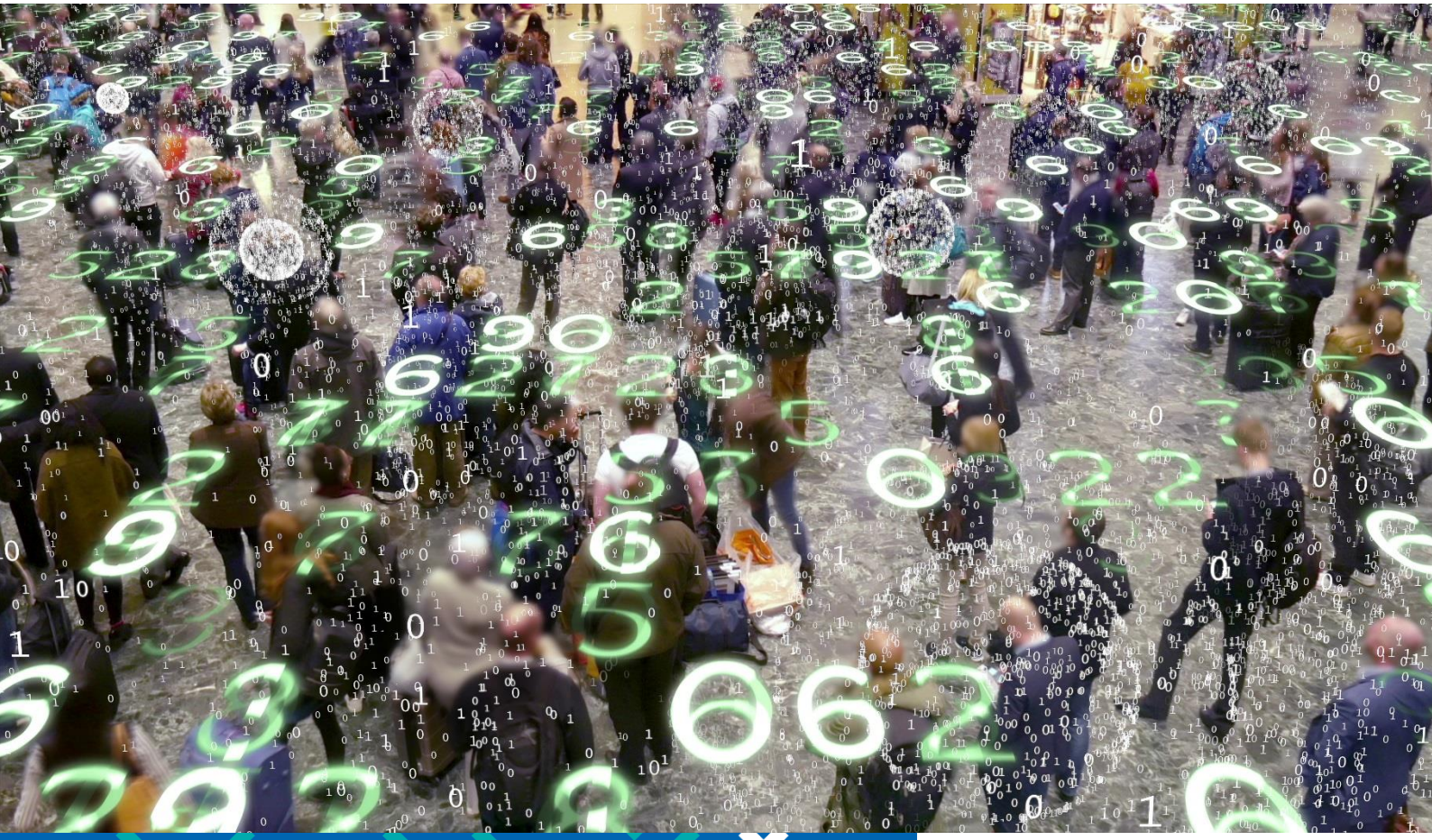
De rol van encryptie in de opsporing

Belemmeringen en mogelijkheden

Auteurs: Jurjen Jansen[1,2], Saskia Westers[1], Wendy Schreurs[2], Maike Berkenpas[1], Greg Alpár[3] & Wouter Stol[1,2,3]

[1]NHL Stenden Hogeschool, [2]Politieacademie, [3]Open Universiteit



NHL STENDEN hogeschool

Open Universiteit

POLITIE Politieacademie

De rol van encryptie in de opsporing
Belemmeringen en mogelijkheden

Datum	Februari 2023
Versie	1.0
Uitgever	Cybersafety Research Group
	NHL Stenden Hogeschool
	www.cybersciencecenter.nl
Vraagarticulatie	Minister van Justitie en Veiligheid
Opdrachtgever / subsidieverstrekker	Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)
Publicatietitel	De rol van encryptie in de opsporing: Belemmeringen en mogelijkheden
Publicatiejaar	2023
Publicatietype	Onderzoeksrapport
Auteurs	Dr. Jurjen Jansen Saskia Westers MSc Dr. Wendy Schreurs Maike Berkenpas BSc Dr. Greg Alpár Prof dr. Wouter Stol
Met medewerking van	Kimberly Bluhm
Met dank aan de begeleidingscommissie	Prof. mr. B. Niemeijer (VU Amsterdam, voorzitter) Dr. ir. J. Henseler (Hogeschool Leiden) Dr. R.S. van Wegberg (TU Delft) B.A. Boonen MSc (Ministerie van JenV) Dr. I.W.J. van der Vegt (WODC, lid tot juli 2022) Dr. L.M. van der Knaap (WODC, lid vanaf juli 2022)

Samenvatting

Encryptie, oftewel de versleuteling van gegevens, komt steeds meer voor bij allerlei vormen van criminaliteit. Dat heeft op hoofdlijnen twee oorzaken. Encryptie wordt steeds vaker standaard toegepast in software en hardware. Ook wordt het bewust gebruikt om relevante informatie en communicatie te verbergen. Een logisch gevolg is dat de opsporing vaker met encryptie te maken heeft. Een vraag die dat oproept is welke rol encryptie speelt in de opsporing. Daarover gaat dit onderzoek.

De aanleiding tot dit onderzoek is een dilemma dat gepaard gaat met encryptie. Dit dilemma is bijvoorbeeld te zien in een resolutie over versleuteling die op 14 december 2020 door de Europese Raad werd aangenomen. Enerzijds geldt encryptie daarin als noodzakelijk middel om de grondrechten en de digitale veiligheid van burgers, overheden, het bedrijfsleven en de samenleving te beschermen. Anderzijds geeft de Raad daarin aan dat de rechtshandhavings- en justitiële autoriteiten hun wettelijke bevoegdheden moeten kunnen uitoefenen om onze samenlevingen en burgers te beschermen terwijl dat door encryptie lijkt te worden bemoeilijkt.

De Nederlandse minister van Justitie en Veiligheid ondersteunt deze resolutie en heeft het WODC verzocht om de *impact* van encryptie in de opsporing nader te laten onderzoeken. Het doel van het onderzoek is het bieden van inzichten die kunnen worden benut bij de gedachtenvorming aangaande het genoemde dilemma. De onderzoekers hebben ervoor gekozen om niet het woord impact, maar rol te gebruiken. Om geenszins de illusie te wekken dat het onderzoek vooropgezet een bepaalde richting uit gaat, verwachtten wij met de term *rol* een neutralere toon aan te slaan. De centrale onderzoeksvraag waarop dit onderzoek een antwoord moet geven luidt: *Wat is de rol van encryptie in opsporingsonderzoeken van de politie?* Deze vraag is uitgewerkt in drie deelvragen: (i) Wat is de aard van encryptie in opsporingsonderzoeken?; (ii) Speelt encryptie een rol in het verloop van opsporingsonderzoeken, en zo ja hoe?; (iii) Speelt encryptie een rol in de opbrengst van opsporingsonderzoeken, en zo ja hoe?

Omdat er nog weinig informatie voorhanden is over dit onderwerp heeft het onderzoek een exploratief karakter. Voor de beantwoording van de hoofd- en deelvragen is desk- en fieldresearch uitgevoerd. Deskresearch bestond uit literatuuronderzoek, media-analyse en een analyse van rechterlijke uitspraken. Daarnaast zijn zestien oriënterende interviews gehouden met negentien medewerkers van de politie, Openbaar Ministerie (OM) en het Nederlands Forensisch Instituut (NFI). Zij konden vanuit hun kennis en ervaring een deskundig oordeel geven over het onderwerp van onderzoek. Ook is een online vragenlijst uitgezet onder medewerkers van de politie die door 177 operationeel specialisten volledig is ingevuld (responsepercentage 20%). Als laatste zijn er diepte-interviews afgenomen onder drie medewerkers van het OM en vijf van de Rechtelijke Macht (RM).

Deelvraag 1: Wat is de aard van encryptie in opsporingsonderzoeken? Er is eerst onderzocht of encryptie een rol speelt bij opsporingsonderzoeken. Op basis van het onderzoek wordt duidelijk dat encryptie overal voor komt, maar in sommige typen criminaliteit meer dan in andere. Dat encryptie voor de politie gemeengoed is geworden is voor een belangrijk deel te wijten aan mobiele telefoons die in beslag worden genomen in opsporingsonderzoeken. Op die telefoons zit vrijwel altijd een vorm van encryptie. Andere vormen van encryptie waarmee de opsporing zich geconfronteerd ziet, zijn versleutelde chatdiensten, vergrendelde devices anders dan mobiele telefoons (bijv. laptops), versleutelde e-maildiensten en cryptotelefoons. Over de omvang van encryptie kunnen op basis van het onderzoek geen concrete uitspraken worden gedaan. Deze laat zich namelijk lastig vaststellen.

Ondanks dat het niet met cijfers is te staven, ervaren politiemensen dat encryptie in de opsporing de laatste jaren sterk is toegenomen. De prevalentie is volgens geïnterviewden sterk afhankelijk van het type criminaliteit.

In termen van delictscategorieën komt encryptie volgens de geïnterviewden het meest voor bij ondermijning en in vrij grote mate ook bij high impact crimes, maar minder bij veelvoorkomende criminaliteit. Wanneer we nader inzoomen op type delicten dan speelt encryptie het meest een rol bij drugsmisdrijven, kinderporno en cybercrime in ruime en enge zin. Verder zeggen de geïnterviewden dat encryptie vooral een rol speelt bij georganiseerde vormen van criminaliteit.

Een aantal geïnterviewden onderscheidt twee soorten encryptie, namelijk technologie-gedreven encryptie (bijv. WhatsApp, waarbij berichten automatisch end-to-end encrypt worden) en mens-gedreven encryptie (bijv. cryptotelefoons, die bewust worden gekocht met als doel informatie te versleutelen). Mens-gedreven encryptie wordt door geïnterviewden beschouwd als indicator van criminaliteit. Dat dit naar voren komt in interviews wil overigens niet zeggen dat dit feitelijk zo is, maar sec dat politiemensen dit zo ervaren vanuit hun opsporingservaring. Immers, het is niet bij wet verboden om gebruik te maken van cryptotelefoons en er zijn mensen die encryptie inzetten voor hun eigen veiligheid, zoals journalisten, of om bedrijfsgeheimen te beschermen.

Deelvraag 2: Speelt encryptie een rol in het verloop van opsporingsonderzoeken, en zo ja hoe?
Om een opsporingsonderzoek waarin encryptie een rol speelt voort te zetten, wordt voornamelijk gekeken naar de prioriteit van de zaak. Ten eerste heeft een opsporingsonderzoek prioriteit als dat in het belang is van de Nederlandse samenleving. Op de tweede plek staat de door de politie gepercipieerde kans om toegang te krijgen tot de data die versleuteld zijn. Hoe groot de kans werkelijk is om toegang te krijgen tot encrypte data, laat zich niet kwantificeren.

Om toegang te krijgen tot versleutelde informatie, heeft de opsporing ruwweg twee mogelijkheden: encryptie omzeilen en encryptie kraken. Beide kunnen veel capaciteit vergen, maar dat is niet altijd het geval. Het stellig kwantificeren van ‘de benodigde tijd’ was binnen de grenzen van dit onderzoek niet haalbaar. Omzeilen kan door het vinden van de sleutel, het raden van de sleutel, het afdwingen van de sleutel, het exploiteren van een lek in de encryptiesoftware, het verkrijgen van toegang tot leesbare tekst als het apparaat in gebruik is en door het lokaliseren van een kopie van de leesbare tekst. Voor het technisch kraken – ofwel toegang krijgen tot een computersysteem met behulp van forensische hulpmiddelen – is adequate soft- en hardware nodig. Het kraken wordt volgens respondenten veelal uitbesteed aan een andere partij of afdeling, zoals het NFI. In geval van een internationale samenwerking kan Europol een rol vervullen. In hoeverre het kraken lukt, hangt af van het toegepaste cryptografische algoritme en de sleutellengte. Daarbij geldt in algemene zin: hoe langer de sleutel hoe lastiger te kraken.

Omtrent het inzetten van opsporingsbevoegdheden bepaalt het OM bijvoorbeeld of capaciteit en tijd van de Nationale Politie of het NFI wordt ingezet om versleutelde data te kraken. De opsporing beschikt over het decryptiebevel (art. 126nh lid 1 Sv) en de hackbevoegdheid (artt. 126nba, 126uba en 126zpa Sv). Hiervan wordt weinig gebruik gemaakt want deze bevoegdheden mogen alleen onder strikte voorwaarden worden ingezet. Daarnaast is de opsporing bij rechtshulpverzoeken afhankelijk van onder andere wet- en regelgeving of opgevraagde data (tijdig) geleverd worden en of ze bruikbaar zijn voor het opsporingsonderzoek.

Encryptie kan van invloed zijn op de voortzetting van opsporingsonderzoeken. Een van de uitkomsten kan zijn dat encryptie ervoor kan zorgen dat een opsporingsonderzoek wordt stopgezet.

Dit is het geval als er te weinig bewijsmateriaal is en de encrypte data (vermoedelijk) niet ontsleuteld kunnen worden. Een nuance is dat ook zonder het doorbreken of omzeilen van encryptie een zaak niet meteen verloren is. Er kan namelijk ook (ander) bewijs worden vergaard via andere manieren, waardoor het toch kan lukken om iemand te veroordelen.

Encryptie kan dus hindernissen opwerpen in de opsporing. De andere kant van de medaille is dat zodra de encryptie omzeild of gekraakt is, het opsporingsonderzoek juist sneller kan gaan. Een respondent illustreert dit door te vertellen dat na decryptie een zaak in een aantal weken rond kan zijn terwijl daar vroeger maanden tot een jaar over werd gedaan. Daarnaast wordt opgemerkt dat encryptie niet altijd een blokkerende rol speelt, omdat verdachten deze soms zelf ontgrendelen. Tot slot speelt het lerend vermogen van de politieorganisatie een belangrijke rol, alsook die van gelieerde partijen zoals het NFI, het OM en de RM. Met het ontwikkelen van kennis en opdoen van ervaring kan het kraken en omzeilen – of het inzetten van alternatieven om de bewijsvoering rond te krijgen – positief bijdragen aan de doorlooptijd van zaken waarin encryptie aanwezig is.

Deelvraag 3: Speelt encryptie een rol in de opbrengst van opsporingsonderzoeken, en zo ja hoe?
Wanneer gesproken wordt over de rol van encryptie in de opbrengst van opsporingsonderzoeken dan bedoelen we daarmee in hoeverre encryptie van invloed is op bijvoorbeeld het identificeren en/of lokaliseren van relevante personen en het succesvol achterhalen van bewijsmateriaal.

In principe speelt encryptie een belemmerende rol aangaande het identificeren en/of lokaliseren van relevante personen en goederen, van samenwerkingsverbanden of (strafrechtelijk relevante) relaties tussen personen, goederen en locaties, en de mogelijkheid om criminele activiteiten vast te stellen (signaleren). De belemmering ligt vooral in de vermindering van directe toegang tot bewijs. Tevens verschillen ontsleutelde en opgevraagde data in bruikbaarheid voor het opsporings-onderzoek. Daarnaast komen opgevraagde data regelmatig te laat, niet of zijn niet bruikbaar.

Hoewel niet duidelijk is te zeggen wat voor data – en daarmee ook bewijsmiddelen – worden gemist, en dat er dus gevallen kunnen zijn waarin verdachten onterecht vrijuit gaan, krijgen we in meerdere gesprekken terug dat het niet kunnen omzeilen of kraken van encryptie niet het einde van een opsporingsonderzoek hoeft te betekenen. In gevallen waarin het niet lukt, kunnen alternatieven ingezet worden om toch het bewijs te vergaren dat nodig is in een zaak. Denk bijvoorbeeld aan de waarde van metadata. En hoewel door encryptie het misschien lastiger en uitdagender is geworden, lukt het in gevallen vaak wel om achter encryptie te komen. Zo wordt door geïnterviewden en respondenten aangegeven dat er een relatief grote slagingskans is om informatie te bemachtigen van devices en applicaties waarbij de encryptie standaard is ingebouwd. Bewust toegepaste encryptie lijkt daarentegen lastiger te omzeilen of kraken. We kunnen dit op basis van het onderzoek echter niet staven met cijfers.

Daarnaast wordt de waarde van ontsleutelde data benadrukt. Het wordt over het algemeen gezien als zuiverder dan bijvoorbeeld (getuigen)verklaringen. De kans is volgens geïnterviewden kleiner dat deze informatie is aangepast door derden. Ook het vrijer communiceren van verdachten – die zich veilig wanen achter encryptie – draagt bij aan de waarde van de informatie. Tevens geeft men aan dat het beeld over criminele samenwerkingsverbanden vollediger is geworden na decryptie in plaats van globaal en fragmentarisch in de situatie voor en/of zonder encryptie. Bovendien, op het moment dat achter de encryptie gekomen kan worden (de fase van decryptie), ligt er potentieel een schat aan data waarmee de opsporing haar voordeel kan doen.

Hoofdvraag: Wat is de rol van encryptie in opsporingsonderzoeken? Dit onderzoek laat zien dat encryptie in opsporingsonderzoeken een prominente rol inneemt. Deze rol werkt twee kanten uit. Encryptie speelt enerzijds een belemmerende rol in de opsporing, maar anderzijds ook een praktische om de opsporing te verbeteren.

Alles overziend kan worden geconcludeerd dat het echter niet eenvoudig is om die rol in kwantitatieve termen weer te geven. Er kan niet worden vastgesteld hoeveel zaken er vanwege encryptie niet worden opgelost en/of hoeveel tijd er door de encryptie verloren gaat. Tegelijk kan ook niet worden vastgesteld hoeveel zaken er extra worden opgelost en/of hoeveel tijd wordt gewonnen. De opsporing is daarvoor een te complex geheel van feiten, toevalligheden, omstandigheden en afwegingen. Het onderzoek geeft een genuanceerd beeld van wat de toepassing van encryptie – bewust of onbewust – betekent in termen van opsporing. Er zitten negatieve kanten aan deze toepassing, maar er zijn ook positieve aspecten te benoemen.

Bij het bestuderen van encryptie moet niet alleen naar het proces van versleuteling gekeken worden. Een holistisch beeld is nodig om tot de kern van het 'probleem' van encryptie te komen. Dat is gedaan door ook bewust decryptie in het onderzoek mee te nemen. Dat de rol van encryptie in de opsporing daarmee genuanceerd ligt, zagen we ook terug in de respons die we kregen via de verschillende onderzoeksmethoden. Dit gaat bijvoorbeeld over het accepteren dat er gedeald moet worden met nieuwe fenomenen en dat daarop geacteerd moet worden. Het zogenoemde kat-en-muisspel dat optreedt tussen politie en criminelen is zo gezien een kans voor de politieorganisatie om zich verder te ontwikkelen.

Het is daarom belangrijk om te (blijven) investeren in het ontwikkelen van kennis en vaardigheden aangaande opsporing en digitale aspecten van politiewerk, zoals encryptie. Ook is het belangrijk om zicht te houden op toekomstige (technologische) ontwikkelingen en wat dat betekent voor de rol van opsporing. Denk daarbij bijvoorbeeld aan kwantumcomputing dat door deelnemers aan dit onderzoek is benoemd, maar ook aan ontwikkelingen die reeds gaande zijn, zoals 5G en op het gebied van AI (artificiële intelligentie).

Tot besluit. Dit onderzoek gaat over de rol die encryptie speelt in de opsporing. Wat we tot besluit willen meegeven is om na te denken over wat de toepassing van encryptie nu echt anders maakt voor de opsporing, en daarmee de vervolgvraag of dit dan ook anders behandeld moet worden.

De politie heeft altijd al te maken met cruciale informatie over criminaliteit die is opgeslagen in een geheugen waartoe zij niet de sleutel heeft. Dat geheugen noemen we het menselijk brein. Omdat de politie dat niet kan uitlezen (geen sleutel heeft) en de crimineel niets wil zeggen, moet zij allerlei manieren bedenken om die beveiliging te omzeilen en/of de sleutel te bemachtigen en/of iemand er toe te verleiden de informatie prijs te geven. Nu hebben we een computer die net als de crimineel zegt: je komt er niet in en ik zeg niks. Dan moet je als politie alternatieven bedenken om daar mee om te gaan. Dat deed de politie altijd al. Dus wat is er nu écht anders?

De neiging kan zijn om de huidige situatie – waarin encryptie dus dagelijks aan bod komt – te vergelijken met de situatie waarin digitale informatie nog niet versleuteld was. De vraag die daar achter ligt is welke norm wordt gevolgd. We kunnen stellen dat ten opzichte van vijf, tien of vijftien jaar geleden de huidige situatie lastiger is geworden voor de politie. We kunnen ook stellen dat in die periode de politie, met (of dankzij) encryptie, beschikt over een informatiepositie die in potentie veel groter is dan voorheen. Uiteindelijk vergt digitalisering meebewegen en aanpassen aan wat er op ons af komt. Daarin zit de voortdurende uitdaging.

