-cyber-security-beeld-nederland-toegenomen-dreiging-ransomware.html.

Davies, Garth., Wu, E. & Frank, R. (2021). 'A Witch's Brew of Grievances: The Potential Effects of COVID-19 on Radicalization to Violent Extremism'. *Studies in Conflict & Terrorism*. https://doi.org/10.1080/1057610X.2021.1923188.

Deuren, S. van, Blokland, A., & Kleemans, E. (2021). 'Examining membership of Dutch Outlaw Motorcycle Gangs and its association with individual criminal careers'. *Deviant Behavior*, 1-16. https://doi.org/10.1080/01639625.2021.1919498.

Di Cataldo, M., & Mastrorocco, N. (2020). 'Organised crime, captured politicians, and the allocation of public resources'. *University Ca'Foscari of Venice, Dept. of Economics*, Research Paper Series, 4, 1-85. https://doi.org/10.2139/ssrn.3599850.

Dickinson, T., & Jacques, S. (2021). 'Drug Control Policy, Normalization, and Symbolic Boundaries in Amsterdam's Coffee Shops'. *The British Journal of Criminology,* 61:1, 22-40. https://doi.org/10.1093/bjc/azaa059.

Dikeç, M. (2018). *Urban rage: The revolt of the excluded*. New Haven and London: Yale University Press.

'Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union' (NIS Directive) (2016). *Journal of the European Union,* L 194:1, 1-30. https://data.europa.eu/eli/dir/2016/1148/oj.

Döring, M. (2020). 'Vorsicht, Ansteckungsgefahr: Stigmatisierung, Vorurteil und Diskriminierung; Der Einfluss der Corona-Krise auf extremistische Radikalisierungsprozesse in Deutschland'. *Netzwerk für Extremismusforschung in Nordrhein-Westfalen*, Bonn: Bonn International Center for Conversion (BICC), 1-8. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-71645-8.

Doumani, T., & Dakwar, J. (2020). 'Rubber Bullets and the Black Lives Matter Protests'. *Human Rights Brief,* 24:2*,* 77-83. https://heinonline.org/HOL/Page?handle=hein.journals/huribri24&id=92&collection=journals&index=.

Egloff, F. (2020). 'Public attribution of cyber intrusions'. *Journal of Cybersecurity,* 6:1, 1-12. https://doi.org/10.1093/cybsec/tyaa012.

Engbersen, G., Bochove, M. van, Boom, J. de, Bussemaker, J., Farisi, B. el, Krouwel, A., Lindert, J. van, Rusinovic, K., Snel, E., Heck, L. van, Veen, H. van der & Wensveen, P. van. (2021). *De Laag-vertrouwen Samenleving*. Rotterdam: Erasmus School of Social and Behavioural Sciences & Kenniswerkplaats Leefbare Wijken.

European Commission. (2016). *Joint Communication To The European Parliament And The Council: Joint Framework on countering hybrid threats, a European Union response.* EUR-Lex - 52016JC0018 – EN. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018.

European Monitoring Center for Drugs and Drug Addiction. (2019). *Netherlands Country Drug Report 2019*. https://www.emcdda.europa.eu/publications/country-drug-reports/2019/netherlands_en.

European Monitoring Center for Drugs and Drug Addiction. (2020). *European Drug Report: Trends and Developments – 2020*. https://op.europa.eu/s/vkXr.

European Union Agency for Fundamental Rights. (2020). *What do Fundamental Rights Mean for People in the EU?* https://op.europa.eu/s/vkXs.

Ferwerda, H., Beke, B. & Bervoets, E. (2017). 'De onzichtbare invloed van bovenlokale criminele netwerken op de wijk'. *Tijdschrift voor de politie*, 79:9/10, 6-11. https://bureaubeke.nl/publicaties/de-onzichtbare-invloed-van-bovenlokale-criminele-netwerken-op-de-wijk/.

Fourie, M., Steenkamp, P., McIntyre-Louw, J. L., & Oellermann, C. (2021). 'Exploring infiltration behaviour by organised crime groups'. *Journal of Money Laundering Control*. https://doi.org/10.1108/JMLC-10-2021-0117.