Inhoudsopgave

1. Inleiding 9
1.1 Context 9
1.2 Aanleiding en relevantie 10
1.2.1 Encryptie en veiligheid 10
1.2.2 Een beperkte eerste indruk van de rol van encryptie in de opsporing 11
1.3 Probleem-, doel- en vraagstelling 12

2. Methodische verantwoording 15
2.1 Deskresearch 15
2.2 Oriënterende interviews 16
2.3 Survey 18
2.4 Diepte-interviews 19
2.5 Analyse politiesystemen 20

3. Theoretische verkenning 22
3.1 Politiewerk in informatieperspectief 22
3.2 Encryptie nader toegelicht 24
3.2.1 Encryptie en hashfuncties in de praktijk 25
3.2.2 Vormen van encryptie 26
3.3 Eerder onderzoek naar de rol van encryptie in de opsporing 28
3.3.1 Delicten waarbij encryptie voorkomt 30
3.3.2 Het verloop van opsporingsonderzoeken 33
3.3.3 De opbrengst van opsporingsonderzoeken 41

4. Resultaten 43
4.1 De aard van encryptie in opsporingsonderzoeken 43
4.1.1 Type misdrijven en encryptie 43
4.1.2 Type toepassingen van encryptie 46
4.1.3 Type verdachten en encryptie 48
4.1.4 Ontwikkelingen van encryptie in opsporingsonderzoeken in de afgelopen vijf jaar 49

4.2 Encryptie en het verloop van opsporingsonderzoeken 52
4.2.1 Factoren die van invloed zijn op het verloop van opsporingsonderzoeken 52
4.2.2 Voortzetten en stopzetten van opsporingsonderzoek 54
4.2.3 Toegang tot encrypte data en communicatie 57
4.2.4 Duiding encryptie op het verloop van opsporingsonderzoeken 67
4.3 Encryptie en de opbrengst van opsporingsonderzoeken 69
4.3.1 Bewijs 69
4.3.2 Strafrechtelijke vervolging 74
4.3.3 Rechterlijke afdoening 76

5. Conclusie, discussie en beperkingen 82
5.1 Conclusies en discussie 82
5.1.1 Wat is de aard van encryptie in opsporingsonderzoeken? 82
5.1.2 Encryptie en het verloop van opsporingsonderzoeken 84
5.1.3 Encryptie en de opbrengst van opsporingsonderzoeken 88
5.1.4 Wat is de rol van encryptie in opsporingsonderzoeken? 89
5.2 Beperkingen 91
5.3 Slotbeschouwing 93

Referenties 94

Bijlage I: Begrippen- en afkortingenlijst 99
Bijlage II: Interviewprotocol oriënterende fase 104
Bijlage III: Informed consent formulier interviews 108
Bijlage IV: Uitnodiging vragenlijst 109
Bijlage V: Vragenlijst 111
Bijlage VI: Pearson correlatietabellen 118
Bijlage VII: Summary (in English) 121

1. Inleiding

1.1 Context

Dit onderzoek gaat over encryptie oftewel de versleuteling van gegevens, en de rol die dat speelt in opsporingsonderzoeken.[1] Encryptie is een belangrijk middel om bijvoorbeeld opgeslagen informatie of internetverkeer te beveiligen. Encryptie-tools stellen gebruikers van digitale apparaten in staat om hun informatie en communicatie af te schermen voor derden. De beschikbaarheid van encryptie is groot en het gebruik ervan neemt toe. Het is essentieel voor de beveiliging van informatie binnen het bedrijfsleven, de overheid alsook voor de maatschappij in de breedste zin van het woord. Een theoretische beschouwing van encryptie is te lezen in par. 3.2.

Het versleutelen van informatie en communicatie biedt een uitkomst voor criminelen omdat zij daarmee de opsporing kunnen bemoeilijken. Een op vervolging gerichte opsporing vereist namelijk uiteindelijk het aanhouden van een verdachte. Daarvoor is nodig: een identiteit en/of een locatie van een persoon, en altijd een inhoudelijke bewijslast. Weet de politie de identiteit van een crimineel, dan kan zij zoeken naar waar die persoon zich bevindt; weet de politie de locatie van de crimineel dan kan zij de persoon die zich op die locatie bevindt aanhouden en daarna naar diens identiteit zoeken. Crimineel gebruik van encryptie is derhalve primair op gericht om bewijslast, identiteit en locatie te verhullen – en bovendien alle andere informatie die tot een identiteit of locatie kan leiden, zoals sociale relaties. Encryptie is relatief nieuw. Het spel van afschermen en onthullen van identiteiten en locaties is het onderliggende, oude principe.

Een voorbeeld van criminele encryptie is EncroChat, een aanbieder van cryptotelefoons voor crimineel gebruik, waarvan het communicatieverkeer volledig versleuteld was totdat deze gehackt werd door een Frans-Nederlandse politiesamenwerking in april 2020.[2] In 2021 hebben opsporingsdiensten een vergelijkbare dienst gehackt.[3] In november 2022 hackte de politie een illegale vuurwerk- en explosievenhandel op de encrypte berichtendienst Telegram.[4] Een voorbeeld uit 2016 betreft het FBI-Apple encryptie dispuut (San Bernandino shooting), waarbij de FBI een smartphone van een verdachte wilde onderzoeken en in een rechtszaak eiste dat Apple de FBI zou helpen om toegang tot de bewuste telefoon te krijgen. Echter, al voor de uitspraak trok de FBI die eis weer in, omdat het was gelukt om met hulp van een derde partij toegang tot de telefoon te krijgen. Details daarover heeft de FBI niet bekend gemaakt (Stol & Strikwerda, 2017). Deze voorbeelden tonen dat de politie niet altijd met lege handen staat tegenover encryptie en zich desondanks toegang tot de versleutelde informatie weet te verschaffen. Is dat eenmaal gelukt, dan lijkt encryptie te veranderen in een voordeel voor de

[1] Voor de leesbaarheid van het verslag worden de volgende termen door elkaar gebruikt en betekenen hetzelfde: 'encrypt' en 'versleuteld', en 'decrypt' en 'ontsleuteld'. Encrypt/versleuteld kan worden beschreven als het beschermen van informatie door deze in een vorm te plaatsen die alleen kan worden gelezen door mensen die de sleutel hebben om dit te doen. Decrypt/ontsleuteld kan worden beschreven als het terug veranderen van elektronische informatie die in code is geschreven in een vorm die men normaal kan begrijpen en gebruiken. Zie Bijlage I voor een begrippenlijst.

[2] Driessen, C. & Meeuws, J. (2021). *Nederlandse politie speelde grote rol bij Encro-hack*. Verkregen via: https://www.nrc.nl/nieuws/2021/03/14/grote-rol-politie-bij-encro-hack-a4035545

[3] Laumans, W. & Vugts, P. (2021). *'Stress in Dubai' na kraak berichtendienst Sky ECC.* Verkregen via: https://www.parool.nl/amsterdam/stress-in-dubai-na-kraak-berichtendienst-sky-ecc~b9fd28fe/

[4] NOS (2022). *Politie ontmantelt netwerk dat in illegaal vuurwerk en explosieven handelde*. Verkregen via: https://nos.nl/artikel/2453548-politie-ontmantelt-netwerk-dat-in-illegaal-vuurwerk-en-explosieven-handelde

opsporing. Omdat criminelen zich achter de encryptie veilig waanden, is er dan ineens een schat aan informatie voor de opsporing beschikbaar.[5] Ook dat aspect krijgt aandacht in dit onderzoek.

De vier zojuist gegeven voorbeelden zijn *grote* zaken, waaraan landelijk opererende politie-specialisten werkten en die media-aandacht trokken. Maar zoals gezegd is encryptie wijd verbreid. Het speelt daardoor ook in talloze *kleine* zaken een rol, zoals een aangifte van mishandeling aan een basisteam (art. 300 Sr). Of sprake is van voorbedachten rade (art. 301 Sr), kan worden vastgesteld op basis van de (encrypte) chats tussen de daders. In dergelijke gevallen gaat het niet direct om grote zaken maar mogelijk wel om grote aantallen. Daarom is encryptie in die context eveneens onderwerp van dit onderzoek.

Vanuit het perspectief van de opsporing kan het gebruik van encryptie door verdachten geduid worden als (digitale) 'anti-forensics'. Conlan e.a. (2016) presenteren een taxonomie op het gebied van anti-forensics. Daarin onderscheidden zij vier hoofdcategorieën: (i) 'data hiding' (het verbergen van data), (ii) 'artifact wiping' (het opzettelijke vernietiging van gegevens die als bewijs kunnen worden gebruikt), (iii) 'trail obfuscation' (de opzettelijke activiteit om een forensisch onderzoek op een digitaal systeem of netwerk te desoriënteren en af te leiden) en (iv) 'attacks against computer forensic tools and processes' (directe aanvallen op de software die wordt gebruikt om digitale media te onderzoeken). Ons onderzoek gaat over encryptie en valt daarmee binnen de eerste categorie.

1.2 Aanleiding en relevantie

Op 14 december 2020 werd door de Europese Raad een resolutie aangenomen over versleuteling waarin enerzijds werd verklaard encryptie als noodzakelijk middel te beschouwen om de grondrechten en de digitale veiligheid van burgers, overheden, het bedrijfsleven en de samenleving te beschermen. Anderzijds geeft de Raad ook aan dat de rechtshandhavings- en justitiële autoriteiten hun wettelijke bevoegdheden moeten kunnen uitoefenen om onze samenlevingen en burgers te beschermen (Europese Raad, 2020). De minister van Justitie en Veiligheid heeft de Tweede Kamer te kennen gegeven deze resolutie te ondersteunen en heeft daarbij het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) verzocht om de impact van encryptie in de opsporing nader te laten onderzoeken.[6] Dit rapport is het resultaat hiervan. Ook in groter internationaal verband speelt dit vraagstuk dus een rol (zie bijv. Ilbiz & Kaunert, 2022; The United States Department of Justice, 2020), maar dit onderzoek beperkt zich tot de Nederlandse situatie.

1.2.1 Encryptie en veiligheid

De aanleiding tot dit onderzoek is het dilemma dat gepaard gaat met encryptie. Vanuit het perspectief van burgers, bedrijven en overheden – waaronder ook de strafrechtketen – fungeert encryptie als een belangrijke tool voor het beschermen van digitale informatie en levert daarmee een belangrijke bijdrage aan veiligheid en privacy. Te denken valt bijvoorbeeld aan preventie van datalekken. Encryptie kan vanuit dit perspectief worden geduid als 'privacy-enhanching technology'. Vanuit het perspectief van de strafrechtketen zijn er signalen dat encryptie vaak ook als een obstakel dient. Wanneer opsporingsdiensten in aanraking komen met encryptie – bewust toegepast of gewoontegetrouw

[5] Driessen, C. (2021). *Internationale coalitie tapte achttien maanden lang criminelen af via 'niet-kraakbare' app*. Verkregen via: https://www.nrc.nl/nieuws/2021/06/08/internationale-coalitie-tapte-achttien-maanden-lang-criminelen-af-via-niet-kraakbare-app-a4046442

[6] Kamerstukken TK 2020-2021, 26643 nr. 729. Verkregen via: https://zoek.officielebekendmakingen.nl/kst-26643-729.html

gebruikt door criminelen/verdachten bij criminele activiteiten – kan dat hun werk hinderen: anti-forensics.

Encryptie heeft dus een januskop: zij dient de bescherming van informatie en privacy, en fungeert tegelijk als anti-forensics, wat de maatschappelijke veiligheid juist weer niet ten goede komt. In dit debat speelt het zogenoemde decryptiebevel, het onder dwang toegang moeten geven tot versleutelde informatie, een centrale rol (Stol & Strikwerda, 2017). De resultaten van dit onderzoek dienen input te vormen voor het debat over het belang van encryptie voor de bescherming van informatie en privacy tegenover het knelpunt dat encryptie vormt voor de slagvaardigheid van de opsporing. Om dit debat voldoende te kunnen informeren, moet eerst onderzocht worden wat de daadwerkelijke rol is van encryptie in de opsporing in de huidige Nederlandse context. Op dit moment is dat onvoldoende inzichtelijk (zie sectie 1.2.2). Met dit onderzoek wordt dit beeld aangescherpt. Dit onderzoek gaat enkel over de feitelijke 'rol-vraag'. In dit onderzoek wordt dus geen standpunt ingenomen in het hiervoor aangeduide maatschappelijk debat over veiligheid versus privacy. Ook draait het onderzoek niet om de politie-interne gevolgen van encryptiegebruik door de politie, zoals beveiligde communicatie tussen politiemensen, maar sec om het criminele gebruik ervan.

1.2.2 Een beperkte eerste indruk van de rol van encryptie in de opsporing

Vooralsnog is onduidelijk wat de precieze rol is van encryptie in de opsporing. In de (inter)nationale literatuur is maar een beperkt aantal schattingen te vinden van het aandeel opsporingsonderzoeken dat belemmerd wordt door encryptie, en van de verschillende vormen van encryptie. De beschikbare aantallen zijn schattingen van betrokkenen in de opsporing en geen resultaat van grootschalige representatieve onderzoeken.

In een enquête uit 2016 onder vijfentwintig EU-lidstaten, uitgevoerd door de Europese Raad en Europol, gaf de meerderheid (twintig lidstaten) aan dat encryptie vaak of bijna altijd opspeelt in opsporingsonderzoeken (Council of the European Union, 2016). Ze spreken over encryptie van zowel online communicatiemiddelen (e-mail) als offline hardware of apps. In het PricewaterhouseCoopers (2020) rapport 'Doorlichting strafrechtketen' wordt aangegeven dat door encryptie van communicatie en grote hoeveelheden data de opsporing tijdrovender en complexer is geworden. In een andere studie geven dertien van de tweeëntwintig geïnterviewde opsporingsambtenaren aan dat het regelmatig voorkomt dat inbeslaggenomen gegevensdragers niet toegankelijk zijn (Mevis e.a., 2016).

Door de toepassing van end-to-end encryptie is 70% van de in de VS gerapporteerde online-kindermisbruikzaken via de platformen van Facebook (Facebook, Instagram, Messenger, WhatsApp) niet te detecteren voor zowel handhavingsinstanties als Facebook zelf (Nb. Facebook heet nu Meta). Terwijl ook uit onderzoek blijkt dat 94% van gerapporteerde online-kindermisbruikzaken wordt aangeboden via deze platformen (Koomen, 2021). Voor de Nederlandse opsporingsinstanties is deze informatie relevant, omdat Europese en specifiek Nederlandse internetservers wereldwijd het meeste online kinderpornografisch beeldmateriaal aanbieden.[7]

Kwantitatieve data in de vorm van tapstatistieken uit de VS tonen dat in 2018 bij ongeveer 5% van de taps sprake was van encryptie (United States Courts, 2020). Van deze 5% was in 87% van de gevallen geen mogelijkheid om toegang te krijgen tot de data. Deze cijfers tonen een toename ten

[7] BBC (2019). *Netherlands 'hosts most child sex abuse images'*. Verkregen via: https://www.bbc.com/news/technology-48022950

opzichte van 2017 en 2016, waarbij respectievelijk in 2,7% en 1,8% van de gevallen sprake was van encryptie. Statistieken van de Officier van Justitie van Manhattan (VS) laten zien dat 64% van de in beslaggenomen telefoons in 2019 vergrendeld is (Manhattan District Attorney's Office, 2019).

Succesvolle decryptie-operaties van de Nederlandse politie wijzen erop dat ontsleutelde informatie een waardevolle bron is voor politieonderzoeken. Een greep uit enkele succesvolle Nederlandse decryptie-operaties zijn die van IronChat (2018, veertien aanhoudingen)[8], EncroChat (2020, tientallen aanhoudingen)[9] en Sky ECC (2021, dertig aanhoudingen).[10] Door encryptie wanen criminelen zich onbespied en delen voor de opsporing bruikbare informatie op deze platformen. Overigens brengt dit wel weer andere (praktische) vragen met zich mee, zoals over de (on)mogelijkheden om grote hoeveelheden data te kunnen 'uit-rechercheren'.

Encryptie lijkt er regelmatig voor te zorgen dat de toegang tot data voor opsporingsdiensten onmogelijk is, omdat wetgeving en leveranciers zoals Apple, Android of Meta de mogelijkheid niet (kunnen of willen) bieden om de data te ontsleutelen. Samengevat laten bovenstaande statistieken slechts een beperkt beeld zien. Dit beeld is ook nog eens niet actueel en niet specifiek voor de Nederlandse context. Onderhavig onderzoek beoogt in die leemte te voorzien door de rol van encryptie in de Nederlandse opsporingspraktijk in kaart te brengen. In dit onderzoek wordt alleen naar encryptie gekeken zoals toegepast door verdachten, en bijvoorbeeld niet zoals toegepast door politiemensen om opsporingsgegevens te beveiligen.

1.3 Probleem-, doel- en vraagstelling

Probleemstelling

Aan de hand van het vorengaande komen we tot de volgende probleemstelling, namelijk dat op moment van aanvang van het onderzoek de rol van encryptie in het verloop en de opbrengst van opsporingsonderzoeken onvoldoende duidelijk is.

We kiezen expliciet voor de term 'rol' in de probleemstelling en niet voor bijvoorbeeld 'impact' of 'effect'. Onder *impact* verstaan wij de invloed van een actie of fenomeen (in dit geval encryptie) op iets of iemand (in dit geval de opsporing). Wij merkten echter bij aanvang van het onderzoek dat impact een negatieve lading met zich meedraagt, waardoor de indruk kan ontstaan dat in het onderzoek (slechts) naar negatieve aspecten van encryptie wordt gekeken. Om geenszins de illusie te wekken dat het onderzoek vooropgezet een bepaalde richting uit gaat, verwachtten wij met de term *rol* een neutralere toon aan te slaan. Onder *effect* kan het maatschappelijke gevolg of resultaat worden verstaan van een actie of een fenomeen. Dit ligt echter buiten de scope van dit onderzoek.

Daarnaast verdienen 'verloop' en 'opbrengst' uit de probleemstelling nadere toelichting. Als we spreken over de rol van encryptie in het *verloop* van opsporingsonderzoeken dan bedoelen we daarmee bijvoorbeeld de slagingskans om encryptie te kraken, te omzeilen of alternatieve opsporings-middelen in te zetten en wat dit betekent in termen van inzet van mensen en middelen. Wanneer we

[8] Politie (2018). *Doorbraak in onderscheppen cryptocommunicatie*. Verkregen via: https://www.politie.nl/nieuws/2018/november/6/02-doorbraak-in-onderscheppen-cryptocommunicatie.html

[9] Andringa R. (2020). *Al tientallen strafzaken na EncroChat-hack en het einde is nog niet in zicht.* Verkregen via: https://nos.nl/artikel/2361112-al-tientallen-strafzaken-na-encrochat-hack-en-het-einde-is-nog-niet-in-zicht

[10] Peters. J. (2021). *Dertig aanhoudingen in Nederland na ontsleutelen communicatie criminelen*. Verkregen via: https://www.nu.nl/binnenland/6120847/dertig-aanhoudingen-in-nederland-na-ontsleutelen-communicatie-criminelen.html

spreken van de rol van encryptie in de *opbrengst* van opsporingsonderzoeken dan bedoelen we daarmee in hoeverre encryptie van invloed is op bijvoorbeeld het identificeren en/of lokaliseren van relevante personen en het succesvol achterhalen van bewijsmateriaal. Meer concreet: in hoeverre encryptie van invloed is op de mogelijkheden om verdachten succesvol of kansrijk te kunnen vervolgen.

In de probleemstelling ligt de focus op opsporingsonderzoeken omdat die nu eenmaal in de strafrechtketen de eenheden zijn waarmee men rekent en waarop men het proces stuurt. Wanneer in het onderzoek bijvoorbeeld aandacht is voor versleutelde telefoons, gaat de aandacht van ons onderzoek uit naar wat voor rol dit speelt in de opsporing − en is de focus bijvoorbeeld niet bij hoeveel van de in beslag genomen telefoons encryptie een rol speelt. Immers, niet 'in beslag genomen telefoons' maar 'opsporingsonderzoeken' zijn de cruciale eenheden in de strafrechtketen.

Doelstelling

Met dit onderzoek willen we kennis verwerven over de rol van encryptie in opsporingsonderzoeken. Het doel van dit onderzoek is drieledig: inzicht bieden in (i) de aard van encryptie in opsporingsonderzoeken, (ii) de rol van encryptie in het verloop van opsporingsonderzoeken en (iii) de rol van encryptie in de opbrengst van opsporingsonderzoeken.

Het onderzoek gaat primair over de opsporing en niet over andere politiestrategieën voor criminaliteitsbestrijding, te weten preventie, verstoring en identificatie van slachtoffers zonder aandacht voor een verdachte. De nadruk in het onderzoek ligt op politiewerk, want in de zogenoemde trechter van de strafrechtketen is de rol van encryptie daar het eerste merkbaar en kan ook daar zorgen voor (vroegtijdige) uitstroom van zaken, of de instroom van zaken verhinderen dan wel de instroom van zaken vergroten. Wel verkennen we de mogelijke implicaties van encryptie op de vervolging en berechting van verdachten.

Het hoger gelegen doel van het onderzoek is om met de vergaarde informatie het debat over encryptie – 'privacy-enhancing' technologie versus 'anti-forensics' – te informeren. Wij vinden het belangrijk om nogmaals expliciet toe te lichten dat met dit onderzoek dus géén positie wordt ingenomen in het grotere encryptiedebat dat momenteel gaande is in de samenleving. Het onderzoek heeft niet tot doel om inzicht te geven in het proportionaliteitsvraagstuk dat onder dit debat ligt. Tevens heeft het onderzoek niet tot doel om de bredere ontwikkelingen op gebied van digitalisering (en de opsporing) – zowel positief als negatief – te duiden.

Vraagstelling

De centrale onderzoeksvraag luidt: Wat is de rol van encryptie in opsporingsonderzoeken van de politie? Om de centrale onderzoeksvraag te beantwoorden zijn onderstaande deelvragen geformuleerd:

1. Wat is de aard van encryptie in opsporingsonderzoeken?
    a. In welke situaties komt encryptie voor in opsporingsonderzoeken?
    b. Welke vormen van encryptie komen voor in opsporingsonderzoeken?
    c. In hoeverre komt encryptie voor in opsporingsonderzoeken?
    d. Is de aard van encryptie in opsporingsonderzoeken tussen 2016-2020 veranderd, en zo ja in welk opzicht?

2. Speelt encryptie een rol in het verloop van opsporingsonderzoeken, en zo ja hoe?
    a. Wat zijn de relevante technische aspecten van de toepassingen van encryptie met betrekking tot opsporingsonderzoeken?
    b. Hoe beïnvloeden externe technische factoren de efficiëntie van het kraken van de encryptie?
    c. Zijn er juridische en/of ethische aspecten die een rol spelen in opsporingsonderzoeken waarin encryptie voorkomt, en zo ja welke?
    d. Tot op welke hoogte lukt het om toegang te krijgen tot voor de opsporing relevante digitale informatie in zaken waarin encryptie voorkomt, en onder welke omstandigheden?
    e. In geval encryptie de toegang belemmert tot voor de opsporing relevante digitale informatie, in hoeverre worden dan alternatieve opsporingsmiddelen ingezet en hoe effectief zijn deze?
    f. Speelt encryptie een rol in de voortzetting en/of doorlooptijd van opsporingsonderzoeken, en zo ja hoe?
    g. Speelt encryptie een rol in beslissingen van het OM omtrent het inzetten van opsporingsbevoegdheden, en zo ja hoe en waarom?

3. Speelt encryptie een rol op in de opbrengst van opsporingsonderzoeken, en zo ja hoe?
    a. Wat is de rol van encryptie aangaande:
        i. Het identificeren en/of lokaliseren van relevante personen en goederen?
        ii. Het vaststellen van samenwerkingsverbanden of (strafrechtelijk relevante) relaties tussen personen, goederen en locaties?
        iii. De mogelijkheid om criminele activiteiten vast te stellen (signaleren)?
        iv. Het vergaren van bewijsmateriaal?

Leeswijzer

In hoofdstuk 2 worden de onderzoeksmethoden verantwoord. Vervolgens wordt in hoofdstuk 3 een theoretische verkenning gepresenteerd. Daarin wordt het theoretisch raamwerk ‘politiewerk in informatieperspectief’ beschreven, het onderwerp encryptie behandeld en wordt ingegaan op bestaande kennis over dit onderwerp in relatie tot de opsporing. In hoofdstuk 4 staan de resultaten centraal. De conclusies en daaruit volgende discussie en beperkingen staan centraal in hoofdstuk 5. Dat hoofdstuk eindigt met een slotbeschouwing.

2. Methodische verantwoording

In dit hoofdstuk staat de methodische verantwoording centraal. Om de onderzoeksvragen te beantwoorden hebben we verschillende onderzoeksmethoden ingezet: deskreseach (par. 2.1), oriënterende interviews (par. 2.2), een survey (par. 2.3) en diepte-interviews (par. 2.4). Tabel 2.1 bevat een methodenmatrix waarin is weergegeven welke deelvragen met welke methoden zijn beantwoord. In par. 2.5 beschrijven we een aanvullende methode die we wilden inzetten, maar die niet is geslaagd.

Tabel 2.1: Methodenmatrix

Methode / ***Deelvraag***	**Deskresearch**	**Oriënterende interviews**	**Survey opsporing**	**Diepte-interviews**
1. Aard encryptie opsporing?	X	X		
2. Rol verloop opsporing?		X	X	X
3. Rol opbrengst opsporing?		X	X	X

2.1 Deskresearch

Deskresearch heeft bijgedragen aan het beantwoorden van deelvraag 1. Daarnaast gaf het enkele inzichten die gebruikt zijn voor het beantwoorden van deelvragen 2 en 3. De deskresearch bestaat uit literatuuronderzoek, media-analyse en een analyse van rechterlijke uitspraken. Hoe invulling is gegeven aan deze vormen van deskresearch is hierna verantwoord.

Literatuuronderzoek. Gezien de afbakening van het onderzoek, dat zich richt op de afgelopen vijf jaar is gezocht op bronnen vanaf 2016. Bij het doorlezen van de gevonden literatuur is aan de hand van referentielijsten soms verwezen naar bronnen van voor 2016. Voor het literatuuronderzoek zijn 33 databases doorzocht, waaronder ScienceDirect, SAGE Premier en Wiley Online Library. De volgende zoektermen (Nederlands en Engels) zijn (al dan niet in combinatie) gebruikt:

- Encrypt*, versleutel*, decrypt*, crypto, code, decode
- Opspor*, handhav*, crimi*, law enforcement, investig*, detection, forensic analysis
- Politie, recht*, instanties, police, europol, OM
- Anon*, EncroChat, SKY ECC, IronChat, ANOM

Media-analyse. Voor de media-analyse is Nexus Uni gebruikt. Nexus Uni is een onderzoeksplatform waar toegang wordt verkregen tot een online krantenarchief. Via Nexus Uni zijn twee zoekslagen uitgevoerd, namelijk ‘encryptie AND politie OR recht’ en ‘versleutel* AND politie OR recht’. Alle zoekslagen richten zich op dezelfde tijdsperiode, namelijk van 1 januari 2016 tot en met 30 juni 2021. Daarnaast zijn dezelfde kranten gebruikt in elke zoekslag, namelijk: NRC, Het Parool, Volkskrant, Trouw, Algemeen Dagblad, de Telegraaf en Nederlands Dagblad.

Bij de eerste zoekterm (93 hits) is ervoor gekozen om elk even artikel te analyseren. Bij de tweede zoekterm (734 hits) elk dertiende artikel zodat er bij de zoekslagen ongeveer een even aantal artikelen kon worden geanalyseerd. De redenen om een willekeurige selectie van mediaberichten te analyseren betreffen prioriteit en tijd. In totaal zijn 102 mediaberichten geanalyseerd. Voor de analyse is een tabel ingevuld waarbij steeds dezelfde informatie werd vastgelegd: soort criminaliteit, jaar, type encryptie, toepassingsvorm encryptie, rol ten aanzien van strafrechtelijk onderzoek en encryptie succesvol omzeild/gekraakt of alternatief toegepast. De resultaten leverden niet veel nieuwe inzichten

op, vergeleken met het literatuuronderzoek en de oriënterende interviews. Enkele bevindingen zijn geïntegreerd in hoofdstuk 3.

Analyse rechterlijke uitspraken. De website rechtspraak.nl stelt men in staat om vrij toegankelijk te zoeken naar rechterlijke uitspraken. Deze bron bevat volgens de voorzitter van de Raad voor de rechtspraak (Rvdr) 'minder dan 5% van alle uitspraken'[11], maar kan niettemin helpen om een (aanvullend) beeld te krijgen van bepaalde fenomenen, zoals encryptie. Op deze website is op gestructureerde wijze een analyse uitgevoerd middels een daarvoor ontwikkeld protocol (op te vragen bij de auteurs). Voor deze analyse zijn twee zoekslagen uitgevoerd. Beide richten zich op dezelfde tijdsperiode van 1 januari 2016 tot en met 30 juni 2022. Door uitloop van het onderzoek (zie par. 2.2 en 2.4) beslaat deze zoekslag een langere tijdsperiode dan de media-analyse.

De zoektermen 'encrypt*' en 'versleutel*' zijn gebruikt. Bij de eerste zoekterm zijn in totaal 237 uitspraken gevonden, waarvan 77 zijn geanalyseerd (elke derde uitspraak). Wat opvalt is dat in de periode 1 januari 2021 t/m 30 juni 2022 meer hits zijn (166) dan in 2016 tot en met 2020 bij elkaar. Bij de tweede zoekterm zijn 483 uitspraken uit de zoekslag voortgekomen waarvan 48 zijn geanalyseerd (elke tiende uitspraak). Ook hier zijn de meeste hits verkregen in het laatste anderhalf jaar van de selectie (248). Net zoals bij de media-analyse is de analyse uitgevoerd op een willekeurige steekproef (125 uitspraken) en zijn dezelfde onderwerpen gescoord: soort criminaliteit, jaar, type encryptie, toepassingsvorm encryptie, rol ten aanzien van strafrechtelijk onderzoek en encryptie succesvol omzeild/gekraakt of alternatief toegepast. In veel gevallen komen de grotere zaken aan bod, zoals Sky ECC, EncroChat en Ennetcom. Hoewel niet veel nieuwe informatie naar voren kwam zijn enkele resultaten van deze analyse geïntegreerd in hoofdstuk 4.

2.2 Oriënterende interviews

Omdat encryptie binnen de opsporing of de bredere strafrechtketen een veelomvattend onderwerp is, is besloten om vooraleerst een reeks oriënterende interviews te houden. De veronderstelling was dat door vanuit verschillende invalshoeken meer te leren over de rol van encryptie, het resterende deel van het onderzoek beter gekaderd en afgebakend kon worden.

Omdat het onderzoek hoofdzakelijk betrekking heeft op de praktische implicaties van encryptie, wat begint bij de opsporing, zijn voornamelijk experts vanuit de politieorganisatie benaderd. Hoewel de primaire focus dus op de politie (opsporing) ligt, kozen we ervoor om ook experts te bevragen van het Openbaar Ministerie (OM) en het Nederlands Forensisch Instituut (NFI) van het Ministerie van Justitie en Veiligheid. Dit zijn namelijk ook belangrijke actoren in dit verhaal: het OM geeft leiding aan het opsporingsonderzoek en het NFI heeft specialistische kennis op het gebied van encryptie en betrokkenheid bij strafzaken.

Om de semigestructureerde interviews in goede banen te leiden is daarvoor een interviewprotocol ontwikkeld (zie bijlage II). Het benaderen van interviewkandidaten die werkzaam zijn voor de politie verliep via het team Onderzoekscoördinatie van Directie Operatiën van de Nationale Politie.[12] Dit betreft een afgesproken werkwijze tussen het WODC en de Nationale Politie.

[11] NRC (2020). *Rechtspraak wil driekwart van de vonnissen online publiceren* Verkregen via: https://www.nrc.nl/nieuws/2021/05/30/rechtspraak-wil-driekwart-van-de-vonnissen-online-publiceren-a4045465

[12] De onderzoekers zijn de oriënterende interviewfase gestart met een andere strategie, namelijk door in het eigen netwerk verzoeken tot deelname aan een interview uit te zetten en via de sneeuwbalmethode in contact te komen met relevante

De betreffende contactpersoon benaderde de door ons aangedragen experts, en droeg ook suggesties aan voor aanvullende experts die zich in hun politiewerk bezighouden met encryptie. Deze werkwijze zorgde er dus niet voor dat de onafhankelijkheid van het onderzoek in het geding kwam.

Voorafgaande aan de vrijwillige en geanonimiseerde interviews zijn de deelnemers geïnstrueerd over het onderzoek en werd hen de gelegenheid gesteld om vragen te stellen ten aanzien van hun deelname aan het interview. Daarnaast vroegen we de deelnemers voorafgaand aan de interviews om – via Microsoft Forms – een informed consentformulier te ondertekenen (zie bijlage III). Daarin konden zij tevens expliciet aangeven in hoeverre de resultaten anoniem verwerkt dienen te worden of dat bijvoorbeeld hun functie genoemd mag worden. Het informed consent formulier is gebaseerd op het informed consent formulier zoals verstrekt door de afdeling Research Support van NHL Stenden Hogeschool op 15 oktober 2021.

We vroegen de deelnemers na ondertekening van het formulier toestemming om de interviews auditief op te nemen. Bij akkoord werkten we aan de hand van de audio-opnames de interviews uit tot een gespreksverslag. We legden het gespreksverslag ter controle voor aan de geïnterviewde. Ook stelde het de geïnterviewde in staat om informatie toe te voegen, bijvoorbeeld wanneer hem of haar dit tijdens het interview was ontschoten. Op het moment dat de geïnterviewde zijn of haar akkoord gaf op het verslag werd deze beschouwd als 'vastgesteld' en werd deze opgeslagen in Research Drive.[13] Na definitieve vaststelling werd het audiobestand – indien aanwezig – verwijderd.

In deze fase van het onderzoek hebben we met negentien deskundigen gesproken in zestien verschillende interviews, zie onderstaande opsomming voor het overzicht van deelnemers. Elf daarvan kwamen binnen via de eerste strategie en acht door middel van de tweede.

- Accountmanager Publiek Private Samenwerking
- Commissaris van de Nationale Politie
- Duo interview: beide digitaal rechercheur
- Landelijk OvJ
- Digitaal rechercheur
- Teamchef
- Senior Wetenschappelijk onderzoeker bij NFI
- Senior adviseur Digitale Opsporing
- Hoofd Dienst Regionale Recherche
- Digitaal rechercheur, Team Bestrijding Kinderporno en Kindersekstoerisme (TBKK)
- Duo interview: beide operationeel specialist, Team High Tech Crime (THTC)
- Digitaal rechercheur, TBKK
- Medewerker afdeling Interceptie
- Afdelingshoofd TBKK en THTC, Dienst Landelijke Recherche
- Commissaris van Politie bij Staf Korpsleiding, Directie Strategie en Innovatie
- Duo interview: beide teamleider, Voorziening Crypto Analyse Team (VCAT)

experts. Conform WODC-beleid hebben we deze werkwijze – na negen interviews, waarbij we met tien politiemensen spraken – moeten stopzetten. Door de wijziging in strategie heeft de oriënterende fase van het onderzoek vertraging opgelopen.

[13] Met Research Drive kunnen in een online omgeving onderzoeksgegevens worden opgeslagen en gedeeld. Research Drive wordt als dienst aangeboden door SURF; een coöperatieve vereniging van Nederlandse onderwijs- en onderzoeksinstellingen. Zie: https://www.surf.nl/

De interviews vonden plaats van 27 oktober 2021 tot en met 20 mei 2022. Ze werden in wisselende samenstelling afgenomen door twee onderzoekers en vonden veelal online plaats (via Microsoft Teams). In vijf gevallen werd het interview in hybride vorm afgenomen en in één geval fysiek. De hybride variant houdt in dat één onderzoeker fysiek op locatie was en de tweede online deelnam. De voornaamste reden om het interview met twee personen af te nemen, was dat het om een (politiek) gevoelig onderwerp gaat, waardoor niet alle geïnterviewden zich comfortabel voelden om het interview op te laten nemen. Bovendien kon op deze manier één de leiding nemen in het gesprek, terwijl de tweede met het gesprek kon mee typen.

We poogden in deze fase nog een aantal aanvullende OM-medewerkers te interviewen. Op drie uitnodigingen werd gereageerd met het bericht dat men niet wilde meewerken. De belangrijkste reden voor deze potentiële interviewkandidaten was de politieke gevoeligheid rondom het onderwerp. Op een interviewverzoek bij Europol kwam geen reactie. Via Onderzoekscoördinatie kwam één weigering terug vanuit de politiedoelgroep. Deze weigering hield verband met een gebrek aan tijd.

Na afronding van deze interviewfase zijn de onderzoeksdata handmatig geanalyseerd. Omdat het een relatief gering aantal geïnterviewden betreft, maakten we voor de oriënterende interviews geen gebruik van kwalitatieve data-analyse software, zoals Atlas.ti.

2.3 Survey

Voor dit onderzoek is tevens een vragenlijst ontwikkeld. De vragen zijn gebaseerd op de onderzoeksvragen en datgene wat we hebben geleerd uit de oriënterende interviews. We hebben getracht de vragenlijst niet te omvangrijk te maken, met het oog op het responspercentage.

De vragenlijst heeft meerdere iteraties ondergaan voordat deze zijn definitieve vorm kende. Eerst is de vragenlijst besproken met de leden van de begeleidingscommissie. Daarop zijn enkele details in de vragenlijst aangepast. Vervolgens is de vragenlijst gepretest onder twee professionals die werkzaam zijn binnen de politieorganisatie. Op basis daarvan zijn enkele bewoordingen en definities aangepast, zodat deze beter passen bij de organisatiecultuur van de politie. Een voorbeeld hiervan is de indeling van de bevraagde criminaliteitsvormen waarmee politiemensen in hun dagelijkse werk te maken hebben.

Vervolgens is de vragenlijst omgezet naar een online versie. Dit is gedaan door een extern bureau dat vragenlijsten ontwerpt en host. De online versie van de vragenlijst is gepretest door drie onderzoekscollega's van NHL Stenden Hogeschool, de Politieacademie en de Open Universiteit. Op basis van die pretest zijn enkele vragen en antwoordcategorieën aangepast, omdat deze multi-interpretabel waren. Ook zijn enkele gebruiksvriendelijkheidsissues aangepakt. Na een laatste check van de onderzoekers op het online instrument, waaruit nog enkele opmaak issues naar voren kwamen, is de ontwikkeling van de vragenlijst afgerond. De eindversie van de vragenlijst staat in Bijlage V.

Met Onderzoekscoördinatie van de Nationale Politie is afgestemd om voor dit surveyonderzoek Operationeel Specialisten A, B en C te benaderen die werkzaam zijn in het vakgebied 'tactische opsporing'. De populatie is N=1.394. Hiervan waren 511 recent benaderd voor medewerking aan andere onderzoeken. Dit betekent dat wij een representatieve steekproef van N=883 niet-benaderde Operationeel Specialisten (OS) mochten uitnodigen om deel te nemen aan het vragenlijstonderzoek. We konden hen benaderen via geanonimiseerde e-mailadressen, die we na de dataverzameling hebben vernietigd. Deze doelgroep opereert vaak vanuit leidinggevende functies. Daarom spreken wij in verschillende onderdelen van de vragenlijst de respondent niet persoonlijk aan,

maar vragen we hen om te antwoorden vanuit het perspectief van het team waarin zij werken c.q. leiding aan geven.

De dataverzameling is gestart op 30 juni 2022. Hiervoor benaderden we N=883 politiemensen (zie Bijlage IV voor de vragenlijstuitnodiging). Na ongeveer anderhalve week hadden 105 politiemensen de vragenlijst volledig ingevuld. Op 12 juli 2022 is een eenmalige herinneringsmail gestuurd. De dataverzameling is geëindigd op 22 juli. Uiteindelijk zijn 240 politiemensen met de vragenlijst gestart. Hiervan behoorden veertien niet tot de doelgroep en zijn daarom uitgesloten van deelname. 49 politiemensen zijn vroegtijdig gestopt met het invullen van de vragenlijst. In 26 gevallen was dit op de 'consent pagina'. In totaal hebben N=177 politiemensen de vragenlijst volledig ingevuld. Dit betekent een netto responsepercentage van 20%.[14] De gemiddelde invultijd was 13:50 minuten en de mediaan was 11:44 minuten. Ook het databestand is opgeslagen in Research Drive.

De respondenten werken voornamelijk op regionaal (45,2%), districtelijk (29,4%) en landelijk (23,2%) niveau. De respondenten zijn werkzaam als OSA (55,9%), OSB (22,6%) en OSC (19,8%). 1,7% vulde een andere functie in, zoals teamchef. Meer dan de helft is al meer dan 10 jaar in de opsporing werkzaam (58,8%). Zoals te verwachten is het merendeel van de respondenten belast met tactisch onderzoek (62,7%). De overige respondenten gaven aan primair belast te zijn met digitaal onderzoek (14,7%), financieel onderzoek (13,6%) of met een ander takenpakket (8,5%), bijvoorbeeld intelligence. Geen van de respondenten deed technisch onderzoek en een zeer klein deel forensisch onderzoek (0,6%). Iets meer dan de helft van de respondenten heeft (heel) veel affiniteit met digitalisering in politiewerk (53,7%) en een derde niet veel, maar ook niet weinig affiniteit (37,3%). Tot slot geeft 57,1% van de respondenten aan geen opleiding op dat gebied te hebben gevolgd.

Voor de analyses hebben we gebruik gemaakt van SPSS (versie 27). Naast de gebruikelijke analyses hebben we gekeken of er samenhang of juist verschillen waren in uitkomsten op het gebied van achtergrondkenmerken van respondenten, type criminaliteit en type encryptie. Hiervoor hebben we ANOVA's gedraaid en correlaties berekend. Daarnaast hebben we aanvullende analyses gedraaid om de samenhang tussen variabelen te bekijken, bijvoorbeeld tussen het type delict en de gebruikte toepassingen, medewerking van verdachte en de duiding van de rol van encryptie. Wanneer het een relatie tussen een dichotome en continue variabelen betreft zijn Spearman correlaties gerapporteerd.

2.4 Diepte-interviews

De diepte-interviews kenden twee doelen. Allereerst wilden we kijken of de ertoe doende elementen verder uitgediept en verklaard konden worden. Ten tweede wilden we ingaan op de tussentijdse resultaten en voorlopige conclusies. Naast medewerkers binnen de opsporing en relevante landelijke coördinatoren en portefeuillehouders binnen de politie, wilden we ook met experts van het OM en Rechterlijke Macht (RM) spreken. De toevoegde waarde van het OM is reeds besproken, namelijk dat zij leiding geeft aan het opsporingsonderzoek. De RM beoordeelt ter zitting onder meer of het onderzoek rechtmatig is uitgevoerd en leek ons om die reden ook een waardevolle actor voor de verdiepende interviewfase.

Voor alle drie de doelgroepen is een interviewprotocol ontwikkeld. Dit betreft een adaptatie van het interviewprotocol uit de oriënterende fase. Op hoofdlijnen waren de protocollen hetzelfde,

[14] We hadden het responspercentage op voorhand willen vergroten door de portefeuillehouder Specialistische Opsporing de uitnodiging naar de vragenlijst te laten ondertekenen, alsook een bericht over het onderzoek en de vragenlijst te communiceren via de website en/of het intranet van de politie. Hiervoor kregen de onderzoekers geen toestemming.

maar ze weken voor de doelgroep relevante context op enkele punten van elkaar af. De interviewprocedure is gelijk aan die van de oriënterende fase (par. 2.2). Dit betreft de punten over vrijwilligheid, anonimiteit, doel van het onderzoek, informed consent, verzoek om opname voor uitwerkingsdoeleinden en controle van het interviewverslag. Gezien het overeenstemmende karakter zijn de betreffende protocollen niet in dit rapport bijgevoegd. Deze zijn op te vragen bij de auteurs. Daar waar de verdere procedures afwijken wordt hieronder verslag gedaan.

Om met experts binnen de RM te spreken, hebben de onderzoekers toestemming gevraagd bij de Raad voor de rechtspraak (Rvdr). Op 28 februari 2022 heeft het Landelijk Overleg Vakinhoud Strafrecht (LOVS) besloten om onder voorwaarden medewerking aan het onderzoek te verlenen. Medewerking houdt hier in dat maximaal vijf interviews afgenomen mogen worden van maximaal anderhalf uur. In totaal zijn vijf interviews afgenomen; drie rechter-commissarissen, een senior rechter en een strafrechter. Alle geïnterviewden hebben affiniteit/ervaring in strafzaken waarin encryptie voorkomt. De interviews vonden plaats tussen 5 september en 25 oktober 2022. Bij het vijfde interview leek al enige saturatie op te treden, omdat dezelfde onderwerpen werden aangehaald die ook in de eerdere interviews naar voren kwamen. Van deze interviews zijn vier fysiek en één via Microsoft Teams afgenomen. De interviews duurden gemiddeld een uur en tien minuten.

Naast experts van de RM wilden we ook met experts spreken die werkzaam zijn bij het OM. Via het eigen netwerk zijn vier personen benaderd. Drie van hen wilden meewerken. Van één kregen we geen reactie. Voordat een interviewafspraak gepland kon worden heeft de betreffende interviewkandidaat als eerste stap toestemming gevraagd om mee te werken aan een interview aan de hoofdofficier van het parket waar de te interviewen officier werkzaam is. Werkafspraken tussen het WODC en het Parket-Generaal omtrent het interviewen van officieren van justitie stellen dat deze toestemming gevraagd moet worden. De drie geïnterviewden – die allen werkzaam zijn als landelijk OvJ – hebben schriftelijk via e-mail laten weten deze toestemming te hebben gekregen. De interviews zijn online afgenomen via Microsoft Teams tussen 14 november en 2 december 2022 en duurden gemiddeld een uur en tien minuten.

Om mensen binnen de politie te spreken aangaande dit onderwerp waren we, net zoals voor de oriënterende interviews, afhankelijk van Onderzoekscoördinatie van de politie. Het verzoek om interviewkandidaten te mogen benaderen is in september 2022 gedaan. Initieel wilden we naast relevante landelijke coördinatoren en portefeuillehouders binnen de politie spreken met politiemensen die vanuit de opsporing kennis en ervaring hebben met de onderscheiden hoofdvormen van encryptie in dit onderzoek. Het bleek voor Onderzoekscoördinatie niet mogelijk om op een dergelijk detailniveau politiemensen te benaderen. Daarop hebben we het verzoek aangepast naar teamchefs op DR-niveau. Ondanks herhaaldelijke pogingen, hebben de onderzoekers op dit verzoek geen medewerking verkregen. In overleg met de opdrachtgever is medio december deze beoogde onderzoeksactiviteit gestaakt. We staan in par. 5.2 nader stil bij de mogelijke consequenties hiervan.

2.5 Analyse politiesystemen

Om cijfermatige informatie over encryptie in opsporingsonderzoeken voor de Nederlandse context te achterhalen, wilden we data uit verschillende politiesystemen gebruiken. Waarom is dit belangrijk? De veronderstelling kan zijn dat voor kinderpornozaken, georganiseerde criminaliteit en sommige cybercrimes digitale opsporingsinformatie mogelijk van groter belang is dan bij huiselijk geweld of inbraken. Maar het is niet enkel het type zaak dat telt. Frequentie doet er ook toe als we iets willen

zeggen over de rol van encryptie. Hinder door encryptie bij een drugszaak die de politie op eigen initiatief start, weegt mogelijk zwaarder dan hinder bij een online oplichting. Maar wat als de politie alle aangiften van online oplichting steevast 'uitscreent' vanwege verwachte encryptie-hinder? Vele malen een minder ernstige impact maakt samen immers ook een ernstige impact. Om dergelijke zaken niet op voorhand uit te sluiten, wilden we nader onderzoek doen binnen de systemen van de politie.