Fussell, S. (September 2021). 'It's Not Easy to Control Police Use of Tech—Even With a Law'. *Wired*. https://www.wired.com/story/hard-control-police-tech-law/

Gaffney, A. W., McCormick, D., Woolhandler, S., & Himmelstein, D. U. (2020). 'US law enforcement crowd control tactics at anti-racism protests: a public health threat'. *The Lancet,* 396:10243, 21. https://doi.org/10.1016/S0140-6736(20)31421-5.

Ganau, R., & Rodríguez-Pose, A. (2018). 'Industrial clusters, organized crime, and productivity growth in Italian SMEs'. *Journal of Regional Science,* 58:2, 363-385. https://doi.org/10.1111/jors.12354.

Gelles, M. Mirkow, A. & Mariani, J. (2019). 'The future of law enforcement: Policing strategies to meet the challenges of evolving technology and a changing world'. *Deloitte Insights.* https://www2.deloitte.com/us/en/insights/focus/defense-national-security/future-of-law-enforcement-ecosystem-of-policing.html.

Giugni, M., & Grasso, M. T. (2019). *Street Citizens: Protest Politics and Social Movement Activism in the Age of Globalization.* Cambridge: Cambridge University Press.

Goel, S. & Nussbaum, B. (Mei 2021). 'Attribution Across Cyber Attack Types: Network Intrusions and Information Operations'. *IEEE Open Journal of the Communications Society,* 2, 1082-1093. https://doi.org/10.1109/OJCOMS.2021.3074591.

Goosdeel, A. & Wainwright, R. (2017). 'Drugs and the darknet: Perspectives for enforcement, research and policy'. [Joint Report] *European Monitoring Centre for Drugs and Drug Addiction & Europol*. https://www.europol.europa.eu/publications-documents/drugs-and-darknet-perspectives-for-enforcement-research-and-policy.

Graaf, Beatrice de (2021a). *Radicale verlossing: Wat terroristen geloven.* Amsterdam: Prometheus.

Graaf, Beatrice de (2021b). 'Eschatologisch ongeduld of martelaarscomplex: Radicalisering op de christelijke flanken?'. *Dutch Biblebelt Network*. Amsterdam: Labarum Academic.

Haciyakupoglu, G., Hui, J. Y., Suguna, V. S., Leong, D., & Rahman, M. F. B. A. (2018). 'Countering fake news: A survey of recent global initiatives'. *Think-Asia.* http://hdl.handle.net/11540/8063.

Heinze, R. G., Bieckmann, R., Kurtenbach, S., & Küchler, A. (2021). 'Bauernproteste in Deutschland: Aktuelle Einblicke und politische Verortung'. *Forschungsjournal Soziale Bewegungen*, 34:3, 360-379. https://doi.org/10.1515/fjsb-2021-0035.

Heisler, M., Mishori, R., & Haar, R. (2020). 'Protests against police violence met by more police violence—A dangerous paradox'. *JAMA Health Forum, American Medical Association,* 1:6, e200739-e200739. https://doi.org/10.1001/jamahealthforum.2020.0739.

Helberger, N. (2020). 'The political power of platforms: How current attempts to regulate misinformation amplify opinion power'. *Digital Journalism,* 8:6, 842-854. https://doi.org/10.1080/21670811.2020.1773888.

Henschke, A., Sussex, M., & O'Connor, C. (2020). 'Countering foreign interference: election integrity lessons for liberal democracies'. *Journal of Cyber Policy,* 5:2, 180-198. https://doi.org/10.1080/23738871.2020.1797136.

Hoboken, J. van, & Ó Fathaigh, R. (2021). 'Regulating Disinformation in Europe: Implications for Speech and Privacy'. *UC Irvine Journal of International, Transnational and Comparative Law*, 6:9, 9-36. https://scholarship.law.uci.edu/ucijil/vol6/iss1/3.