Navraag bij politiemensen uit ons netwerk (o.a. een data-analist en een bedrijfsvoerings-specialist) leerde ons dat de we de aard en omvang van encryptie in opsporingsonderzoeken welhaast onmogelijk op een deugdelijke manier op basis van data uit politiesystemen kunnen bepalen. De uitkomsten zullen te veel onzekerheden bevatten; vals positieven (omdat bijv. wel het woord encryptie voorkomt, maar het in de opsporing geen rol speelde) en vooral vals negatieven (omdat encryptie wel een rol speelde, maar niet met name is genoemd). Daarnaast hebben we te maken met een groot dark number en mogelijke doublures. De inspanning om de onzekerheden eruit te halen zou te tijdrovend worden. Het zou namelijk veel omslachtige, handmatige controles vergen. 'Omslachtig' onder meer omdat de benodigde informatie is opgeslagen in diverse documenten die aan opsporingsdossiers zijn gekoppeld. 'Handmatig', omdat dit de eerste keer is dat een dergelijke analyse zou worden gedaan en er dus geen referentie bestaat voor wat betreft de foutmarge.

Dan speelt nog de doorlooptijd om de juiste toestemming te verkrijgen om deze documenten in te mogen zien, en is ondanks een inzage-toestemming de medewerking van de politie om de documenten daadwerkelijk in te zien niet gegarandeerd. Hoewel we op basis van deze beperkingen geen absolute aantallen wilden presenteren, leek deze exercitie nog steeds nuttig, namelijk om te onderzoeken bij welk type zaken encryptie vooral voorkomt en om te onderzoeken of we trends in de tijd konden ontdekken (afgelopen vijf jaar). Bij dergelijke analyses speelt het bezwaar van vals positieven en negatieven minder zwaar; er van uit gaande dat de 'afwijkingen' zich bij alle type zaken en in alle jaren in soortgelijke mate voordoen.

Het primaire politiesysteem dat we wilden inzetten is Blueview; een verzamelpunt van informatie uit de 'handhavingssystemen' van de politie. Met Blueview kan dus in andere politiesystemen van de politie worden gezocht, zoals Summ-IT; een politieregistratiesysteem van de Nederlandse politie dat inzicht geeft in opsporingsinformatie. Door gebruik te maken van het zoeksysteem met bijvoorbeeld de sleutelwoorden 'encrypt*' of 'versleutel*' kan naar voren worden gehaald in hoeveel zaken encryptie dan wel versleuteling is vermeld. Hoewel deze methode geen sluitende antwoorden geeft, wilden we het gebruiken als een hulpmiddel bij het maken van nadere afbakeningen in het onderzoek.

Uiteindelijk is van deze methode afgezien, omdat nadere analyse van Blueview-data uitwees dat het aantal vals positieven en negatieven veel groter was dan verwacht. Daarnaast betreft het merendeel van de hits Summ-IT. Summ-IT kan niet dieper geraadpleegd worden zonder een bepaald autorisatieniveau. Mogelijk kan in vervolgonderzoek gezocht worden met aanvullende, specifiekere sleutelwoorden of met andere technieken, zoals 'machine learning', waarbij dan de complete tekst van de dossiers onderzocht moet worden. Daarbij moet worden gezegd dat geavanceerde technieken de grote ruis in de registraties niet oplossen.

3. Theoretische verkenning

Dit onderzoek is afgebakend tot opsporingswerk in de strafrechtketen. We gaan expliciet niet in op het maatschappelijk debat over de balans tussen enerzijds beveiliging die encryptie de gebruiker biedt en anderzijds de betekenis van encryptie voor de opsporing.[15] Dit betekent dat we voor dit onderzoek niet een bredere maatschappelijke theorie gebruiken, zoals 'politie als sociale controle' (Cachet, 1990). Als theoretisch raamwerk gebruiken we het in eerder verricht onderzoek ontwikkelde 'politiewerk in informatieperspectief' (Stol, 1996, 2014; Stol e.a., 2005), zie par. 3.1. Na een beschrijving van dit raamwerk staan we nader stil bij cryptografie en encryptie (par. 3.2). Daarna gaan we dieper in op de bestaande kennis over de rol van encryptie in de opsporing (par. 3.3).

3.1 Politiewerk in informatieperspectief

Politiewerk is te zien als informatiewerk. Met opsporingsonderzoek moet de politie uiteindelijk antwoord geven op de vraag wie wanneer, waar, wat gedaan heeft, en waarom. Het gaat uiteindelijk om informatie over *personen* want ons strafrecht is gebaseerd op individuele daden en verantwoordelijkheden. Naast personen zijn er nog twee andere basale informatiedragers: goederen (waaronder geld en voertuigen) en locaties, beide in de breedste zin van het woord, dus ook digitaal.[16] Verder gaat het in politiewerk niet alleen om informatie over deze drie informatiedragers maar ook om informatie over *relaties* tussen de informatiedragers, dus relaties tussen mensen, goederen en locaties. Het kan gaan om een relatie tussen een locatie (bijv. pand en webadres) en een persoon of tussen een goed (bijv. auto en bitcoin) en een persoon, of tussen personen onderling. Belangrijk zijn ook de unieke *aanknopingspunten* die dienen om informatie te koppelen aan een bepaalde persoon, goed of locatie. Aanknopingspunten voor informatie zijn bijvoorbeeld naam, serienummer en webadres. Het gaat immers om informatie over één specifieke informatiedrager want opsporingsinformatie is nu eenmaal precieze informatie.

In deze benadering gaat het 'spel' tussen criminelen en de opsporing om het ontsluiten van bepaalde informatie en, belangrijker nog, het verbinden van die informatie aan een persoon, goed of locatie. Elke verbinding die de opsporing legt, is dan het leggen van een stukje van de puzzel, op weg naar voldoende overtuigend bewijs dat is gekoppeld aan een persoon, én de arrestatie van die persoon.[17] Afgezien van een veroordeling bij verstek, is voor een berechting nodig dat de overheid het lichaam van de persoon in handen heeft plus de informatie over wat die persoon wanneer en waar heeft gedaan. Voor het daadwerkelijk uitvoeren van het vonnis is hoe dan ook het lichaam van de veroordeelde vereist. Het is de Franse filosoof Michel Foucault (1975) geweest die het belang van controle over het lichaam heeft benadrukt en het koppelen van informatie daaraan. Gezien in informatieperspectief leggen criminelen zich toe op (i) het verhullen van aanknopingspunten voor informatie (bijv. verhullen van namen en adressen), zodat geen informatie aan een persoon, goed of locatie kan worden verbonden, (ii) het onherkenbaar maken of verbergen van informatie zodat er niets is om aan een persoon, goed of locatie te verbinden en (iii) het verhullen van de locaties van mensen

[15] Voor die discussie, zie bijvoorbeeld www.bitsoffreedom.nl/2021/04/09/vijf-dingen-die-belangrijk-zijn-in-onderzoek-naar-effect-encryptie-op-opsporing/

[16] In hun overzicht van gevonden sporensoorten noemen Stol e.a. (2005) enkel sporen die verband houden met personen en goederen. Maar opsporing in informatieperspectief draait niet enkel om sporen maar om informatie die nodig is om te kunnen vervolgen. Locaties spelen dan een rol omdat inbeslagname en aanhouding een locatie vereisen.

[17] Bewijs is behalve voor schuld ook van belang voor onschuld.

en goederen, zodat de opsporing die mensen en goederen niet feitelijk in haar macht kan krijgen via inbeslagname of aanhouding.

Het zijn oude principes (zie Foucault), en dus niet gebonden aan digitalisering, maar ze zijn nog wel steeds van kracht in een digitale samenleving. De invalshoek van 'politiewerk in informatieperspectief' helpt te zien en te ordenen hoe encryptie ingrijpt op de opsporing. Emmen e.a. (te verwachten) bespreken bijvoorbeeld politiewerk op het Tor-netwerk[18] (een digitaal versleutelde omgeving) en schrijven: "If users use the options correctly and do not reveal their true identity, the police have no point of departure for further investigation: not a body to arrest, no location to go to and no identified person to search for. This is the core challenge ACNs [Anonymous Communication Networks] like Tor confront the police with: absent and anonymous suspects whose locations and identities are effectively hidden behind encryption." Ook in het opsporingswerk in deze encrypte omgeving, gaat het om informatie over personen, locaties (online en offline) en goederen (bijv. pakketjes en bitcoins).

We spreken hierboven over informatie, maar niet alle informatie is relevant. Het gaat in de opsporing uiteindelijk om informatie die bijdraagt aan duidelijkheid over of iemand een strafbaar feit wel of juist niet heeft gepleegd. Informatie die daaraan kan bijdragen is relevant. In relatie tot encryptie gaat het dan om digitaal opgeslagen informatie (bijv. opgeslagen afbeeldingen van seksueel kindermisbruik) en om digitaal stromende informatie (bijv. een lopende conversatie). Onderschepte digitale informatie kan belangrijk bewijsmateriaal opleveren (Oerlemans, 2012, 2017). Het moet wel gekoppeld kunnen worden aan een persoon, locatie of een goed, om een bijdrage te kunnen leveren aan de bewijsvoering. Tijdigheid speelt daarbij een rol. Wanneer de politie 'realtime' ingrijpt, bijvoorbeeld via het aftappen van communicatie, kan zij meteen actie ondernemen met een arrestatie of heterdaadsituatie (Odinot e.a., 2012). Hoe lastiger de encryptie is te decoderen of te omzeilen, hoe groter de rol is die encryptie speelt in de opsporing (Oerlemans, 2012). Wanneer de politie door de vertraging een heterdaadmoment mist, kan dit doorwerken op de strafrechtelijke vervolging en afdoening van de zaak.

We gebruiken bovengenoemd perspectief als raamwerk of lens voor het bestuderen van de rol van encryptie in de opsporing. Het helpt de aandacht te richten op de diverse manieren waarop encryptie kan worden gebruikt en de rollen die het kan spelen. Daarbij hebben we oog voor zowel een negatieve rol (belemmering) als positieve rol (mogelijkheden). Bij dat laatste denken we bijvoorbeeld aan de vele informatie over personen, locaties en goederen die op versleutelde devices van verdachten aanwezig is en na ontsleuteling is in te zien. Ook kan encryptie betekenen dat de politie een verscheidenheid aan werkwijzen ontwikkelt om informatie te achterhalen en te koppelen aan een persoon, locatie of goed – wat haar handelend vermogen ten goede komt. Het onderzoek zal op haar beurt helpen om het raamwerk van 'politiewerk in informatieperspectief' verder te ontwikkelen. Wat encryptie omvat staat beschreven in de volgende paragraaf.

[18] Tor staat voor The Onion Router. Tor biedt een methode om anoniemer op het internet te surfen en geeft ook toegang tot het dark web. Het dark web is "een besloten deel van het internet dat men niet vindt met normale browsers en zoekmachines. Het staat vooral bekend als een plek waar criminelen hun zaken doen" (Cybersecurity Alliantie & Cyberveilig Nederland, 2021, p.28).

3.2 Encryptie nader toegelicht

Om de hoofdvraag 'wat is de rol van encryptie in opsporingsonderzoeken van de politie' te beantwoorden is het belangrijk om eerst het onderwerp nader toe te lichten. Cryptologie heeft twee deelgebieden: cryptografie en cryptanalyse. Beiden hebben een sterk (wiskundig-)theoretische achtergrond. Cryptografie, de wetenschap van het verbergen en authentiseren van berichten, houdt zich bezig met het maken van nieuwe algoritmen. Cryptanalyse, daarentegen, houdt zich bezig met het kraken van bestaande cryptografische algoritmen en hun implementaties. Hoewel cryptologie een theoretische wetenschap is, wordt deze tegenwoordig veel gebruikt in de praktijk. Het kraken van cryptografische algoritmen is vrijwel onmogelijk in de praktijk. Cryptanalyse en het verkrijgen van de beveiligde data is wel denkbaar. Immers, het toepassen van de cryptografische algoritmen is vaak onvolledig, waardoor de sleutel of de originele data bemachtigd kunnen worden.

Encryptie, waarop we ons in dit rapport richten, is het proces waarin data worden omgezet in beveiligde data, om het te beschermen tegen ongeautoriseerde toegang of wijzigingen van andere partijen, om de vertrouwelijkheid en integriteit van informatie te waarborgen (Kerr & Schneider, 2017; Europol & Eurojust Public Information, 2019). Tegenwoordig wordt encryptie veelal gebruikt om digitale data te beschermen. Encryptie wordt echter al veel langer toegepast. Sinds 100 voor Christus wordt encryptie gebruikt in het Romeinse Rijk. Julius Caesar stuurde door middel van geheimschrift op een veilige manier zijn berichten. Hiervoor gebruikte hij een simpele vervanging van letters, waarin bijvoorbeeld de letters in het alfabet een vast aantal letters naar achteren schuiven. Deze vorm van encryptie is tegenwoordig bekend als Caesarcijfer. Ter illustratie, de a wordt een x, de b een y, de c een z, et cetera. Dit soort encryptie is niet meer in gebruik omdat het makkelijk te kraken is met moderne computers.

In de twintigste eeuw (1933-1945) gebruikte het Duitse leger de Enigma machine om versleutelde berichten te sturen. Deze berichten werden verstuurd met een encryptiesleutel die dagelijks veranderde. Het kraken van de Enigmacode door Alan Turing was voor de geallieerden een belangrijk moment in de overwinning van de Tweede Wereldoorlog. Bovendien is het kraken van de Enigma machine één van de meest significante ontwikkelingen in de geschiedenis van encryptie.

In de jaren '70, na de opkomst van commercieel computergebruik, heeft IBM een 'cryptogroep' opgezet om een cijferschrift/versleuteling te ontwerpen ter bescherming van data van klanten. Dit ontwerp is gecreëerd samen met de NSA van de VS. In 1976 is Data Encryption Standard (DES) als encryptiestandaard gekozen. DES was een wereldwijde standaard voor encryptie, totdat het in 1999 publiekelijk werd gekraakt (door distrubted.net en de Electronic Frontier Foundation). Vervolgens heeft het Amerikaanse National Institute of Standards and Technology (NIST) de encryptiestandaard DES ingetrokken en een nieuwe codering van encryptie ontworpen. De opvolger van DES is Advanced Encryption Standard (AES), de eerste cryptografische standaard die door een open wetenschappelijke wedstrijd (in 2001) werd gekozen. Tegenwoordig is AES een wereldwijde standaard voor de encryptie van digitale data.

Zowel het Caesarcijfer als DES en AES maken gebruik van dezelfde sleutel aan beide kanten van de communicatie: de verzender en de ontvanger moeten de sleutel van tevoren kiezen die ze tijdens de beveiligde communicatie gebruiken. Aangezien dezelfde sleutel aan beide kanten wordt gebruikt wordt dit *symmetrische* versleuteling genoemd. In het Caesarcijfer is deze sleutel de informatie over hoe de letters worden vervangen. Bij DES en AES is de sleutel een bit-string van lengte 56 bits en respectievelijk 128/192/256 bits (AES kent meerdere varianten voor verschillende

beveiligingsniveaus). Met gebruik van deze sleutel kunnen de partijen versleutelde berichten met elkaar uitwisselen (zolang de sleutel niet gekraakt wordt door een derde partij).

Om een sleutel aan te maken wordt tegenwoordig vaak een ander type encryptie gebruikt dat ook in de jaren '70 is ontwikkeld. Met *asymmetrische* cryptografie (oftewel publieke-sleutelcryptografie) is het mogelijk om een sleutel aan te maken zonder elkaar te zien. In deze digitale technologie heeft iedere partij twee aparte sleutels: een publieke sleutel en een privésleutel. De publieke sleutel, net als een telefoonnummer, hoort tot één partij en is openbaar. Deze sleutel wordt gebruikt om mee te versleutelen. Iedereen kan dus een geencrypt bericht naar deze partij sturen. De privésleutel is daarentegen alleen bij deze partij bekend. Deze partij is dus de enige die versleutelde berichten kan ontsleutelen.

Met asymmetrische cryptografie kunnen partijen een nieuwe AES-sleutel voortbrengen op meerdere manieren. Een methode is om een bit-string van 128 willekeurige bits door een partij te laten kiezen en deze met de publieke sleutel van de andere partij te versleutelen. Deze beveiligde sleutel kan daarna naar de andere partij gestuurd worden. Let daar in dit geval op dat de sleutel door een van beide partijen wordt gekozen. Een andere methode in publieke-sleutelcryptografie is sleuteluitwisseling waarbij de partijen samen een geheime encryptiesleutel kunnen creëren over een onbeveiligd netwerk (bijv. het internet). Beide methodes worden tegenwoordig gebruikt op het internet: RSA (Rivest-Shamir-Adleman) voor de versleuteling en DH (Diffie-Hellman) voor de sleuteluitwisseling.

Kortom, de cryptografische algoritmen worden onderscheiden in symmetrische en asymmetrische coderingen, die in de praktijk beide worden gebruikt (Europol & Eurojust Public Information, 2019). Veel principes van oude systemen zoals de Caesarcode zijn terug te vinden in moderne vormen van encryptie. In essentie is het verschil is dat er een veel ingewikkelder stappenplan wordt gebruikt in moderne encryptie om de data te versleutelen (Sharma e.a., 2022).

3.2.1 Encryptie en hashfuncties in de praktijk

Zoals in de vorige paragraaf beschreven, wordt asymmetrische cryptografie vooral gebruikt om een nieuwe sleutel aan te maken. We kunnen ons afvragen waarom symmetrische cryptografie sowieso nodig is en waarom niet alleen publieke-sleutelcryptografie wordt gebruikt. Het antwoord is eenvoudig. Publieke-encryptietechnieken zijn veel minder efficiënt: de cijfertekst[19] is langer en het encryptieproces is trager. Daarom wordt een combinatie van de twee aanpakken gebruikt. Deze combinatie is in staat om de voordelen van symmetrische (snel en doelgericht) én asymmetrische (betere sleutelverdeling en minder vertrouwen onder de partijen nodig) codering te verenigen. In het bijzonder, in een communicatiesessie wordt in de praktijk eerst een sessiesleutel gemaakt door middel van asymmetrische cryptografie waardoor het niet nodig is dat de partijen van tevoren de sleutels hoeven te weten. De net gemaakte sleutel wordt dan gebruikt voor de symmetrische encryptie van het informatieverkeer binnen de gegeven sessie. Kortom, de meeste cryptografische protocollen maken in de praktijk gebruik van beide coderingen.

[19] Terminologie. Klare tekst: *plaintext* in het Engels. Dit is een niet-versleuteld bericht. Cijfertekst: *ciphertext* in het Engels. Dit is een versleuteld bericht. Zonder een cryptografische sleutel is het meestal niet mogelijk om welke informatie dan ook over de klare tekst te krijgen. Sleutel: *key* in het Engels. Een sleutel is een bit-string, bijvoorbeeld een AES-sleutel van 128 bits of een RSA-sleutel van 4096 bits.

Bij de toepassing van versleuteling moet, naast de hiervoor beschreven aspecten van encryptie, ook de sleutellengte vermeld worden. Transport Layer Security (TLS), een van de meest gebruikte cryptografische protocollen, kan met verschillende sleutellengtes gebruikt worden. Een bekende aanval op een vroegere versie van TLS is om de server te dwingen een kortere sleutellengte (bijv. 1024 bits in plaats van 2048 bits) te gebruiken.

Cryptografische hashfuncties gebruiken geen sleutels om data te versleutelen. Hashfuncties passen een algoritme toe op de data om een hashcode te creëren. Een hashcode kan als een digitale vingerafdruk gezien worden. Tevens heeft een hashcode een vaste lengte. Ter illustratie, het woord 'koffie' heeft net zo'n lange hashcode als de complete tekst van een toneelstuk van Shakespeare. Aangezien een hashcode kan worden aangepast zonder een sleutel, is een aanvullend mechanisme nodig om de data te beveiligen. Als deze met het bovengenoemde mechanisme samen wordt gebruikt, garandeert de hashcode de authenticiteit van de data. Op deze wijze kan verzekerd worden dat de data niet zijn gewijzigd door bijvoorbeeld malware. Cryptografische hashfuncties kunnen over het algemeen niet worden omgezet in de originele tekst (klare tekst). De meest gebruikt cryptografische hashfuncties zijn MD5, SHA-1, SHA-2 en SHA-3; in de praktijk worden tegenwoordig de laatste twee aanbevolen.

3.2.2 Vormen van encryptie

In de eenentwintigste eeuw heeft bijna iedereen in de westerse wereld een persoonlijk digitaal apparaat in de vorm van een telefoon, computer of anderszins. Deze digitale apparaten worden onder meer gebruikt om foto's en video's te maken en op te slaan, te communiceren met anderen en locaties op te zoeken via GPS. De meeste data en informatie die worden verstuurd, ontvangen en opgeslagen op onze digitale apparaten, zijn versleuteld. Deze versleutelde informatie kan worden gecategoriseerd als 'in motion' of 'at rest', waarbij beide unieke implicaties hebben voor opsporingsinstanties (Manpearl, 2017).

Bij data of berichten *in motion* wordt gecommuniceerd tussen de zender en bedoelde ontvanger. Met end-to-end encryptie (E2EE) (zie hieronder) hebben alleen de verzender en ontvanger een sleutel om het bericht te ontsleutelen. Data of berichten in motion kunnen telefoongesprekken, chatberichten, social mediaberichten en e-mails zijn. Deze kunnen worden onderschept met een (internet)tap. Data of informatie *at rest* zijn opgeslagen op een digitaal apparaat. De encryptie van dergelijke data en informatie wordt endpoint encryptie genoemd. Voorbeelden hiervan zijn opgeslagen e-mails, berichten, kalenders, contacten, foto's en video's. De meeste persoonlijke digitale apparaten van technologiegiganten, zoals Apple en Google, bieden opties om data van gebruikers op een versleutelde manier op te slaan.

E2EE is een veilig communicatiekanaal waar alleen de ontvanger de data kan lezen (Europol & Eurojust Public Information, 2019). In het bijzonder kan de serviceprovider ook de data niet lezen. Bij een berichtendienst wordt een tekst versleuteld verstuurd. Afhankelijk van de applicatie, zal het bericht bij de cloud aankomen waar de versleutelde informatie opgeslagen wordt totdat de ontvanger beschikbaar is. Als de informatie is ontvangen op het apparaat van de ontvanger, dan wordt het pas leesbaar met de juiste sleutel. De dienstaanbieder heeft dus zelf geen toegang tot de versleutelde informatie. Een veel gebruikte vorm van E2EE is Pretty Good Privacy (PGP). Deze toepassing wordt onder andere door journalisten gebruikt om op veilige manier te communiceren (Hartel & Van Wegberg, 2021). Door E2EE versleuteling van reguliere chat-apps zoals WhatsApp, Signal of Telegram

is het onderscheppen van communicatie moeilijk. Opsporingsinstanties moeten zich wenden tot alternatieven zoals het actief inbreken op iemands telefoon. Dit kost meer tijd en geld dan het onderscheppen van berichten, zoals mogelijk was vóór encryptie.

E2EE die zich vooral richt op twee of meer partijen met elkaar vertrouwelijk te laten communiceren, is een belangrijk voorbeeld voor 'user-controlled' encryptie. Deze maakt het mogelijk voor gebruikers om ultieme controle te hebben over de encryptie en decryptie van hun data (Europol & Eurojust Public Information, 2020b) zowel in communicatie als voor opslag. De serviceprovider heeft namelijk geen sleutel, en daarmee geen toegang tot de gebruikersdata. Het is waarschijnlijk dat met name diensten en applicaties waarbij data in motion zijn, geneigd zijn om gebruik te maken van deze encryptievorm. Voor directe berichtendiensten (bijv. WhatsApp), waar E2EE wordt gebruikt, of audiocommunicatie is dataherstel namelijk niet zo belangrijk. Voor diensten zoals e-mail, zakelijke berichtendiensten, kalenders en samenwerkingsprogramma's is dataherstel belangrijker. Daarom is het aannemelijk dat deze diensten niet snel gebruik zullen maken van user-controlled encryptie. Net als met E2EE, maakt deze vorm van encryptie het opsporingsinstanties in theorie lastiger om bewijs te verzamelen voor opsporingsonderzoeken. Serviceproviders kunnen met deze encryptie namelijk moeilijk of niet voldoen aan rechtshulpverzoeken.