Hornick, J. (n.d). '3D Printing New Kinds of Crime.' *International Association of Chiefs of Police*. https://www.policechiefmagazine.org/3d-printing-new-kinds-of-crime/?ref=05ceb1d39d8b832ee7ab768f8919f9d2.

'Jongen (17) krijgt allereerste 'online gebiedsverbod' in Nederland, maar wat betekent dat eigenlijk?' (November 2021). *Algemeen Dagblad.* https://www.ad.nl/utrecht/jongen-17-krijgt-allereerste-online-gebiedsverbod-in-nederland-maar-wat-betekent-dat-eigenlijk~a246c189/.

Karlsson, P., Ekendahl, M., Månsson, J., & Raninen, J. (2019). 'Has illicit drug use become normalised in groups of Swedish youth? A latent class analysis of school survey data from 2012 to 2015'. *Nordic Studies on Alcohol and Drugs,* 36:1, 21-35. https://doi.org/10.1177/1455072518814306.

Kessel, S. van, Sajuria, J., & Hauwaert, S. M. van (2021). 'Informed, uninformed or misinformed? A cross-national analysis of populist party supporters across European democracies'. *West European Politics*, 44:3, 585-610. https://doi.org/10.1080/01402382.2019.1700448.

Kilcullen, D. (2013). *Out of the mountains: The coming age of the urban guerrilla*. London: Hurst & Company.

Korte, L. R. de, & Kleemans, E. R. (2021). 'Contract killings: a crime script analysis'. *Trends in Organized Crime*, 1-14. https://doi.org/10.1007/s12117-021-09411-4.

Kraak, H. (Augustus 2021). 'Geweld door jongeren minder, wel harder'. *De Volkskrant*, 9.

Laak, T. ter (September 2021). 'Designer drugs dodge the law: Use of 3-MMC evident in sewage.' *KWR, Bridging Science to Practice*. https://www.kwrwater.nl/en/actueel/designer-drugs-dodge-the-law/

Larres, K. & Hof, T. (Red.)(2022). *Terrorism and Transatlantic Relations: Threats and Challenges.* London: Palgrave Macmillan.

Lefebvre, R. (2019). 'Les Gilets jaunes et les exigences de la représentation politique'. *La vie des idées*. https://laviedesidees.fr/Les-Gilets-jaunes-et-les-exigences-de-la-representation-politique.html.

Levi, M. (2021). 'Making sense of professional enablers' involvement in laundering organized crime proceeds and of their regulation'. *Trends in Organized Crime*, 24:1, 96-110. https://doi.org/10.1007/s12117-020-09401-y.

Levi, M., & Soudijn, M. (2020). 'Understanding the laundering of organized crime money'. *Crime and Justice*, 49:1, 579-631. https://doi.org/10.1086/708047.

Lieber, U. (Augustus 2020). 'Landwirte verärgert über Plakate der AfD'. *Westfälische Nachrichten*. https://www.wn.de/muensterland/kreis-warendorf/sassenberg/landwirte-verargert-uber-plakate-der-afd-821476.

Lim, S. S., & Bouffanais, R. (2019). 'Tuning Networks for Prosocial Behavior: From Senseless Swarms to Smart Mobs [Commentary]'. *IEEE Technology and Society Magazine,* 38:4, 17-19. https://doi.org/10.1109/MTS.2019.2948437.

Madarie, R., & Kruisbergen, E. W. (2020). 'Traffickers in Transit: Analysing the Logistics and Involvement Mechanisms of Organised Crime at Logistical Nodes in the Netherlands: Empirical Results of the Dutch Organised Crime Monitor'. In D.

Weisburd, E.U. Savona, B. Hasisi, F. Calderoni (Eds.), *Understanding Recruitment to Organized Crime and Terrorism*, Cham: Springer International Publishing, 277–308.

McKinsey & Company (2021). 'Study on the societal acceptance of Urban Air Mobility in Europe'. *European Union Aviation Safety Agency*. https://www.easa.europa.eu/sites/default/files/dfu/uam-full-report.pdf.

Mendonca, R. F., & Bustamante, M. (2020). 'Back to the Future: Changing Repertoire in Contemporary Protests'. *Bulletin of Latin American Research*, 39:5, 629-643. https://doi.org/10.1111/blar.13087.