Wanneer we proberen om de vormen van encryptie explicieter te maken, helpt het om te kijken naar onderscheid in de toepassing ervan. Voor dit onderzoek delen we encryptie op in vier type toepassingen, namelijk: (i) het versleutelen van communicatie, (ii) het versleutelen van apparaten en data, (iii) versleutelde onlinediensten en (iv) tools voor het verhullen van digitale locaties.

Versleutelen van communicatie. Voorbeelden die van toepassing zijn voor het versleutelen van communicatie betreffen cryptotelefoons en E2EE van diensten zoals WhatsApp, Telegram en ProtonMail. Cryptotelefoons zijn versleutelde mobiele telefoons met een garantie voor anonimiteit; ook wel PGP-telefoons genoemd. Voorbeelden van cryptotelefoons zijn Phantom Secure, IronChat, Ennetcom, EncroChat en Sky ECC. Op deze telefoons zijn de hardware en software die verantwoordelijk zijn voor externe communicatie, waaronder microfoon, GPS-navigatie, camera, internettoegang en berichtapplicaties verwijderd. Deze zijn meestal vervangen door VPN's en andere encryptiemethoden.[20] Tevens wordt veelal een optie aangeboden om eenvoudig alle data van de telefoon te verwijderen. Voor de encryptie van berichten, video- en audiogesprekken bij WhatsApp, Facebook Messenger en Signal wordt het Signal Protocol gebruikt. Dit protocol wordt getypeerd als één van de meest veilige cryptografieën. Mailprogramma's bieden meerdere lagen van encryptie. De meest gebruikte e-mail encryptiestandaard wereldwijd is OpenPGP. De bekendste versleutelde e-mailservice is ProtonMail met een miljoen gebruikers. Deze aanbieder gebruikt E2EE en slaat versleutelde informatie op in een eigen fysieke server in plaats van bij een van de clouddienstverleners. Om de veiligheid te garanderen, worden verschillende encryptiemethoden gecombineerd, zoals AES, RSA en OpenPGP.

Versleutelen van apparaten en data. In deze categorie spelen versleutelde smartphones, harde schijven en cryptocontainers een rol. Hoewel dit vanuit technisch perspectief geen encryptie betreft, spelen versleutelde mobiele telefoons (bijv. met pincode, gezichtsherkenning, vingerafdruk) een rol.

[20] VPN staat voor Virtual Private Network. Dit is een "uitbreiding van een computernetwerk over een openbaar netwerk. Via die uitbreiding kunnen gebruikers vanaf elke plek veilig gegevens delen met het computernetwerk. Voor de gebruikers is het alsof ze rechtstreeks op het netwerk zijn aangesloten. De veilige verbinding valt te omschrijven als een tunnel" (Cybersecurity Alliantie & Cyberveilig Nederland, 2021, p.76).

Dit geldt ook voor andere devices dan mobiele telefoons, zoals laptops en desktop computers. Op het gebied van encryptie spelen verder versleutelde gegevensdragers (bijv. usb-sticks en harde schijven) en cryptocontainers (versleutelde data, bijv. met VeraCrypt of BitLocker) een rol.

Versleutelde online diensten. Bij online diensten spreken we bijvoorbeeld over wachtwoord-beveiliging op social media accounts. Daarnaast spelen versleutelde cloudopslag en 'bulletproof hosting' een rol. "Een bulletproof hosting service is een dienst van een bedrijf die serverruimte verhuurt aan cliënten, waarbij hun klanten bewust de ruimte en mogelijkheden krijgen alle typen inhoud – ook illegale inhoud – aan te bieden. De naam refereert naar de 'bescherming' die diensten bieden tegen opsporingsdiensten en andere partijen de materiaal offline willen halen" (Oerlemans, 2019). Er zijn dertig à veertig vermoedelijke bulletproof hosts actief in Nederland.[21] Hier wordt op grote schaal gebruik van gemaakt door onder andere Russische en Oost-Europese criminele groepen.

Tools voor het verhullen van digitale locaties. Om anonimiteit bij online activiteiten te vergroten worden anonimiserende applicaties aangeboden. Gebruikers kunnen daarmee het web doorzoeken zonder hun identiteit of locatie te onthullen. Via een VPN kunnen een of meerdere apparaten, zoals servers en computers, via het internet verbinden met een privénetwerk. Binnen dit netwerk kunnen data verstuurd worden zonder dat deze informatie onderschept of achterhaald kan worden. Het zogenoemde dark web (ook wel darknet genoemd) is een besloten deel van het internet dat niet via traditionele servers en zoekmachines bereikbaar is. Alle communicatie op dit deel van het internet is versleuteld. Om anoniem op het dark web te komen is een speciale browser nodig, zoals Tor. Deze tools verhullen IP-adressen op verschillende manieren, maar waarborgen de anonimiteit van gebruikers overigens niet per se. Immers, wie op een 'dark market' zijn echte naam gebruikt, geeft aan alle bezoekers, waar onder mogelijk politiemensen, zijn identiteit prijs.

3.3 Eerder onderzoek naar de rol van encryptie in de opsporing

Voordat we ingaan op de rol van encryptie, staan we kort stil bij de opsporing; de context waarop de onderzoeksvragen van toepassing zijn. Jansen e.a. (2020) geven een theoretische beschrijving van het opsporingsproces. Dit bestaat uit de volgende zes fasen (p. 82): "(1) kennis nemen van een misdrijf (via melding, aangifte of politiestraatwerk), (2) initieel onderzoek (informatie veiligstellen), (3) evaluatie opsporingsonderzoek (beslissen om wel of niet over te gaan tot opsporingsonderzoek), (4) waarheidsvinding (identificeren van verdachten en vergaren van zowel belastend als ontlastend materiaal), (5) evaluatie bewijs (beslissen om opsporingsonderzoek [vroegtijdig] te beëindigen of aanvullend onderzoek te verrichten), en (6) afronding onderzoek (strafrechtelijk dossier opmaken en overdragen aan het Openbaar Ministerie)."

Hoe invulling wordt gegeven aan deze fasen hangt onder andere af van het type criminaliteit. De politie onderscheidt drie typen criminaliteit: veel voorkomende criminaliteit (VVC), high impact crime (HIC) en ondermijning. VVC omvat eenvoudige criminaliteitsvormen zoals vernieling, bedreiging en winkeldiefstal. HIC omvat criminaliteit met een grote impact op het slachtoffer en/of de maatschappij, zoals overvallen, woninginbraak en geweldsdelicten. Ondermijning is een verzamelnaam voor delicten die de integriteit c.q. het functioneren van de rechtstaat bedreigen. Dit

[21] Politie (2022). *Waarschuwingslijst*. Verkregen via: https://content.app-us1.com/egmj6/2022/10/14/a844663a-56c5-4d21-a4cc-6022a3eb19f0.pdf?utm_source=ActiveCampaign&utm_medium=email&utm_content=CORRECTIE%3A+Brief+en+waarschuwingslijst+van+Landelijke+Politie&utm_campaign=20221014+-+Politie+-+Brief+en+waarschuwingslijst+landelijke+politie

zijn delicten die bijvoorbeeld in georganiseerd verband worden uitgevoerd, zoals drugshandel, afpersing en corruptie.

Er zijn geen officiële statistieken bekend van de hoeveelheid opsporingsonderzoeken met digitale bewijsmiddelen of onderzoeken die ontsleuteling van data vereisen. Desondanks merken opsporingsinstanties op dat beide soorten opsporingsonderzoeken toenemen (Europol & Eurojust Public Information, 2019). In 2016 heeft de Raad van de Europese Unie, zoals eerder in dit rapport beschreven, een enquête uitgezet onder de lidstaten. Uit de resultaten blijkt dat in de meerderheid van de lidstaten (twintig) encryptie vaak tot bijna altijd wordt aangetroffen in criminele onderzoeken. Vijf lidstaten geven aan soms encryptie aan te treffen. Het gaat hierbij zowel om encryptie in motion (bijv. versleutelde e-mails en berichten via communicatiediensten, zoals Facebook, Skype, WhatsApp en Telegram) als om encryptie at rest (bijv. versleutelde digitale apparaten en applicaties).

De twee soorten opsporingsonderzoeken, zoals hierboven beschreven, voeren terug naar begin jaren ’90 van de vorige eeuw. Henseler (2017) beschrijft in zijn lectorale rede dat het begin van het forensisch computeronderzoek zich qua bewijsgaring destijds vooral richtte op met wachtwoord beveiligde computers en elektronische zakagenda’s. De adoptie en het gebruik van internet was in die tijd nog zeer beperkt. Deze ontwikkelingen kenden hun weerslag op de opsporing. In ander werk beschrijft Henseler (2010) dat ontwikkelingen in wat hij digitale waarheidsvinding noemt eind jaren ’80 zijn begonnen in Nederland. In de jaren ’90 kwam het zoeken naar digitale sporen in opkomst bij de politie en bijzondere opsporingsdiensten. In navolging van de oprichting van speciale teams computercriminaliteit, gaat het NFI (toen Gerechtelijk Laboratorium) in deze ontwikkeling mee (forensisch computeronderzoek). Medio jaren ’90 groeit de interesse. “Het ging toen niet meer alleen om elektronische zakagenda’s, maar om de versleuteling van digitale gegevens door criminelen […]” (Henseler, 2010, p.8). Ook andere ontwikkelingen, zoals de toenmalige highspeed modems en GSM-netwerken, zorgden destijds volgens Henseler voor diverse problemen en uitdagingen.

In het eerste decennium van deze eeuw werd digitaal bewijs vooral gezocht in e-mails en documenten, en in gevallen in foto’s, video’s en internetgeschiedenis. In Nederland gebeurde het (juridisch) doorzoeken van digitale data volgens Henseler (2017) toen nog mondjesmaat. In het tweede decennium, wat werd gekenmerkt door de opkomst van social media, smartphones en cloud computing, nam de toepassing hiervan toe. Henseler stelt dat sinds die tijd digitaal bewijs een vergelijkbare rol aanneemt als dat van traditioneel bewijs.

Opsporingsinstanties merken een transitie in crimineel gebruik van veilig applicaties en andere diensten bij verschillende soorten criminaliteit (Nogala & Schröder, 2019). De meerderheid zijn populaire diensten en apps die ook dagelijks worden gebruikt door de gemiddelde bevolking, denk aan WhatsApp en e-mail.[22] Dergelijke populaire applicaties en apparaten worden steeds veiliger door het standaard invoeren van bijvoorbeeld E2EE. Deze encryptie zorgt ervoor dat criminelen relatief betrouwbaar en veilig kunnen communiceren. Criminelen lijken ook meer gebruik te maken van Apple-apparaten. Er is een stijging waarneembaar in de inbeslaggenomen Apple-apparaten bij opsporingsonderzoeken; van 59,4% in 2014 naar 82,2% in 2019 (Europol & Eurojust Public Information, 2020b).

Daders gebruiken ook regelmatig anonimiserende of encryptiehulpmiddelen zoals VPN en Tor (Europol & Eurojust Public Information, 2019). Ten eerste, omdat de nieuwe generatie daders

[22] Lensink, H. (2018). *Big brother will be watching – of valt dat wel mee?* Verkregen via: https://www.ftm.nl/artikelen/big-brother-will-be-watching-of-valt-dat-wel-mee

opgegroeid is met technologie en gemakkelijk IT gebruikt. Ten tweede, omdat deze technologieën gebruiksvriendelijk zijn en weinig technische kennis vereisen. Ook social media-applicaties hebben standaard E2EE, waardoor daders zonder technische vaardigheden in relatieve anonimiteit kunnen communiceren. Een basisniveau digitale geletterdheid is voldoende om gebruik te maken van encryptie en/of anonimiserende hulpmiddelen.

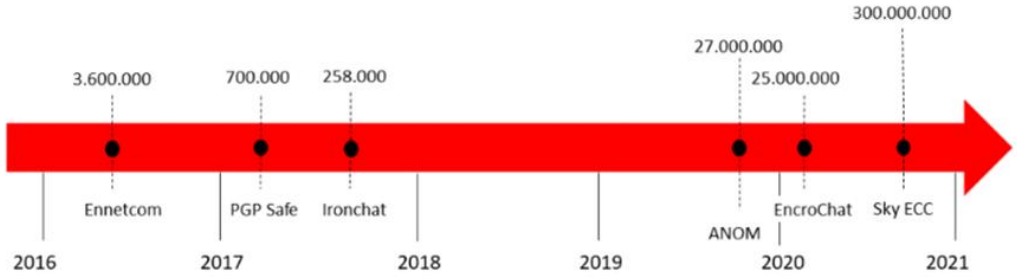
Op het dark web zijn zowel encryptie als anonimiserende technologieën van toepassing (Goodison e.a., 2019). Om online een transactie te voltooien die veilig is voor zowel de koper als verkoper, moet worden voldaan aan vijf cruciale voorwaarden (Moore & Rid, 2016): privacy, anonimiteit, authenticatie, hidden exchange en betaling. Voor privacy is het van belang dat communicatie tussen de participanten veilig is en ontoegankelijk voor derden; de anonimiteit moet gewaarborgd zijn. Tegelijkertijd is authenticatie van beide partijen nodig, om zeker te zijn van de persoon waarmee wordt gehandeld. Hidden exchange, oftewel een verborgen warenruil is nodig voor een veilige transactie. De verkoper moet de markt kunnen voortzetten zonder exposure. Tot slot, betaling, om een transactie veilig te laten verlopen is het belangrijk dat het niet terugleidt tot de koper. De oplossing hiervoor is cryptovaluta. Het doel van cryptovaluta in een criminele transactie is om de afhankelijkheid van overheid, politieke en financiële instellingen weg te nemen en de transactie te baseren op een niet door de overheid gecontroleerde technologie (cryptografie). De bekendste cryptomunt is Bitcoin; geïntroduceerd in 2008. Het gebruik van cryptovaluta biedt een uitdaging voor opsporingsinstanties om het geld te 'volgen'. Daarmee wordt de kans verkleind om frauduleuze transacties te voorkomen en om geld te vinden.

3.3.1 Delicten waarbij encryptie voorkomt

Dat encryptie lijkt toe te nemen in opsporingsonderzoeken is één, maar bij welke delicten komt encryptie voor? In 2016 heeft Europol een multidisciplinair initiatief gestart om het benutten van verhullende technieken (encryptie) door criminelen tegen te gaan (Europol & Eurojust Public Information, 2020b). Dit initiatief resulteert in het Europol European Cybercrime Centre (EC3) decryptie platform. Dit platform ondersteunt Europese wethandhavingsinstanties die moeite hebben met de ontsleuteling van legaal verkregen versleuteld bewijs (Europol, 2020a; Ilbiz & Kaunert, 2022). Met dit platform worden meerdere onderzoeken uitgevoerd voor cybercrime, seksueel kindermisbruik, bankpasfraude, wapenhandel, drugshandel, witwassen, terrorisme, mensensmokkel en moord (Europol & Eurojust Public Information, 2019; Europol & Eurojust Public Information, 2021). Dit toont aan dat criminelen gebruik maken van encryptie bij onder andere deze verschillende criminele activiteiten.

In de media-analyse (zie par. 2.1) zagen we qua criminaliteit dat de volgende criminaliteitstypen vaker dan één keer voorkomen: handel in drugs en wapens, witwassen, corruptie (bij de haven en politie), kinderporno en moord (aanslag, poging tot en moordplannen). Ook cybercrime, zoals malware en ransomware-aanvallen en hacken kwamen in de media-analyse naar voren. Deze typen houden echter meer verband met criminelen die systemen van derden versleutelen. Verder zagen we in de door ons geanalyseerde mediaberichten dat veel aandacht uitging naar grotere zaken. De media deed uitgebreid verslag van chatdiensten, zoals Sky ECC, IronChat en Ennetcom. In een rapport van Europol & Eurojust Public Information (2021) wordt benoemd dat de markt voor versleutelde communicatieproviders (zoals aanbieders van cryptotelefoons) voor georganiseerde misdaadgroepen stijgt. Uit een onderzoek naar inbeslaggenomen servers van aanbieders van

cryptocommunicatie blijkt dat criminele gebruikers via deze communicatiediensten openlijk over hun criminele activiteiten berichten (Vermeulen e.a., 2021). Oerlemans (2022) laat in een overzicht zien hoeveel miljoenen berichten er in de afgelopen jaren via cryptodiensten zijn verstuurd (figuur 3.1). Dit overzicht is gebaseerd op persberichten van het OM, politie en rechtspraak.



Figuur 3.1: Overzicht aantal berichten verstuurd via cryptodiensten (Oerlemans, 2022)[23]

Hierna beschrijven we enkele criminele activiteiten waarvan het meest bekend is over encryptie: (i) georganiseerde criminaliteit, (ii) kinderpornografie en kindersekstoerisme en (iii) terrorisme.

Georganiseerde criminaliteit. Een van de belangrijkste uitdagingen voor opsporingsinstanties is het gebruik van versleutelde communicatie door georganiseerde misdaadgroepen (Europol & Eurojust Public Information, 2020b). In 2017 werd in het Nationaal dreigingsbeeld van georganiseerde criminaliteit al beschreven dat binnen de georganiseerde criminaliteit versleutelde diensten laagdrempelig toegankelijk zijn. De wijdverspreide en groeiende invloed van digitale ontwikkelingen, waaronder encryptie, draagt bij aan de dreiging van georganiseerde criminaliteit omdat hierdoor de reikwijdte van criminelen vergroot wordt (Boerman e.a., 2017). Europol heeft de dreigingen van serieuze en georganiseerde misdaad in kaart gebracht, evenals het gebruik van encryptie (Europol, 2021b). Daaruit blijkt dat in Europa criminelen versleutelde communicatie gebruiken zoals social media en berichtendiensten om met elkaar te communiceren. Ze gebruiken de diensten ook om illegale goederen te adverteren en desinformatie te verspreiden. Al deze digitale platformen bieden toegang tot versleutelde communicatie en anonieme betalingsmogelijkheden. Tevens gebruiken ze hulpmiddelen zoals VPN's, proxies, anonieme browsers (o.a. Tor Browser) en cryptotelefoons.

Doordat criminelen meer gebruik maken van encryptie, anonimiserende hulpmiddelen (bijv. VPN en Tor), virtuele munten en het dark web, is het lastiger voor opsporingsinstanties om de fysieke locatie van een verdachte te achterhalen. Verlies van locatie is een substantiële uitdaging in effectieve onderzoeken en vervolgingen. Daarnaast zijn er digitale sporen waarvan onduidelijk is onder welk rechtsgebied ze vallen en welke juridische kaders gelden om het bewijs te verzamelen. Te denken valt aan het online monitoren van criminele activiteiten of het opslaan van data (EMCDDA & Europol, 2017).

Ter illustratie, het plegen van geweldsdelicten als een dienst wordt in toenemende mate aangeboden op het dark web waarbij met versleutelde communicatietechnieken worden toegepast. Deze geweldsacties variëren van dreigingen, intimidatie, vandalisme en mishandeling tot kidnapping, marteling, verminking en moord. Een ander voorbeeld waarbij encryptie faciliteert is 'wildlife' criminaliteit; het stropen, verzamelen, verhandelen, importeren, exporteren, bezitten, verkrijgen en

[23] De oorspronkelijke auteur heeft toestemming gegeven om de afbeelding over te nemen in dit rapport.

consumptie van wilde flora en fauna, wat in strijd is met (inter)nationale wetgeving. De meerderheid van verhandelde dieren wordt online verkocht en gekocht via social media, mobiele apps en speciale online marktplaatsen. Reguliere communicatiemiddelen zoals mobiele apps en online chats worden veel gebruikt door handelaren, verkopers en kopers. Een laatste voorbeeld betreft mensensmokkel waarbij social media en versleutelde communicatietechnieken worden gebruikt om diensten aan te bieden, smokkelroutes te coördineren en slachtoffers te werven. Ook wordt het ingezet om routes te delen en audio- en videomateriaal evenals documenten zoals tickets te delen (Europol, 2021b).

Onlangs is gerapporteerd dat migrantensmokkelaars ook gebruik maken van cryptovaluta, wat naar verwachting in frequentie zal toenemen (Europol, 2021b). Cryptovaluta is een belangrijk middel om te betalen voor criminele goederen en diensten. Daarnaast wordt het gebruikt voor cybercriminaliteit (zoals ransomware), financiële fraude (zoals vastgoedfraude) en om geld wit te wassen. Er worden crypto-geldautomaten aangeboden die crimineel geld kunnen omzetten in cryptovaluta.

Kinderpornografie en kindersekstoerisme. Online kindermisbruikers gebruiken in toenemende mate online anonimiteit- en encryptiehulpmiddelen om materiaal te maken en delen. Ze gebruiken reguliere apps en apparaten en het dark web. Daders van online kindermisbruik gebruiken ook anonimiserende hulpmiddelen zoals VPN's, proxy servers en Tor (Europol, 2021b). Meldingen van online kindermisbruik zijn de laatste tien jaren drastische toegenomen (Koomen, 2021). Het Amerikaanse centrum voor missende en uitgebuite kinderen hebben een *CyberTipline* waar het bezit, maken of distributie van materiaal (video, audio) van online seksueel kindermisbruik (Child Sexual Abuse Material [CSAM]) gemeld kan worden.

Van deze meldingen is de EU wereldwijd de grootste geografische hub waar materiaal van seksueel kindermisbruik gedeeld wordt. Negen van de tien gerapporteerde URL's worden gehost in Europa. 94% van deze meldingen waren op platformen van het bedrijf Facebook (tegenwoordig Meta) zoals Messenger, Instagram en WhatsApp (NCMEC, 2020). Europol bevestigt het gebruik van peer-to-peer communicatiekanalen zoals Facebook Messenger voor het delen van CSAM (2021c). Sinds 2019 heeft Facebook E2EE uitgerold voor haar diensten. Daardoor zijn onlinekindermisbruik zaken moeilijker waarneembaar voor Facebook en opsporingsinstanties. Het gebruik van encrypte communicatie-apps zoals Signal en Telegram worden populairder onder daders van kindermisbruik (Broadhurst, 2019; in Holt, Cale, Leclerc & Drew, 2020).

Terrorisme. De AIVD (2012) beschrijft zo'n tien jaar geleden dat jihadisten elkaar treffen op het internet op 'openbare' virtuele plekken zoals social media, webfora en chatprogramma's, maar ook op semiopenbare of besloten virtuele plekken zoals het dark web. Op het dark web vinden de jihadistische activiteiten plaats die de grootste dreiging vormen. Organisatoren achter het jihadistische internet zijn geen leden van jihadistische organisaties, maar worden door de AIVD beschreven als de 'producenten' van het jihadistisch internet. De administrators (beheerders) en moderators (toezichthouders) van de kernfora zijn de meest invloedrijke producenten. Er wordt jihadistische gedachtengoed gedeeld op het 'reguliere internet' vanaf het dark web.