Miller, M. K. (2021). 'A Republic, If You Can Keep It: Breakdown and Erosion in Modern Democracies'. *The Journal of Politics*, 83:1, 198-213. https://doi.org/10.1086/709146.

MIT Technology Review (2021). 'Accelerating development in aerospace for more urban mobility'. *Humans and Technology.* https://www.technologyreview.com/2021/11/16/1039433/accelerating-development-in-aerospace-for-more-urban-mobility/.

Nassauer, A. (2021). '"Whose streets? Our streets!": - Negotiations of Space and Violence in Protests'. *Social problems*, 68:4, 852-869. https://doi.org/10.1093/socpro/spaa051.

National Intelligence Council (2021). *Global Trends 2040: A More Contested World.* Office of the Director of the National Intelligence Council, NIC 2021-02339.

NCTV (2020). *Cybersecuritybeeld Nederland (CSBN).* Den Haag: Ministerie van Justitie en Veiligheid. https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2020/juni/29/csbn-2020/CSBN+2020.pdf.

NCTV (2021a). *CSBN.* Den Haag: Ministerie van Justitie en Veiligheid. https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2021/06/28/cybersecuritybeeld-nederland-2021/TK+Bijlage+CSBN2021.pdf.

NCTV (2021b). *Dreigingsbeeld Terrorisme Nederland 55.* Den Haag: Ministerie van Justitie en Veiligheid. https://www.nctv.nl/binaries/nctv/documenten/publicaties/2021/10/26/dreigingsbeeld-terrorisme-nederland-55/Dreigingsbeeld+Terrorisme+Nederland+55.pdf.

Noordanus, P.G.A. (2020). *Een pact voor de rechtsstaat: Een sterke terugdringing van drugscriminaliteit in tien jaar*. Den Haag: Aanjaagteam Ondermijning.

Omand, D. (2018). 'The threats from modern digital subversion and sedition'. *Journal of Cyber Policy,* 3:1, 5-23. https://doi.org/10.1080/23738871.2018.1448097.

Oosthoek, K. & Doerr, C. (2020). 'Cyber Threat Intelligence: A Product Without a Process?'. *International Journal of Intelligence and CounterIntelligence,* 34:2, 300-315. https://doi.org/10.1080/08850607.2020.1780062.

Patton, D. (2018). 'Navigating drugs at university: normalisation, differentiation and drift?'. *Safer Communities*, 17:4, 224-237. https://doi.org/10.1108/SC-01-2018-0002.

Paulissen, W. (2019). 'Nederland drugsland'. *Cahiers Politiestudies*, 3:52, 149-164.

Pearl, R. C., Torbati, S., & Geiderman, J. M. (2021). 'Kinetic Projectile Injuries Treated During Civil Protests in Los Angeles: A Case Series'. *Clinical Practice and Cases in Emergency Medicine*, 5:4, 385-389. https://doi.org/10.5811/cpcem.2021.7.52885.

Peeples, L. (Mei 2020). 'What the data say about police brutality and racial bias—and which reforms might work'. *Nature*, 583, 22-25. https://www.nature.com/articles/d41586-020-01846-z?utm_source=Nature+Briefing&utm_campaign=761bed091d-briefing-dy-20200622&utm_medium=email&utm_term=0_c9dfd39373-761bed091d-44992633.

Pennay, A. E., & Measham, F. C. (2016). 'The normalisation thesis–20 years later'. *Drugs: Education, Prevention and Policy*, 23:3, 187-189. https://doi.org/10.3109/09687637.2016.1173649.

Pew Research Center. (2021). *Public Trust in Government: 1958-2021.* https://www.pewresearch.org/politics/2021/05/17/public-trust-in-government-1958-2021/.

Poell, T., & van Dijck, J. (2017). 'Social media and new protest movements'. *In SAGE Handbook of Social Media*, London: Sage, 546-561.

Porta, D. D. (1995). *Social Movements, Political Violence, and the State: A Comparative Analysis of Italy and Germany.* Cambridge: Cambridge University Press.

Portos, M. (2021). 'Grievances and public protests: Political mobilisation in Spain in the age of austerity'. Cham: Palgrave Macmillan.

Prasad, E. (Juli 2021). 'Cash Will Soon Be Obsolete. Will America Be Ready?'. *The New York Times,* 8. https://www.nytimes.com/2021/07/22/opinion/cash-digital-currency-central-bank.html.

Prats, M. & Meunier, A. (2021). 'Political efficacy and participation: An empirical analysis in European countries'. *OECD Working Papers on Public Governance*, 46, 1-23. https://doi.org/10.1787/4548cad8-en.

Putnam, R. (2000). *Bowling alone*. New York: Simon & Schuster.

Rapoport, D. (2022). *Waves of Global Terrorism: From 1878 to the Present.* New York: Columbia University Press.

Rebrina, L. N., Shamne, N. L., Milovanova, M. V., & Malushko, E. Y. (2021). 'Smart Technologies in Protest Communication: Current Practices and Trends'. In *Institute of Scientific Communications Conference*, Cham: Springer International Publishing, 141-151.

Ricard, J., & Medeiros, J. (2020). 'Using misinformation as a political weapon: COVID-19 and Bolsonaro in Brazil'. *Harvard Kennedy School Misinformation Review*, 1:2, 1-8. https://doi.org/10.37016/mr-2020-013.

Richardson, B. J. (Eds.) (2020). *From student strikes to the extinction rebellion: New protest movements shaping our future.* Cheltenham: Edward Elgar Publishing.

Richardson, L. (2006). *What Terrorists Want: Understanding the enemy, containing the threat.* New York: Random House Publishing Group.

Robinson, G., McLean, R., & Densley, J. (2019). 'Working county lines: child criminal exploitation and illicit drug dealing in Glasgow and Merseyside'. *International Journal of Offender Therapy and Comparative Criminology*, 63:5, 694-711. https://doi.org/10.1177/0306624X18806742.

Roks, R. A., Leukfeldt, E. R., & Densley, J. A. (2021). 'The hybridization of street offending in the Netherlands'. *The British Journal of Criminology*, 61:4, 926-945. https://doi.org/10.1093/bjc/azaa091.

Romaniuk, S. N. & Manjikian, M. (Red.) (2021). *Routledge Companion to Global Cyber-Security Strategy.* London: Routledge.

Rostani, A. & Mondani, H. (2019). 'Organizing on two wheels: Uncovering the organizational patterns of Hells Angels MC in Sweden'. *Trends in Organized Crime*, 22, 34-50. https://doi.org/10.1007/s12117-017-9310-y.

Roth, R. (2018). 'Eine neue Generation von Protesten?'. *Zeitschrift für Vergleichende Politikwissenschaft*, 12:2, 429-452. https://doi.org/10.1007/s12286-018-0389-6.

Saviano, R. (Juli 2021). 'Nederland is het rottende hart van Europa'. *NRC Handelsblad*, 2-3. https://www.nrc.nl/nieuws/2021/07/30/nederland-is-het-rottende-hart-van-europa-a4053069.

Schuurman, B., Buuren, J. van & Bakker, E. (2021). *Dreigingsontwikkelingen relevant voor het stelsel bewaken en beveiligen: een blik op verleden en mogelijke toekomst.* Universiteit Leiden: ISGA Rapport.

Shek, D. T. (2020). 'Protests in Hong Kong (2019–2020): A perspective based on quality of life and well-being'. *Applied Research in Quality of Life*, 15, 619-635. https://doi.org/10.1007/s11482-020-09825-2.

Sherman, J. (September 2020). 'The Protests Prove the Need to Regulate Surveillance Tech'. *Wired*. https://www.wired.com/story/opinion-the-protests-prove-the-need-to-regulate-surveillance-tech/.

Smith, R.G., Oberman, T. & Fuller, G. (2020). 'Corruption of public officials by organised crime: understanding the risks, and exploring the solutions'. In A.