Sociale media worden vooral gebruikt voor tijdelijke verspreiding van jihadistische propaganda. Op sociale media worden ongewenste uitingen actief door moderators verwijderd, wat de berichten tijdelijk van aard maakt. Doordat accounts (tijdelijk) werden geblokkeerd of verwijderd op Twitter en Facebook, is men overgestapt naar alternatieve platformen, zoals Telegram en Parler. Dit biedt de voorkeur voor terreurorganisaties om berichten te delen vanwege de veiligheid en

encryptie (Bloom e.a., 2017; NCTV, 2021). Als berichten door een gebruiker worden verwijderd, dan worden deze ook voor andere gebruikers verwijderd. Bovendien wordt gebruikt gemaakt van een 'zelfvernietiging' timer, zodat berichten automatisch worden verwijderd zodra de ontvanger het heeft gelezen. Telegram heeft een belangrijk rol gespeeld in de werving en coördinatie van de terrorisme aanvallen in Europa. De daders van de aanvallen in Brussel en Parijs hadden hun plannen gecoördineerd en gecommuniceerd via Telegram (Bloom e.a., 2017).

3.3.2 Het verloop van opsporingsonderzoeken

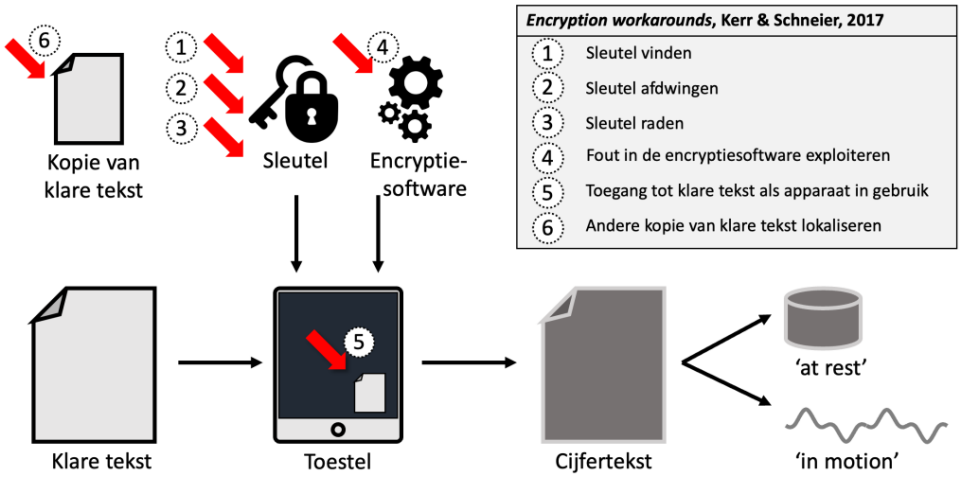
In deze paragraaf gaan we nader in op wat reeds bekend is over het verloop van opsporingsonderzoeken waarin encryptie voorkomt. We gaan daarbij specifiek in op (i) opsporingstactieken en (ii) doorlooptijd. Er is in de literatuur geen informatie gevonden over de slagingskans om achter encrypte data en encrypte communicatie te komen. Tevens was geen informatie beschikbaar over de voortzetting en/of het stopzetten van opsporingsonderzoek op moment dat op (complexe) encryptie wordt gestuit. Hoewel we in dit onderzoek een beperking opleggen door alleen naar de Nederlandse context te kijken, kunnen we niet om het grenzeloze karakter van criminaliteit heen. Dit heeft namelijk ook zijn weerslag op het verloop van opsporingsonderzoeken. Daarom worden enkele relevante aspecten in relatie tot encryptie en de internationale context benoemd (iii).

Twee opsporingstactieken: encryptie omzeilen en encryptie kraken

Naast de interne factoren die te maken hebben met encryptie – de encryptiemechanismen en sleutellengten – zijn externe factoren belangrijk in het kraken van een systeem. Ook al zijn de theorie en de implementatie perfect, externe aspecten kunnen helpen bij het ontcijferen. Bijvoorbeeld, side-channel-aanvallen zijn vaak mogelijk als er fysieke toegang tot de hardware is. Verder kunnen systemen geanalyseerd worden met gebruik van de broncode. Dit heet ook wel whitebox-analyse. De broncode van open source systemen (zoals Signal) is makkelijk te onderzoeken.[24] Tevens komt het vaak voor dat een 'proprietary' systeem (systemen waarvan de code niet onthuld wordt) open source componenten bevat. Deze componenten kunnen kwetsbaarheden hebben die het kraken van het hele systeem kan faciliteren. Tot slot komt het voor dat het sleutelbeheer slordig wordt uitgevoerd. In dat geval kan de sleutel gevonden worden. Als de sleutel gebruikt kan worden, maakt de sterkte van de encryptie niet meer uit. Voor opsporingsinstanties zijn er twee manieren om met encryptie om te gaan in opsporingsonderzoeken: encryptie omzeilen en encryptie kraken (Europol & Eurojust Public Information, 2019). Deze lichten we nu toe.

Encryptie omzeilen. Kerr en Schneier (2017) noemen in hun artikel zes tactieken om encryptie te omzeilen, iets wat zij aanduiden als 'encryption workaround'. Dit zijn het vinden van de sleutel, afdwingen van de sleutel, raden van de sleutel, exploiteren van een fout in de encryptiesoftware, toegang tot leesbare tekst (klare tekst) als het apparaat wordt gebruikt en het lokaliseren van een kopie van de leesbare tekst (figuur 3.2). De sleutel kan staan voor een wachtwoord, toegangscode of wachtwoordzin. Hierna lichten we de zes technieken toe.

[24] Open source wil zeggen dat de broncode publiek beschikbaar is.



Figuur 3.2: Wijzen om encryptie te omzeilen (gebaseerd op Kerr & Schneier, 2017)

(1) De eerste tactiek is het vinden van (een kopie van) de sleutel. Om deze tactiek succesvol te laten zijn moet er sprake zijn van de volgende situatie. Ten eerste, moet de sleutel ergens beschikbaar zijn. De verdachte moet de sleutel ergens hebben opgeschreven, bijvoorbeeld fysiek op een post-it of in een schrift, of in een digitaal bestand op een computer of telefoon. Een versleutelingsprogramma kan ook per ongeluk een kopie van de sleutel opgeslagen hebben op de harde schijf van de computer. Ten tweede, de opsporingsinstanties moeten de sleutel vinden en kunnen lezen. De sleutel kan verstopt zijn in een computer waardoor forensische analyse nodig is om een sleutel te lokaliseren. Of een sleutel is zelf versleuteld en een tweede sleutel is nodig om tot de originele tekst te komen. Denk aan software zoals een wachtwoordkluis waar honderden wachtwoorden opgeslagen kunnen worden, maar een meesterwachtwoord nodig is om de 'kluis' te openen. Als laatste moeten de opsporingsinstanties op rechtmatige wijze toegang krijgen tot de sleutel. Dit kan met een huiszoeking of verregaande maatregelen zoals het gebruik van een keylogger; software dat bijhoudt en vastlegt wat iemand op een toetsenbord typt.

(2) De tweede tactiek is om de sleutel af te dwingen van iemand die de sleutel heeft of kent. In de ideale situatie biedt de verdachte de sleutel aan. Een belangrijke voorwaarde is om binnen het juridisch geldende kader te blijven om de sleutel op rechtmatige wijze te verkrijgen. In sommige jurisdicties kan de sleutel worden afgedwongen bij de verdachte zelf of bekenden van de verdachten. Ten tijde van dit onderzoek is de Innovatiewet van kracht gegaan (1 oktober 2022).[25] Met deze wet zijn er mogelijkheden geïntroduceerd om – binnen kaders – de sleutel onder dwang af te laten staan door een verdachte. In hoofdstukken 4 en 5 komt dat nadrukkelijker aan de orde.

(3) Het raden van de sleutel is een realistischere optie dan het vinden van een sleutel, maar is uitdagender daar het veel capaciteit en tijd vraagt. Om het proces te versnellen kunnen opsporingsinstanties informatie over de verdachte gebruiken om een geïnformeerde gok te wagen. Als een wachtwoord door een persoon is aangemaakt in plaats van een computer, dan is de kans groot dat het wachtwoord niet volledig random is.

De meeste wachtwoorden hebben namelijk een specifieke volgorde. Wachtwoorden met een vereiste van een hoofdletter en een cijfer, starten vaak met letters en eindigen met een cijfer. Bovendien gebruiken mensen vaak dezelfde wachtwoorden, of een variatie hiervan. Voorgaande

[25] Zie ook: https://www.eerstekamer.nl/wetsvoorstel/35869_innovatiewet_strafvordering

wachtwoorden van verdachten kunnen voor het raden van het wachtwoord dus waardevolle informatie opleveren. Ook informatie over de verdachte zelf kan waardevolle informatie opleveren. Door mens aangemaakte wachtwoorden hebben regelmatig een vorm van persoonlijke of sociale informatie (huisdier, hobby, geboortedata van familie, et cetera).

Een techniek om het wachtwoord te raden is om verschillende onderdelen van het bestaande wachtwoord te combineren tot een nieuw wachtwoord. Deze aanpak wordt gebruikt in sommige technische hulpmiddelen, zoals Hashcat.[26] Contextuele informatie over de verdachte vraagt om een doelgerichte benadering om het wachtwoord juist te raden. Het raden van het wachtwoord vergt zowel technologische hulpmiddelen, zoals rekenkracht, en voldoende en vaardig personeel. Een deel van dit proces kan geautomatiseerd uitgevoerd worden, maar een groter deel moet uitgevoerd worden door experts om de benodigde informatie te achterhalen om het wachtwoord te raden. Als tijdens een opsporingsonderzoek een sleutel legaal wordt gevonden of geraden, dan mag deze over het algemeen worden gebruikt in het onderzoek (Europol & Eurojust Public Information, 2019). De tactische recherche kan een rol spelen bij het vinden en/of raden van de juiste sleutel.

(4) Het exploiteren van een fout of fouten in de encryptiesoftware is een vierde manier om toegang te krijgen tot data zonder kennis van de sleutel. Een fout, of kwetsbaarheid, kan komen van een systeemontwerper of een lek in het encryptiealgoritme. Zowel criminelen, overheden en anderen profiteren van dergelijke kwetsbaarheden. Als een kwetsbaarheid bekend is bij softwareontwikkelaars, dan kunnen ze dit herstellen met een patch (een nieuwe versie van de software). De patch kan bijvoorbeeld worden uitgevoerd met een software-update.

Kwetsbaarheden in de software die niet bekend zijn bij de softwareontwikkelaar worden ook wel zero-days genoemd. Overheden worden door de cybersecuritygemeenschap heftig bekritiseerd als ze gebruik maken van zero-day kwetsbaarheden. Het zou zorgen voor een vertraging in het rapporteren van kwetsbaarheden met als gevolg dat het niet alleen de verdachte kwetsbaar maakt, maar alle gebruikers van deze software. Deze kritiek geldt alleen voor zero-day kwetsbaarheden en niet voor kwetsbaarheden waar al een patch voor beschikbaar is, maar die nog niet is gebruikt door de verdachte (bijv. wanneer de update nog niet is uitgevoerd).

(5) De vijfde tactiek is om toegang te krijgen tot leesbare tekst als het apparaat wordt gebruikt. Als een apparaat in gebruik is, dan wordt bepaalde informatie ontsleuteld en omgezet in leesbare tekst. Als bijvoorbeeld een bericht via WhatsApp wordt gestuurd, dan kan de ontvanger dit versleutelde bericht pas lezen als de mobiele telefoon wordt gebruikt. Deze leesbare tekst (oftewel klare tekst) is waardevol voor opsporingsinstanties.

Deze tactiek is gebonden aan ‘realtime’, dat wil zeggen dat er een continue toegang moet zijn tot het digitale apparaat. Om toegang te krijgen tot versleutelde bestanden kunnen opsporingsinstanties een keylogger installeren om bij te houden wat de verdachte typt of een verborgen camera installeren in de kamer om te filmen wat de verdachte aan het typen en lezen is. Een alternatief is om een verdachte fysiek aan te houden terwijl diens digitale apparaten open staan. Als een verdachte is ingelogd op een mailprogramma of een dark market, kunnen overheidsinstanties direct na de aanhouding informatie uit de accounts halen, zonder dat een wachtwoord nodig is. Als fysiek geen toegang kan worden verschaft tot het apparaat, dan kan op afstand het apparaat gehackt

[26] Hashcat is een wachtwoordkraker. Het toepassen van hashes gebeurt om wachtwoorden in gecodeerde vorm op te slaan in databases. Dit betekent dus dat wanneer een database wordt gestolen, een aanvaller niet meteen directe toegang heeft tot wachtwoorden. Zie: https://www.security.nl/posting/551346/Prestaties+wachtwoordkraker+Hashcat+sterk+verbeterd.

worden. Hier kleven technische en juridische haken en ogen aan. Juridisch is het 'binnentreden op afstand' geregeld in de Wet Computercriminaliteit III, die in werking trad op 1 maart 2019.

(6) De zesde en laatste techniek is het lokaliseren van een kopie van de leesbare tekst. Deze tactiek omzeilt encryptie volledig. Opsporingsinstanties kunnen sleutels en/of informatie opvragen bij derde partijen (personen en/of legale partijen). De meeste EU-lidstaten hebben een specifieke of algemene wettelijke bepaling waarin deze derde partijen kunnen worden verplicht om een sleutel of informatie over te dragen (Europol & Eurojust Public Information, 2019). Lidstaten ervaren nog steeds moeilijkheden bij het opvragen van data of sleutels bij service providers. De service providers stellen dat ze niet aan het verzoek kunnen voldoen vanwege de data die end-to-end versleuteld zijn.

Veel communicatie loopt via private communicatiediensten zoals Twitter, WhatsApp, Gmail, Facebook, et cetera. Het gebruik van een internettap gaat via de aanbieder van een communicatiedienst, oftewel een internet service provider (art. 126m Sv). Om data te ontsleutelen moeten opsporingsinstanties samenwerken met deze private partijen. De politie kan bijvoorbeeld aan een cloud provider verzoeken om een kopie van een onversleutelde back-up in de cloud te verstrekken. Het bekendste voorbeeld is het verzoek van de FBI aan Apple om een iCloud back-up te achterhalen voor de terroristische aanslag in San Bernardino in Californië (zie ook hoofdstuk 1). Om succesvol een kopie van de klare tekst te kunnen lokaliseren moet een onversleutelde kopie bestaan. Daarna moeten de opsporingsinstanties de kopie kunnen vinden en op een rechtmatige wijze zoeken en in beslagnemen. Tot slot moet de onversleutelde kopie voldoende overeenkomsten hebben met de het versleutelde origineel om een adequate vervanging te zijn. De inhoud van harde schijven kunnen met de tijd veranderen en de gekopieerde data hoeft niet noodzakelijkerwijs gelijk te zijn aan het origineel.

Het komt echter vaak voor dat deze tussenliggende private diensten niet onder het tapbevel en de ontsleutelplicht vallen of dat de diensten in het buitenland gevestigd zijn en daardoor niet verplicht kunnen worden om mee te werken (Custers, 2018). Daarnaast werkt de politie bijvoorbeeld op het gebied van cybercriminaliteit graag samen met private partijen waarbij de expertise van de private partij kan helpen bij de oplossing van een specifiek probleem in de opsporing. Deze private partijen kunnen echter botsende belangen hebben. Hierbij moet bijvoorbeeld rekening gehouden worden met welke informatie de politie aan private partijen geeft en wie er op toe ziet dat de informatie enkel voor beoogde doelen gebruikt wordt (Van den Eeden e.a., 2021). Ook in het monitoren van trends in het gebruik van applicaties en software door criminelen en het onderhouden van bewustzijn van verschillende opsporingstechnieken is het essentieel dat opsporingsinstanties relaties onderhouden met private partijen omdat deze hen kan adviseren op gebieden waar zij zelf te weinig technisch vermogen beschikt (Pisariç, 2021).

Als een land ontsleutelde informatie wil gebruiken uit een ander land voor eigen onderzoek, dan moeten de data volgens de wetgeving van het land waarin het ontsleuteld is legaal zijn verkregen. Daarnaast moet het vragende land dit bewijs legaal krijgen van het land dat het heeft ontsleuteld, normaal gesproken via een European Investigation Order (EIO) of Mutual Legal Assistance verzoek (MLA) (Europol & Eurojust Public Information, 2021). Er wordt dan een EIO of MLA gestuurd naar het land dat op legale manier de data heeft ontsleuteld om ook bezit te krijgen over de data als bewijs. In Nederland mogen cryptoberichten niet worden geanalyseerd zonder toestemming van een rechter-commissaris (rc) (Nationale politie, 2021). Een gevolg daarvan is dat veel informatie en mogelijk bewijs nooit gebruikt wordt. De rc heeft ten aanzien van het gebruik van de data van verschillende datasets bepaald dat deze slechts mag worden geanalyseerd aan de hand van woorden die zijn gerelateerd aan

ernstige strafbare feiten. Alleen bij serieuze verdenking van bijvoorbeeld cocaïnehandel kan de rc toestemming verlenen om de volledige inhoud van de berichten te lezen.

Encryptie kraken. Als de encryptie niet omzeild kan worden, dan kan getracht worden om de encryptie te kraken. Encryptie kan gekraakt worden door toegang tot een computersysteem te krijgen met behulp van forensische hulpmiddelen. In de meeste landen moet worden voldaan aan de bestaande generieke opsporingsbevoegdheden. Er is een aantal landen in de EU die specifieke juridische kaders hebben. Nederland heeft ook specifieke juridische kaders om onder bepaalde omstandigheden te mogen hacken.

Op 1 maart 2019 heeft de politie op basis van de wet Computercriminaliteit III nieuwe bevoegdheden gekregen (Van Uden & Van den Eeden, 2022). Onder strikte voorwaarden mogen opsporingsinstanties heimelijk en op afstand binnendringen in geautomatiseerde werken van verdachten. Dit mag alleen worden ingezet bij verdenking van een ernstig strafbaar feit. Er is één team met leden van de politie, FIOD en KMAR dat deze speciale opsporingsbevoegdheid heeft. Dit is het Digital Intrusion Team (DIGIT).[27]

De AIVD heeft de mogelijkheid om bepaalde communicatie (zoals internet of telefoon) te onderscheppen, mits dat nodig voor veiligheidsonderzoeken.[28] Dit wordt Onderzoeksopdrachtgerichte Interceptie (OOG) genoemd en mag alleen onder strikte voorwaarden. Er is toestemming nodig van de minister van Binnenlandse Zaken en een onafhankelijk Toezichtscommissie Inzet Bevoegdheden (TIB) (Van Uden & Van den Eeden, 2022). Sinds april 2022 stelt een tijdelijke wet de AIVD en de MIVD in staat om hun bestaande bevoegdheden, zoals OOG, effectiever en sneller in te zetten tegen cyberdreigingen (AIVD, 2022).

In de VS heeft de FBI een 'network investigation technique' (NIT) ingezet om de locatie van daders van online kindermisbruik te achterhalen. De NIT betreft malware in iemands browser, wat het mogelijk maakt om het originele IP-adres en andere informatie te verzamelen (o.a. Garcha, 2018; in Holt e.a., 2020). Deze techniek was succesvol in het hacken van meerdere computers en heeft geleid tot meerdere arrestaties van deelnemers en administrators van een website met onlinekindermisbruik. Advocaten hebben de rechtmatigheid van bewijsmateriaal dat NIT heeft opgeleverd in twijfel getrokken op basis van het vierde amendement in de VS (Garcha, 2018, in Holt e.a., 2020). Het vierde amendement verbiedt onredelijke huiszoekingen en inbeslagnemingen, waar het gebruik van malware onder zou kunnen vallen. Uiteindelijk heeft de rechter besloten dat het inzetten van NIT onrechtmatig was.[29]

Doorlooptijd

Succesvolle opsporingsoperaties zoals EncroChat, Sky ECC en ANOM hebben ervoor gezorgd dat het opsporingswerk voorzien wordt van startinformatie. Dit zorgt voor een kortere doorlooptijd van zaken (Nationale Politie, 2021). De Nationale Politie geeft een voorbeeld: de opsporing is vorig jaar met zes man een half jaar bezig geweest met een zaak en kreeg deze niet rond. Door de ontsluiting van

[27] Politie (z.d.). *Legaal hacken*. Verkregen via: https://kombijde.politie.nl/vakgebieden/ict/legaal-hacken

[28] AIVD (2018). *Onderzoeksopdrachtgerichte interceptie (OOG): Hoe onderzoeken wij communicatiestromen?* Verkregen via: https://www.aivd.nl/onderwerpen/onderzoeksopdrachtgerichte-interceptie-oog

[29] Cushing, T. (2017). *Judge says FBI's NIT warrant invalid, points out FBI agent knew it was invalid when he requested it.* Verkregen via: https://www.techdirt.com/2017/04/07/judge-says-fbis-nit-warrant-invalid-points-out-fbi-agent-knew-it-was-invalid-when-he-requested-it/

cryptoberichten heeft één rechercheur in drie weken een zaak opgebouwd waarvoor diezelfde verdachte alleen nog aangehouden en verhoord moet worden.

De politie moet naar eigen zeggen soms het gevoel onderdrukken om alles eruit te halen wat erin zit bij gekraakte berichten. Er moet selectief gelezen worden en twee belangrijke zaken uit een enorme hoeveelheid berichten kiezen om een afgerond proces verbaal te maken. Alles uitpluizen terwijl er niet meer dan een lage straf te verwachten is, is vaak niet de moeite waard, zeker niet nu er zoveel informatie van andere criminelen beschikbaar is, aldus de Nationale Politie (2021).

In onderstaande twee casussen zijn dergelijke opsporingsoperaties kort samengevat. Let op dat dit 'succesverhalen' zijn. Verhalen over politieonderzoeken waarin veel is geïnvesteerd, maar die tot weinig of geen bewijs hebben geleid, zijn we niet in openbare bronnen tegengekomen.

Casus 1: Ennetcom

Ennetcom is een telecombedrijf uit Nederland dat cryptotelefoons aanbood met PGP-versleuteling. Deze versleuteling maakt het moeilijker voor opsporingsdiensten om berichten te onderscheppen en maakt het criminelen makkelijker om zonder codetaal te communiceren. De telefoons waren te koop voor een prijs tussen de 1.400 en 2.200 euro. Op 19 april 2016 is het volgende bericht in vier talen gestuurd naar de 19.000 klanten van Ennetcom: 'vanaf nu kunt u (voorlopig) geen gebruik meer maken van deze diensten in verband met een grootschalig strafrechtelijk onderzoek naar criminele eindgebruikers van versleutelde informatie'. In Nederland valt de recherche binnen op de verschillende adressen van het Nijmeegse telecombedrijf, dat verdacht werd van witwassen en het faciliteren van criminele activiteiten, en aan de andere kant van de oceaan wordt een kopie gemaakt van de BlackBerry Enterprise Server (BES) in Toronto, Canada. De berichten (Ennetcom-data) waren namelijk door het bedrijf opgeslagen op BES-servers in Canada.

Een half jaar later ontvangt het OM op last van de Canadese rechter zeven terabyte aan versleutelde bestanden en ruim 3,6 miljoen berichten. THTC en het NFI onderzoeken deze berichten. De vermeende daders waanden zich veilig en spraken vrijuit over hun daden of modus operandi of met versluierd taalgebruik. Zo wijst 'iets onder z'n waggie' op een peilbaken (GPS-tracker) en 'vegen' staat voor 'vermoorden'. In een artikel van Follow the Money (een platform voor onderzoeksjournalistiek) geeft een officier van justitie dat deze Ennetcom-data 'van belang [zijn] in zeker honderd strafzaken'.[30]

Casus 2: EncroChat en Sky ECC

In 2020 is het versleutelde netwerk EncroChat ontmanteld, wat een grote shock is voor de georganiseerde misdaad in Europa (Europol & Eurojust Public Information, 2020a). EncroChat biedt een cryptotelefoon met een abonnement aan. Het is een Android telefoon waar alle kwetsbaarheden af zijn gehaald en alleen de EncroChat communicatie app was geïnstalleerd (Europol & Eurojust Public Information, 2021). Alle functies die een kwetsbaarheid zouden vormen voor de anonimiteit van de gebruiker zijn weggehaald, zoals de camera, microfoon, GPS en usb-poort. Verder is het klantaccount niet gekoppeld aan het apparaat en wordt er geen gebruik gemaakt van een simkaart. Daarnaast bood het product extra veiligheidsopties zoals het verwijder-

[30] Lensink, H (2017). *Hoe brute moorden leiden tot een discussie over privacy*. Verkregen via: https://www.ftm.nl/artikelen/moorden-discussie-privacy-pgp

Casus 2 (vervolg): EncroChat en Sky ECC

en van alle data. Dit kan op afstand worden gedaan door de helpdesk of leverancier (bijv. bij arrestatie door de politie) of door een aantal keer het verkeerde wachtwoord in te voeren. De cryptotelefoons kostten ongeveer 1.000 euro per stuk en een zes maanden abonnement met internationaal bereik en 24/7 helpdesk kostte 1.500 euro.

In 2017 kwamen de Franse politie (Gendarmerie) deze telefoons regelmatig tegen in opsporingsonderzoeken naar georganiseerde misdaad. In 2020 leek EncroChat één van de grootste providers van versleutelde digitale communicatie waarvan vermoedelijk een groot deel van de gebruikers criminele activiteiten pleegden. De hotspots van gebruikers waren op locaties die bekend staan om onder andere de handel van cocaïne en cannabis.

In 2019 hebben de Franse autoriteiten een zaak geopend bij Eurojust (het Agentschap van de EU voor justitiële samenwerking in strafzaken). Eurojust faciliteerde het opzetten van een Joint Investigation Team (JIT) tussen Frankrijk en Nederland in april 2020, met participatie van Europol: Operatie Lemont, zoals het in Nederland werd genoemd. Honderden onderzoeken hebben met autorisatie van de magistraat, communicatie onderschept van duizenden criminelen. Frankrijk leidde de operatie, die daar Emma 95 werd genoemd. De interceptie van berichten eindigden op 13 juni 2020, toen het bedrijf zich realiseerde dat overheidsinstanties het platform hadden geïnfiltreerd. EncroChat heeft vervolgens een waarschuwing naar alle gebruikers gestuurd met het advies om hun telefoon te vernietigen.

In totaal zijn er 100 miljoen onderschepte berichten gedeeld door tienduizenden gebruikers, voornamelijk uit Europa (Europol & Eurojust Public Information, 2021). De data waren in eerste instantie gedeeld met Nederland, door deelname aan JIT. Andere landen wilden ook toegang tot de ontsleutelde data van EncroChat. Ontsleutelde data zijn geleverd voor honderden lopende opsporingsonderzoeken. Deze data zorgden voor nieuw bewijs en verstoring van criminele activiteiten zoals drugshandel op grote schaal, witwassen, corruptie en andere vormen van gewelddadige criminaliteit zoals moord, afpersing, diefstal, zware aanvallen en gijzelingen. Tevens heeft het geleid tot het openen van nieuwe opsporingsonderzoeken.

Na het neerhalen van EncroChat in juni 2020, zijn veel gebruikers overgestapt naar het populaire Sky ECC platform (Europol, 2021d). Wereldwijd had het platform 170.000 gebruikers, waarvan 20% uit België en Nederland. Het platform had een eigen infrastructuur en applicaties die opereerden in de VS en Canada, met computerservers in Europa. Wereldwijd werden dagelijks drie miljoen berichten gedeeld via Sky ECC.

Niet veel later na Ennetcom volgde nog een succesvolle vergelijkbare operatie in maart 2021: de *takedown* van Sky ECC (Europol, 2021a). Vanaf medio februari 2021 hebben autoriteiten 70.000 gebruikers kunnen monitoren die gebruik maakten van Sky ECC. Dit leidde op 9 maart 2021 tot meerdere arrestaties en huiszoekingen in België en Nederland. Een internationale groep van opsporingsinstanties (België, Frankrijk en Nederland) hebben met hulp van Europol en Eurojust de communicatiedienst Sky ECC neergehaald. Na het neerhalen van Sky ECC was de strategie van het Operation Task Force Greenlight/Operation Trojan Shield om gebruikers te laten migreren naar het platform ANOM, het platform onder beheer van de FBI.[31]

[31] Zie voor meer informatie: https://www.europol.europa.eu/media-press/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication

Internationale samenwerking

Bij internationale opsporingsonderzoeken worden twee categorieën van zaken onderscheiden waarin encryptie een rol speelt (Europol & Eurojust Public Information, 2021). In het eerste type zaak gaat het om decryptie van de tool zelf. Dus de encryptie-tool die door criminelen wordt gebruikt is de focus van het onderzoek. Het tweede type zaak is een spin-off zaak, waar de focus ligt op andere aspecten dan encryptie, maar waarbij de ontsleutelde communicatie van criminelen wel nodig is als bewijs. Bijvoorbeeld verder onderzoek naar drugshandelzaken naar aanleiding van de EncroChat-berichten.

Coöperatie en coördinatie van verschillende landen is belangrijk, specifiek vanuit het technische en juridische perspectief. Er is internationale wetgeving aanwezig, maar er zijn verschillen in nationale juridische kaders van de EU-landen. Tevens zijn er andere juridische kaders buiten de EU. Dit kan zorgen voor een belemmeringen in het opsporingsproces. Er is dan ook steeds meer behoefte aan een geharmoniseerd juridisch kader op EU-niveau om online onderzoeken uit te voeren (Council of the European Union, 2016a, in EMCDDA & Europol, 2017). Het gebrek aan dergelijke harmonisatie beperkt de mogelijkheden om online criminele activiteiten te monitoren en rechtmatig kritieke bewijsstukken te verzamelen online. Aan de andere kant moeten deze juridische kaders er volgens Losavio en collega's (2019) tegelijkertijd voorkomen dat er een 'panopticon' maatschappij ontstaat waarbij de overheid bij de hele maatschappij mee kan kijken.

Er bestaat al een aantal manieren waarop internationaal wordt samengewerkt. Het is mogelijk om een JIT op te zetten als samenwerkingsverband (zie bijv. casus 2). Daarnaast kan Eurojust in dergelijke internationale samenwerkingen ondersteunen. Eurojust ondersteunt de justitiële coördinatie en samenwerking tussen nationale overheden in de strijd tegen terrorisme en zware georganiseerde misdaad waarbij meer dan één EU-land betrokken is. De fysieke locatie van Eurojust is Den Haag. Eurojust heeft bijvoorbeeld gefaciliteerd in de operatie van EncroChat.

Sinds 2016 wordt het EC3 Decryptie Platform gebruikt om meerdere opsporingsonderzoeken te ondersteunen (Europol & Eurojust Public Information, 2021). Vanaf 2020 is het nieuwe decryptie platform van Europol gestart, waardoor Europol meer capaciteit heeft om rechtmatig informatie te kunnen ontsleutelen. In casus 3 en 4 is internationale samenwerking belangrijk. Hoewel de link met encryptie in casus 4 minder aan de orde is, hebben we deze ingevoegd omdat daarin het aspect 'locatie' wordt belicht. In de toekomst zullen technologische ontwikkelingen elkaar blijven opvolgen, wat er voor pleit om in het juridische kader te anticiperen en te ontwikkelen op de toekomst (Losavio e.a., 2019).

Casus 3: Phantom Secure

Phantom Secure was een Canadese onderneming dat gemodificeerde Blackberries leverde, kortom cryptotelefoons. Op de telefoon was het mogelijk om met PGP-beveiliging te communiceren en om WhatsApp te gebruiken (Hartel & van Wegberg, 2021). Het bedrijf had 20.000 gebruikers. In tien jaar tijd heeft het bedrijf een winst van 80 miljoen dollar behaald (Europol & Eurojust Public Information, 2020b). In 2019 hebben Europol en Eurojust samengewerkt in Operation Icebreaker. Dit heeft geresulteerd in het aanhouden van de CEO en tevens in het ontmantelen van een internationale georganiseerde misdaadgroep, verantwoordelijk voor grootschalige drugshandel, sigarettenhandel, liquidaties en witwassen.

Casus 3 (vervolg): Phantom Secure

In totaal zijn honderd cryptotelefoons in beslag genomen. Uit een transcript tussen de voorgaande CEO van het bedrijf en een undercover FBI-agent blijkt dat Phantom Secure specifiek is ontwikkeld om drugshandel te faciliteren (Europol & Eurojust Public Information, 2020b). Het bedrijf faciliteerde met de telefoons moord en drugshandel in landen zoals VS, Australië, Mexico, Canada, Thailand en delen van Europa (Europol & Eurojust Public Information, 2020b).

Casus 4: AlphaBay en Hansa

AlphaBay was één van de grootste dark web marktplaatsen voor drugs (EMCDDA & Europol, 2017). Het had 200.000 gebruikers en 40.000 verkopers. Er is naar schatting voor 1 miljard Amerikaanse dollar verhandeld op het platform. Tevens werd geschat dat AlphaBay verantwoordelijk was voor 28% van alle drugsverkoop tussen 2015-2017. In 2017 werd AlphaBay offline gehaald door de FBI. Dat leidde er toe dat een groot deel van de gebruikers overstapten naar andere dark markets zoals Hansa Market. Hansa was in die tijd de op twee na grootste criminele marktplaats, vooral gericht op drugshandel. Dagelijks stapten 5.000 gebruikers over naar Hansa Market, maar deze marktplaats werd beheerd door de Nederlandse politie. Met operatie Bayonet heeft THTC toegang gekregen tot een server waarop Hansa Market draaide. In plaats van het offline halen van Hansa, heeft THTC in samenspraak met de FBI ervoor gekozen om deze voor één maand zelf te beheren. In de 27 dagen die volgden heeft de politie informatie verzameld over 27.000 transacties en data verzameld over 420.000 gebruikers, inclusief 10.000 huisadressen (EMCDDA & Europol, 2017).

3.3.3 De opbrengst van opsporingsonderzoeken

Uiteindelijk draait het in opsporingsonderzoek om bewijs. Zoals in de vorige sectie beschreven maakt Eurojust een onderscheid in twee categorieën van zaken waarin encryptie voorkomt, namelijk zaken waar decryptie van het technische hulpmiddel, dat door criminelen wordt gebruikt, de focus is van het opsporingsonderzoek, en de zogenoemde spin-off zaken. In een krantenartikel uit 2017 waarin wordt gesproken over in beslag genomen berichten van PGP-telefoons en servers wordt gesteld dat het OM ongeveer 3,6 miljoen berichten kon ontcijferen. Deze 'goudmijn aan informatie' zou een mokerslag voor de onderwereld kunnen betekenen.[32] Fukami en collega's (2021) stellen dan ook dat forensische analyse op encrypte apparaten ondertussen een essentiële opsporingsvaardigheid voor opsporingsinstantie is.

Encryptie kan dus in positieve en negatieve zin een rol spelen in de opbrengsten van een opsporingsproces. Hierbij kan qua bewijsvoering bijvoorbeeld worden gedacht aan het lokaliseren van relevante personen en goederen. Door het toenemende gebruik van encryptie, anonimisatietechnieken, cryptovaluta en het dark web kunnen opsporingsinstanties moeilijker informatie achterhalen over de fysieke locatie van een verdachte, de criminele infrastructuur of digitaal bewijs verzamelen (Europol & Eurojust Public Information, 2018). Bovendien zorgt het toenemende gebruik van cloud-dataopslag dat de data worden opgeslagen op fysieke locaties in andere rechtsgebieden. Het verlies van de locatie zorgt voor onzekerheid in de

[32] Beerekamp, H. (2017). *Waarom de waggie niet gevlamd is….* Verkregen via: https://www.nrc.nl/nieuws/2017/06/01/waarom-de-waggie-niet-gevlamd-is-10866041-a1561244

opsporingsbevoegdheden in verschillende rechtsgebieden. Juridische autoriteiten zoals Eurojust kunnen ondersteuning bieden.

In dezelfde lijn van redenering kan encryptie ook een rol spelen in de bewijsvoering aangaande het identificeren van relevante personen en goederen, het vaststellen van samenwerkingsverbanden en relaties en het signaleren van (mogelijke) criminele activiteiten. Hoewel encryptie in eerste instantie een verduisterende werking heeft hierop, ligt er zodra de encryptie is gekraakt of omzeild een schat aan waardevolle data c.q. mogelijke bewijslast. Om aan de toestroom van meldingen en data te voldoen, wordt de keuze welke verdachten nadere aandacht verdienen steeds belangrijker. Met de hoeveelheid beschikbare data is het ook mogelijk om criminele samenwerkingsverbanden en hun netwerken in kaart te brengen (Boerman e.a., 2017). Succesvolle operaties zoals SKY ECC, EncroChat en ANOM hebben voor een enorme hoeveelheid data gezorgd (Nationale Politie, 2021).

4. Resultaten

In dit onderzoek is eerst via zestien oriënterende interviews met negentien experts van de politie, het Openbaar Ministerie (OM) en het Nederlands Forensisch Instituut (NFI) in kaart gebracht of encryptie een rol speelt in de opsporing, en zo ja hoe die rol eruit ziet. Deze beelden zijn daarna aangevuld met enkele bevindingen uit de analyse van rechterlijke uitspraken en vragenlijstresultaten van 177 politiemensen die werkzaam zijn in de opsporing, en vervolgens verrijkt en verdiept met resultaten uit acht verdiepende interviews met experts van het OM (n=3) en de Rechtspraak (RM, n=5). Wanneer in de tekst wordt gesproken over 'respondenten' dan doelen we daarbij op de deelnemers aan de vragenlijst. In andere gevallen spreken we van 'geïnterviewden'. Om de anonimiteit van de deelnemers zo goed mogelijk te waarborgen, vermelden we geen gedetailleerde informatie van wie de quotes (interviews) of tekstovernames (vragenlijst) afkomstig zijn.

In dit hoofdstuk wordt eerst verkend welke toepassingen van encryptie zoal voorkomen, op welke wijze deze voorkomen en wat de ontwikkelingen op dit gebied zijn in de afgelopen vijf jaar (par. 4.1). Daarna gaan we in op het verloop van opsporingsonderzoeken waarin encryptie voor komt (par. 4.2) en de opbrengst ervan (par. 4.3). In sommige gevallen kan het zijn dat de gepresenteerde inhoud past in meerdere paragrafen of secties. Hierdoor kan soms sprake zijn van enige herhaling.

4.1 De aard van encryptie in opsporingsonderzoeken

Voordat we het kunnen hebben over de rol van encryptie in opsporingsonderzoeken is vooraleerst nodig te weten óf encryptie een rol speelt. Geïnterviewden geven aan dat encryptie iedere dag een rol speelt binnen de opsporing. In elke fase van een onderzoek loopt de politie tegen een vorm van encryptie aan. Dit loopt van de beginfase van een onderzoek, zoals bij taps, tot aan de eindfase bij bijvoorbeeld de in beslagname van gegevensdragers die versleuteld zijn. De prevalentie is volgens geïnterviewden sterk afhankelijk van type misdrijf (4.1.1), type toepassing (4.1.2) en type verdachte (4.1.3). Tot slot staan we stil bij de ontwikkelingen van encryptie in de afgelopen jaren (4.1.4).

Op basis van vragenlijstonderzoek onder 177 politiemensen die werkzaam zijn in de opsporing wordt duidelijk dat alle respondenten en/of hun team in de afgelopen vijf jaar met encryptie te maken hebben gehad. Sterker, 83,6% van de respondenten heeft veel of uitsluitend met dergelijke zaken te maken. Encryptie is gemeengoed in opsporingsonderzoeken. De vraag is dus niet of men er mee te maken heeft, maar wat de rol van encryptie inhoudt en wat dit betekent voor de opsporingspraktijk.

4.1.1 Type misdrijven en encryptie

De geïnterviewden vertellen dat encryptie vrijwel overal voorkomt; *"er zijn geen zaken met encryptie of zonder encryptie; encryptie is overal."* Tevens geven zij aan dat encryptie voorkomt in alle delicten waarbij gecommuniceerd wordt. Immers, bijna elke communicatiemiddel dat wordt gebruikt is tegenwoordig versleuteld; ook reguliere telefoongesprekken. Een geïnterviewde stelt verder: *"Bij een winkeldiefstal en geweldsdelicten waarschijnlijk niet, maar in alle misdrijven waar planning aan vooraf gaat komt wel encryptie voor."*

Van de respondenten die in hun werk met ondermijning te maken hebben (n=157) geeft 91% aan dat encryptie in de helft tot alle zaken een rol speelt. Voor high impact crime (HIC, n=110) is dat 73% en voor veelvoorkomende criminaliteit (VVC, n=72) 36%. Een respondent geeft in het kader van VVC – waar de rol van encryptie dus minder vaak wordt genoemd – aan: *"Binnen VVC zaken wordt encryptie niet eens aangeboden. Kost te veel tijd en capaciteit gezien de vele zaken die wij hebben en*

loont niet om dit te doen. Jammer, want vaak begint hier al de ondermijning…" Een rechter-commissaris (rc) geeft ook aan encryptie niet tegen te komen in VVC-zaken, maar vooral bij georganiseerde misdaad. Een andere geïnterviewde geeft aan dat encryptie wel voorkomt bij VVC, omdat het de meer gangbare en veel gebruikte vormen betreft, zoals WhatsApp en Signal, terwijl voor ondermijning *"men alles inricht met de gedachte 'dit alles moet zo snel mogelijk weg en niemand mag dit zien'."* Bij ondermijning is de belemmering van encryptie volgens deze, maar ook andere geïnterviewden, echter het grootst.

Ook andere geïnterviewden vertellen dat encryptie voornamelijk voorkomt in alle vormen van georganiseerde misdaad. Daarbij wordt aangegeven dat encryptie veelal wordt toegepast door criminele samenwerkingsverbanden die actief zijn op het gebied van verdovende middelen, en in iets mindere mate bij mensenhandel. Ook stuiten geïnterviewden naar eigen zeggen vaak op encryptie bij cybercrimezaken. Eén geïnterviewde zegt dat vooral in de midden-criminaliteit zoals ram- en plofkraken en gewapende overvallen de nadelige effecten van encryptie het grootst zijn, en minder bij de zware, georganiseerde criminaliteit. Tot slot komt encryptie volgens de geïnterviewden veel voor bij complexere kinderpornozaken en kindersekstoerisme, maar minder in andere typen zedenzaken. Ook milieuzaken worden genoemd als een type misdrijf waar encryptie minder voorkomt.

Wanneer we op kwantitatieve wijze inzoomen op type delicten dan zien we het volgende (tabel 4.1). Encryptie wordt het vaakst genoemd bij opsporingsonderzoeken naar georganiseerde criminaliteit, drugsmisdrijven, kinderporno en cybercrime in ruime en enge zin (i.e., gedigitaliseerde criminaliteit en cybercrime). Let op dat georganiseerde criminaliteit geen soort misdrijf is, maar een uitvoeringswijze. Veel drugsmisdrijven kunnen derhalve ook uit georganiseerde misdaad bestaan en andersom. Delicten waarin encryptie volgens respondenten nauwelijks een rol speelt, zijn milieucriminaliteit (overeenkomstig met bevindingen uit de interviews), verkeersdelicten en vandalisme/vernieling. Hierbij moet worden gelet op het geringe aantal respondenten dat met deze delictscategorieën te maken heeft in het dagelijks werk (respectievelijk n=11, n=5, n=11) en dus ook alleen deze vraag hebben beantwoord. Hierdoor kan een mogelijke vertekening zijn ontstaan. Ook dient rekening te worden gehouden met dat encryptie hier in de meest brede zin van het woord is uitgevraagd. De specifieke toepassingen van encryptie staan centraal in sectie 4.1.2.

Tabel 4.1: Soorten opsporingsonderzoeken waar dagelijks mee te maken en hoe vaak daarbinnen encryptie een rol speelt (N=177)

	Met welke ops.onderz. dagelijks te maken (Let op: encryptie hoeft geen rol te spelen)		**Hoe vaak speelt encryptie een rol in deze soorten opsporingsonderzoeken** (% van personen die hebben aangegeven hier dagelijks mee te maken hebben gehad)				
Delict	% Ja	N ja	Nooit	Weinig	Niet weinig/ niet veel	Veel	Altijd
Drugsmisdrijven	73,4	130	0%	2,3%	5,4%	62,3%	30,0%
Georganiseerde criminaliteit	72,9	129	0%	0,8%	2,3%	51,2%	45,7%
Levensdelicten (bijv. doodslag en (poging tot) moord)	54,8	97	3,1%	8,2%	22,7%	51,5%	14,4%
Wapendelicten (bijv. wapenbezit en -handel)	49,7	88	1,1%	6,8%	21,6%	52,3%	18,2%

Noot. Aflopend gesorteerd op hoe vaak respondenten dagelijks met de delicten te maken hebben.

Tabel 4.1 (vervolg): Soorten opsporingsonderzoeken waar dagelijks mee te maken en hoe vaak daarbinnen encryptie een rol speelt (N=177)

	Met welke ops.onderz. dagelijks te maken (Let op: encryptie hoeft geen rol te spelen)		**Hoe vaak speelt encryptie een rol in deze soorten opsporingsonderzoeken** (% van personen die hebben aangegeven hier dagelijks mee te maken hebben gehad)				
Delict	% Ja	N ja	Nooit	Weinig	Niet weinig/ niet veel	Veel	Altijd
Geweldsdelicten (bijv. mishandeling, bedreiging en stalking)	44,1	78	2,6%	16,7%	25,6%	46,2%	9,0%
Vermogensdelicten (bijv. diefstal, inbraak en fraude/bedrog)	40,1	71	9,9%	0%	22,5%	62,0%	5,6%
Gedigitaliseerde criminaliteit (IT slechts als middel) (bijv. online oplichting)	33,3	118	0%	5,1%	18,6%	59,3%	16,9%
Cybercrime (IT zowel doel als middel) (bijv. hacken en DDoS-aanval)	22,6	40	0%	2,5%	10,0%	52,5%	35,0%
Seksuele misdrijven / zeden	11,9	21	0%	9,5%	28,6%	61,9%	0%
Kinderporno	10,2	18	0%	0%	11,1%	61,1%	27,8%
Vandalisme / vernieling	6,2	11	0%	45,5%	27,3%	27,3%	0%
Milieucriminaliteit	6,2	11	9,1%	36,4%	36,4%	18,2%	0%
Verkeersdelicten (bijv. verlaten plaats ongeval en rijden onder invloed)	2,8	5	40,0%	20,0%	20,0%	20,0%	0%

Noot. Aflopend gesorteerd op hoe vaak respondenten dagelijks met de delicten te maken hebben.[33]

In onze analyse van rechterlijke uitspraken van zaken waarin encryptie een rol speelt, komen relatief vaak druggerelateerde zaken naar voren. Zaken hebben betrekking op smokkel, invoer, handel en bezit van drugs zoals cocaïne, heroïne en ketamine. Daarna komt witwassen het meeste voor, zowel als een op zichzelf staand delict als in combinatie met andere criminaliteitsvormen. In interviews met rechters en rc'en kwamen bovengenoemde zaken ook meermaals naar voren. Een rechter geeft aan dat encryptie voorkomt in *"alles wat in georganiseerd verband is gebeurd."* Deze rechter stelt ook: *"De 'gewone' drugsdealer is minder bezig met het beveiligen van zijn computer en maakt vaak gebruik van een gewone telefoon."* Zaken die niet in de analyse van rechterlijke uitspraken naar voren komen, maar wel in de interviews zijn besproken betreffen: online bedreigingen en opruiïngen via internet.