Graycar (Eds.) *Handbook on Corruption, Ethics and Integrity in Public Administration*, Cheltenham: Edward Elgar Publishing. , 80-96.

'Social Grievances and Violent Extremism in Indonesia: Exploring the appetite for psychosocial support among at-risk audiences' (December 2020). *Moonshot CVE.* https://moonshotcve.com/indonesia-social-grievances-violentextremism/.

Thijssen, G., Masthoff, E., Sijtsema, J., & Bogaerts, S. (2021). 'Understanding violent extremism: Socio-demographic, criminal and psychopathological background characteristics of detainees residing in Dutch terrorism wings'. *Criminology & Criminal Justice,* 00:0, 1-19. https://doi.org/10.1177/17488958211049019.

Thompson, J., Pronk, D. & Manen, H. van (2021). *Geopolitieke Genesis: Het Nederlandse Buitenland- En Veiligheidsbeleid in Een Wereld Na COVID-19*. The Hague: The Hague Centre for Strategic Studies. https://hcss.nl/report/strategische-monitor-2020-2021-geopolitieke-genesis/.

Thunberg, Greta, [@GretaThunberg] (13 november 2021). 'The #COP26 is over. Here's a brief summary: Blah, blah, blah. But the real work continues outside these halls. And we will never give up, ever'. *Twitter*. https://twitter.com/GretaThunberg/status/1459612735294029834?s=20.

Ting, T. Y. (2020). 'From 'be water' to 'be fire': nascent smart mob and networked protests in Hong Kong'. *Social Movement Studies,* 19:3, 362-368. https://doi.org/10.1080/14742837.2020.1727736.

Tops, P. & Tromp, P. (2017). *De achterkant van Nederland: Hoe onder- en bovenwereld verstrengeld raken*. Amsterdam: Uitgeverij Balans.

Tops, P. & Tromp, P. (2020). *Nederland drugsland*. Amsterdam: Uitgeverij Balans.

Trejo, G., & Ley, S. (2018). 'Why did drug cartels go to war in Mexico? Subnational party alternation, the breakdown of criminal protection, and the onset of large-scale violence'. *Comparative Political Studies*, 51:7, 900-937. https://doi.org/10.1177/0010414017720703.

Uhm, D. P. van, & Nijman, R. C. (2020). 'The convergence of environmental crime with other serious crimes: Subtypes within the environmental crime continuum'. *European Journal of Criminology*, 00(0), 1-20. https://doi.org/10.1177/1477370820904585.

United Nations Office on Drugs and Crime. (n.d). *Money Laundering*. https://www.unodc.org/unodc/en/money-laundering/overview.html

Vermeer, M. J., Woods, D., & Jackson, B. A. (2020). 'Would Law Enforcement Leaders Support Defunding the Police?: Probably-if Communities Ask Police to Solve Fewer Problems'. *RAND Corporation*, 1-20. https://www.jstor.org/stable/resrep26518.

Voeten, T. (2021). 'Field Report: The Netherlands as a narcostate and the emergence of a methamphetamine industry'. *Small Wars Journal*.

https://smallwarsjournal.com/jrnl/art/field-report-netherlands-narcostate-and-emergence-methamphetamine-industry.

Vugts, P. (2017). *Afrekeningen. De onderwereldoorlog op straat en in de rechtszaal*. Amsterdam: Uitgeverij de Kring.

Wainwright, T. (2016). *Narconomics: How to run a drug cartel*. London: Ebury Press.

Wijk, A. van, & Lenders, A. (2018). *Betonrot. Een kwalitatief onderzoek naar het fenomeen ondermijnende criminaliteit in Brabant-Zeeland, de effecten van en richting voor de overheidsaanpak*. Arnhem: Bekereeks.

Zuckerman, E. (2019). 'QAnon and the emergence of the unreal'. *Journal of Design and Science*, 6. https://doi.org/10.21428/7808da6b.6b8a82b9.

Zwartsen, A. (2020). 'Hazard Characterisation of New Psychoactive substances: Legal highs - A problem in disguise?'. Doctoral thesis, Utrecht University. https://dspace.library.uu.nl/handle/1874/390881.