Kinderpornozaken en cybercrime komen ook voor in de zaken die we geanalyseerd hebben van Rechtspraak.nl, maar in mindere mate. Een rc geeft aan dat ten opzichte van een aantal jaar geleden de frequentie van encryptie in kinderpornozaken aan het afnemen is, of in ieder geval dat het minder als probleem wordt ervaren in strafzaken. Dat kan volgens de rc met meerdere facetten te

[33] In de interviews is gevraagd in hoeverre cryptovaluta in dit verband een rol speelt. De geïnterviewden geven aan cryptovaluta wel tegen te komen in hun opsporingswerkzaamheden, maar ook dat het volgens hen niet noemenswaardig is, omdat zij hier niet een directe link met encryptie zien. Om die reden is cryptovaluta buiten de vragenlijst gehouden.

maken hebben, zoals minder prioriteit van de politie of dat daders denken 'het helpt niet' of 'ze komen er toch doorheen'. Hij stelt verder dat vroeger het NFI bij wijze van spreken tien jaar bezig was om in een kinderpornozaak de encryptie te kraken, terwijl dat al lang niet meer zo is. De politie en NFI hebben zich daarin ontwikkeld, terwijl de methoden die door verdachten gebruikt worden, zoals databestanden opslaan in een veilige map met wachtwoord en cryptocontainers, niet vooruit zijn gegaan.

4.1.2 Type toepassingen van encryptie

Nu we weten in welke opsporingsonderzoeken encryptie een rol speelt, kijken we naar wat voor toepassingen van encryptie worden gebruikt. De toepassing van encryptie wordt door geïnterviewden in verschillende typen verdeeld. Op hoofdlijnen betreft het stromende data en opgeslagen data. Daarnaast spreekt men over het (i) versleutelen van communicatie, (ii) versleutelen van hardware en data, (iii) versleutelen van onlinediensten en (iv) het verhullen van digitale locaties. Hieronder vallen weer verschillende toepassingen van encryptie.

In tabel 4.2 staat een overzicht met deze toepassingen zoals in de survey bevraagd. De vijf meest voorkomende toepassingen die respondenten in hun werk tegenkomen zijn: versleutelde mobiele telefoons (88,1%), versleutelde chatdiensten (81,3%), versleutelde devices, anders dan mobiele telefoons (68,9%), versleutelde berichtendiensten (67,3%) en crypto-telefoons (65,0%). De dagelijkse frequentie van het voorkomen van encryptie in de opsporing is dus voor een belangrijk deel toe te schrijven aan inbeslaggenomen mobiele telefoons. Een geïnterviewde politiemedewerker geeft aan dat in beslag genomen telefoons in 90-95% van de gevallen versleuteld zijn.

Tabel 4.2: Toepassingen van encryptie in opsporingsonderzoeken (N=177)

Toepassing encryptie	Niet	Weinig	Niet weinig/ niet veel	Veel	Altijd	Weet niet/ ken ik niet
Versleutelde communicatie (end-to-end-encryptie)						
Versleutelde chatdiensten (bijv. Telegram, Signal, WhatsApp)	4,5%	5,1%	7,3%	41,8%	39,5%	1,7%
Versleutelde berichtendienst (bijv. Sky ECC, PGP)	9,6%	6,8%	14,7%	55,4%	11,9%	1,7%
Crypto-telefoons (bijv. Ennetcom, EncroChat)	8,5%	9,0%	15,8%	53,7%	11,3%	1,7%
Versleutelde maildiensten (bijv. ProtonMail)	17,5%	33,3%	22,0%	15,8%	2,8%	8,5%
Versleutelde hardware en data						
Versleutelde mobiele telefoons (bijv. met pincode, gezichtsherkenning)	4,5%	1,7%	4,0%	49,7%	38,4%	1,7%
Versleutelde devices, anders dan mobiele telefoons (bijv. laptop en desktop comp.)	4,0%	7,9%	17,5%	52,5%	16,4%	1,7%
Versleutelde gegevensdragers (bijv. usb-sticks, harde schijf)	4,0%	16,9%	33,3%	38,4%	5,1%	2,3%
Cryptocontainers (versleutelde data) (bijv. met VeraCrypt, BitLocker)	10,7%	35,6%	21,5%	19,8%	1,7%	10,7%

Tabel 4.2 (vervolg): Toepassingen van encryptie in opsporingsonderzoeken (N=177)

Toepassing encryptie	Niet	Weinig	Niet weinig/ niet veel	Veel	Altijd	Weet niet/ ken ik niet
Versleutelde onlinediensten						
Sociale media (bijv. wachtwoordbeveiliging)	4,5%	13,0%	20,3%	44,1%	11,9%	6,2%
Versleutelde cloudopslag	11,3%	24,3%	27,7%	20,3%	1,7%	14,7%
Bulletproof hosting	18,6%	20,3%	12,4%	11,3%	0,6%	36,7%
Tools voor verhullen digitale locaties (IP-adres)						
VPN (Virtual Private Network)	7,9%	22,0%	16,9%	27,7%	6,2%	19,2%
Tor (The Onion Router)	13,6%	28,2%	15,8%	17,5%	2,8%	22,0%

In tabel 4.2 valt verder op dat social media accounts zijn benoemd. Sociale media accounts hebben veelal geen end-to-end encryptie (E2EE), maar zijn wel versleuteld met een wachtwoord. Door geïnterviewden wordt anders gedacht over het wel of niet onder encryptie scharen van dit type beveiliging (zie ook par. 5.1). Dit geldt ook voor de toepassing van bijvoorbeeld biometrie, VPN en Tor. De belangrijkste reden om deze wel uit te vragen is dat het door geïnterviewden werd genoemd in relatie tot encryptie. Tot slot kan een opmerking worden geplaatst bij de gehanteerde voorbeelden. In sommige gevallen passen de voorbeelden onder meerdere toepassingsvormen. Ter illustratie, EncroChat kan worden gezien als een aanbieder van versleutelde berichtendiensten, maar ook als een aanbieder van cyptotelefoons (waarmee versleutelde berichten kunnen worden verstuurd). Waar geen discussie over lijkt te zijn betreft het doel dat met encryptie wordt nagestreefd; het afschermen of verhullen van informatie.

Om geen toepassingen van encryptie te missen, hebben we respondenten gevraagd welke toepassingen zij in hun werk nog meer tegenkomen. Twee respondenten noemen de toepassing van https (d.w.z. gebruik van TLS om webverkeer te beveiligen). Toepassingen die eenmaal worden genoemd omvatten Tails of soortgelijke besturingssystemen (waarbij de respondent benoemt dat dit weinig voorkomt), versleutelde (lokale) databases, gebruik van virtuele machines (waarbij de respondent aangeeft dat dit mogelijk onder cryptocontainers kan vallen) en cryptovaluta ‘wallets’. Door een geïnterviewde werd tot slot aangegeven dat nog een eenvoudige manier van encryptie wordt gebruikt, namelijk ‘Bargoens’; een sociale taalvariatie. Met Bargoens wordt een ‘geheimtaal’ gebruikt waarmee verdachten communiceren.

Rechters en rc’en geven in interviews aan met de volgende toepassingen van encryptie in aanraking te komen in strafzaken: cloudopslag, Signal, Telegram, WhatsApp, dark web (kinderporno), BitLocker, Tor (illegale dark web handelsplaatsen) en smartphones met pincode of gezichtsherkenning. ProtonMail ziet men ook terug in zaken, vooral bij drugshandel, wapenzaken, zedenzaken en terrorismeverdenking, maar in mindere mate. Ook ziet men in mindere mate bulletproof hosting voorbij komen in zaken. Dit komt bijvoorbeeld voor in zaken die gaan over het aanbieden van criminele diensten en het opslaan van bestanden met data van gestolen creditcards. Volgens geïnterviewden uit de oriënterende fase wordt bulletproof hosting voornamelijk toegepast bij het plegen van cybercrime.

Om te onderzoeken of toepassingen juist vaker of minder vaak voorkomen bij bepaalde type delicten is een correlatietabel gemaakt tussen het type criminaliteit waarmee opsporingsmedewerkers aangeven dagelijks te maken te hebben en de toepassingen waarmee zij te maken hebben in hun

opsporingsonderzoek. De toepassingen van cryptotelefoons en versleutelde berichtendiensten (bijv. Ennetcom en EncroChat) komen vaker voor bij drugsmisdrijven, georganiseerde criminaliteit en wapendelicten en juist minder bij seksuele misdrijven/zeden en kinderporno (en versleutelde berichtendiensten bij vandalisme). Cryptocontainers komt men daarentegen vaker tegen bij opsporingsonderzoeken naar vermogensdelicten, cybercrime en milieucriminaliteit. Versleutelde gegevensdragers komen vaker voor in kinderpornozaken. Verder blijken versleutelde chatdiensten, versleutelde mobiele telefoons[34], versleutelde devices, bulletproof hosting en Tor niet vaker of minder vaak als toepassing bij een bepaald type delict voor te komen. In bijlage VI (tabel VI.1) staat een overzicht van deze correlaties.

4.1.3 Type verdachten en encryptie

Encryptie is tegenwoordig alom aanwezig in allerlei producten en diensten die door bedrijven en burgers gebruikt worden. Daarnaast zijn er encryptiediensten die volgens geïnterviewden voor 99% enkel door criminelen worden gebruikt, zoals cryptotelefoons. In de interviews merkten we dat een aantal geïnterviewden de aard van encryptie classificeert in twee categorieën, namelijk technologie-gedreven encryptie (ook wel *encryption-by-design* genoemd) en mens-gedreven encryptie (ook wel *encryption-by-choice* genoemd). Let op dat dit geen wetenschappelijke definitie is of wederzijds uitsluitende categorieën zijn; het is hoe verschillende politiemensen het in interviews beschouwen.

Onder technologie-gedreven encryptie verstaan geïnterviewden dat encryptie standaard is verwerkt in de technologie. Hierbij kan gedacht worden aan Over-The-Top (OTT) communicatiediensten, zoals WhatsApp en Telegram, maar ook aan vingerafdrukbeveiliging en gezichtsherkenning op mobiele telefoons (biometrie). Een geïnterviewde geeft aan dat deze vorm over het algemeen het meest voorkomt in opsporingsonderzoeken en dat het gebruik ervan veelal onbewust is. Technologie-gedreven encryptie wordt steeds vaker gebruikt door criminelen om minder op te vallen, voornamelijk wanneer bedrijven achter die diensten zitten die niet of nauwelijks bereid zijn om informatie te delen met de overheid. Ook minder technisch onderlegde criminelen en/of beginnende criminelen maken volgens geïnterviewden (onbewust) gebruik van technologie-gedreven encryptie. Wel hangt een en ander volgens geïnterviewden samen met het type dader; wel of geen affiniteit met technologie.

"Op het moment dat een doorzoeking plaatsvindt in een 'huis-, tuin- en keukenzaak', zul je altijd verschillende digitale gegevensdragers aantreffen, maar om daar binnen te komen en om de encryptie te omzeilen of te ontsleutelen, dat is daar doorgaans geen probleem; in de meeste gevallen lukt het wel. Op het moment dat je een crimineel hebt die digitaal onderlegd is, is het anders." De betreffende OvJ benoemt daarbij dat er gevallen zijn waar mensen geen wachtwoord op de computer hebben. *"Bij een cybercrimineel zie je dat absoluut niet."* Tevens geeft hij aan dat in de toekomst de meeste mensen wellicht beter digitaal onderlegd zullen zijn, en dat in die zin encryptie mogelijk lastiger wordt. Aan de ander kant benoemt hij dat de opsporing en vervolging zich ook verder zullen ontwikkelen.

Mens-gedreven encryptie wordt door geïnterviewden beschreven als encryptie die bewust door een persoon wordt toegepast of ingesteld, bijvoorbeeld op een device, applicatie of online

[34] Een mogelijke oorzaak dat mobiele telefoons niet sterk correleren – wat misschien wel verwacht zou worden – kan zijn dat Operationeel Specialisten die zich met meerdere type delicten bezighouden, ook op meerdere delicten 'ja' hebben geantwoord. Daarmee zouden (mogelijke) correlaties getroebleerd kunnen zijn.

omgeving. Mens-gedreven encryptie zou veelal ingezet worden om iets bewust te verhullen, heimelijk op te slaan of te gebruiken. Een geïnterviewde zegt hierover: "*De slimmere [verdachten] zijn andere types. Ze zijn scherper; in het beveiligen van data, maar ook bijvoorbeeld met toestemming geven. De minder slimme types hebben zoiets van 'we worden toch wel een keer gepakt' en werken ook eerder mee met het politieonderzoek.*" Mens-gedreven encryptie wordt door geïnterviewden dan ook beschouwd als indicatie van verdachte activiteiten: "*Mensen die willens en wetens met verkeerde dingen bezig zijn, zijn over het algemeen bewust met encryptie bezig.*" Een andere geïnterviewde geeft aan: *"Als er 70 normale telefoons in beslag genomen worden en twee encrypted telefoons, dan leggen we de focus op de versleutelde telefoons."* Ook een respondent zegt hier iets over: *"Encryptie zegt in onze tak van sport meestal wat over de mate waarin mensen wat te verbergen hebben."*

Een belangrijke opmerking die wij willen maken is dat politiemensen de rol van mens-gedreven encryptie uitleggen in de context van het onderzoek, waarbij bewijsgaring en de criminele toepassing van encryptie centraal staat. Wij willen niet de indruk wekken dat wij de verbinding tussen encryptiegebruik en criminaliteit leggen. Immers, niet iedereen die gebruik maakt van Telegram, Tor of Signal is meteen een verdachte. Dit zijn net zo goed individuen die heel bewust omgaan met hun privacy. Een respondent benoemt dit ook: *"[…] encryptie wordt voor 99% gebruikt voor legitieme doeleinden."* Het bewust toepassen van encryptie komt volgens een geïnterviewde relatief weinig voor en hij schat in dat dit in ongeveer 5% van de zaken een rol speelt. Bovendien is volgens een OvJ vaak ook al sprake van een verdenking op het moment dat daar zo over wordt gedacht.

4.1.4 Ontwikkelingen van encryptie in opsporingsonderzoeken in de afgelopen vijf jaar

Vrijwel alle geïnterviewden – zowel in de oriënterende als verdiepende fase – zeggen dat de aard en toepassing van encryptie in de opsporing in de afgelopen vijf jaar is veranderd en dat het gebruik ervan is toegenomen. Respondenten op de vragenlijst geven ook aan dat volgens hen de frequentie waarmee zij in hun team te maken hebben met encryptie in de afgelopen vijf jaar is toegenomen (88,7%). Ongeveer een op de twintig politiemensen geeft aan dit niet te weten (5,6%) of dat de frequentie (vrijwel) gelijk is gebleven (5,1%). Eén respondent gaf aan dat de frequente is afgenomen.

Een exacte uitspraak over omvang of frequentie kunnen geïnterviewden niet geven. Daarnaast zeggen geïnterviewden dat de omvangvraag niet alleen moeilijk is te beantwoorden, maar dat die vraag ook minder relevant is. Een belangrijkere vraag is volgens hen: *"Hoe vaak is het echt een probleem als je bijvoorbeeld niet in een telefoon of laptop kunt komen? Stel je voor dat er vier devices in beslag genomen worden. Als het bij drie devices lukt om binnen te komen, en bij de vierde niet, is het dan een probleem?"* We vroegen OvJ's hierop door en een van het zei: *"Je kan er niet bij, dus je hebt geen idee wat erop staat. Je moet het doen met de drie telefoons die je wel hebt en de rest. Of dat genoeg is hangt af van wat je hebt en je weet nooit wat op die andere gestaan heeft."* Een andere OvJ stelt dat er van tevoren een verdenking is van een strafbaar feit. Als informatie uit die drie devices daaraan ondersteunend is, dan maakt het minder uit wat er op de vierde staat. Waarbij wel een kanttekening wordt gemaakt dat daardoor het beeld wellicht completer zou zijn en mogelijk andere strafbare feiten aan het licht waren gekomen. Deze OvJ kan zich geen zaken heugen waardoor in een dergelijk geval sprake was van te weinig bewijs.

In sommige gevallen kunnen wat specifiekere aantallen worden genoemd over de omvang. Het Voorziening Crypto Analyse Team (VCAT) richt zich met name op opsporingsonderzoeken waar cryptotelefoons een rol spelen. Sinds 2016 speelt encryptie een rol in hun opsporingsonderzoeken.

Het startpunt voor dit team betreft enkele hoofdonderzoeken, maar daaruit rollen wel vele verschillende deelonderzoeken. Ten tijde van het interview zijn de inzichtelijk gemaakte data in 1.200 tot 1.300 strafrechtelijke onderzoeken gebruikt. Naar eigen zeggen komen er elke week/maand meerdere onderzoeken bij.

Ook rechters en rc'en geven aan dat encryptie in toenemende mate aanwezig is in strafzaken. Een rechter geeft aan vijf jaar geleden nog niet met encryptie in zaken in aanraking te zijn gekomen, althans niet zoals het nu voorkomt. Deze rechter verwacht dat er nog veel zaken zullen volgen waarin encryptie een rol speelt. Een rc zegt dat het is verveelvoudigd. En dat betreft niet de standaard encryptie zoals bij WhatsApp, maar bewust toegepaste encryptie, zoals PGP, Ennetcom en de opvolgers daarvan.

Twee gebeurtenissen zijn volgens verschillende geïnterviewden van invloed geweest op een verandering in de toepassing van encryptie in de opsporing. Twee geïnterviewden beschrijven dat de onthullingen door Snowden in 2013 over de gebruikte surveillancetechnieken van de NSA in de VS hebben geleid tot een vergrote bewustwording van Nederlanders over de hoeveelheid en de manier waarop overheidsdiensten informatie kunnen verzamelen.

Daarnaast zou ook de bekendmaking van door de politie verkregen toegang tot cryptodiensten effect hebben gehad op de manier waarop criminelen encryptie zijn gaan gebruiken. Hierbij kan gedacht worden aan toegang tot communicatie via BlackBerry, en meer recent Ennetcom, EncroChat en Sky ECC. Criminelen zijn nadat de politie toegang kreeg tot data van cryptotelefoons minder centraal op één platform gaan communiceren, maar verspreiden hun communicatie meer, aldus politiemensen. Zo constateren zij bijvoorbeeld dat criminelen via de ene communicatiedienst een bericht sturen waarna door de andere partij via een andere communicatiedienst geantwoord wordt. Hierdoor heeft de politie maar de helft van de informatie wanneer ze één van de twee diensten ontsleutelt. Dit maakt het voor de politie moeilijker om in één keer een grote slag te slaan. Een OvJ ziet dat vooral bepaalde chatdiensten worden gebruikt, omdat chats niet worden opgeslagen en e-mails wel.

Daarnaast zijn er trends op technologisch gebied die in de afgelopen jaren effect hebben gehad op de aard van encryptie. Twee politiemensen noemen bijvoorbeeld de opkomst van *dedicated security chips*, zoals de Trusted Platform Module (TPM). TPM is een chip in de computer, waarmee encryptiesleutels, gebruikersgegevens en andere gevoelige data beveiligd kunnen worden. Constante technologische ontwikkelingen maken het steeds lastiger om versleutelde systemen te kraken. *"Om de slagingskans te vergroten heeft de politie veel rekenkracht nodig in combinatie met technische aanwijzingen. Bij moderne versleuteling wordt dit een lastige opgave."*

Verder wordt sinds de opkomst van biometrische gegevens (zoals vingerafdruk- en irisherkenning) een andere vorm van encryptie toegevoegd, en is de omvang van encryptie vergroot door de opkomst van deze 'technologie-gedreven' encryptie. Vrijwel iedereen die dit soort applicaties gebruikt, maakt immers ook standaard gebruik van encryptie. De data achter deze technologie-gedreven encryptie zijn lastig te verkrijgen, omdat grote commerciële bedrijven (zoals Google en Meta) volgens de geïnterviewden steeds vaker weigeren informatie te delen met de overheid, of enkel toegang geven tot metadata.[35] Dit onderwerp komt uitgebreider aan bod in de komende paragrafen.

[35] Metadata zijn "gegevens die de eigenschappen van andere gegevens beschrijven. Bijvoorbeeld van wie de gegevens zijn, of wie ze verstuurd heeft, of wanneer ze voor het laatst gewijzigd zijn" (Cybersecurity Alliantie & Cyberveilig Nederland, 2021, p.49).

In navolging van het voorgaande, delen interviewkandidaten hun observatie dat het toepassen van encryptie gebruiksvriendelijker wordt en integraal onderdeel uitmaakt van installatieprocessen. Een geïnterviewde illustreert dit als volgt: *"bij de installatie van een nieuwe Windows-versie is er een menu om bijvoorbeeld BitLocker aan te zetten. De gebruiker merkt hier niet veel van. Eerst was het een operatie waar je technische kennis voor nodig had en het is nu dat sommige mensen niet eens weten dat ze het hebben, terwijl de impact even groot is."* Of zoals een andere geïnterviewde beschrijft: *"Encryptie is standaard geworden. Ik ben begonnen in 2007. Als je toen keek naar internettap dan was grootste gedeelte van tap leesbaar en nu is het grootste gedeelte versleuteld."*

Een van de rechters, alsook een OvJ, die we hebben geïnterviewd wijdt de vlucht van encryptie meer aan technologische ontwikkelingen an sich. *"Lang geleden was er een tijd waarin de politie er aan dacht om bij elk aangehouden persoon de telefoon te bekijken. Daar werd veel verweer tegen gevoerd, en terecht denk ik. Het is nu meer afgebakend wat wanneer mag en wie er toestemming voor moet geven. Dat is ook een ontwikkeling van de laatste 10-15 jaar. Ik denk dat de politie de laatste 10 jaar meer inzet op digitaal rechercheren van computers en harde schijven en dat daar meer bewijs uit voorkomt, ongeacht of het encrypted is."* De OvJ zegt dat vanaf de invoering van mobiele telefoons encryptie een 'steeds grotere vlucht neemt' binnen opsporingsonderzoeken. *"Sinds de invoering van de mobiele telefoon en internettap […] rond 2008-9, zie je steeds meer informatie standaard versleuteld worden door degene die de informatie laat verzenden of verzendt, waarbij het voor opsporingsteams steeds moeilijker wordt gedurende de heimelijke opsporing om toegang te krijgen tot de inhoudelijke informatie, namelijk in de tap. En dat zien we op dit moment ook steeds sterker in de fase van de niet-heimelijke opsporing, dus na beslag."*

Een toekomstige verandering, die al deels gaande is, ziet een politiemedewerker op het gebied van encryptie aankomen. Op moment van het interview kan de politie de locatie van een mobiele telefoon vrij precies achterhalen door gebruik te maken van een IMSI-catcher.[36] Met een IMSI-catcher kan een IMSI-nummer worden opgevraagd en daarmee de locatie worden achterhaald. Een IMSI-nummer is een nummer gekoppeld aan het 06-nummer c.q. de simkaart. De politie heeft in theorie de mogelijkheid om met een IMSI-catcher communicatie af te luisteren, maar dit is bij wet verboden. Criminelen die zich een IMSI-catcher kunnen veroorloven kunnen wel communicatie afluisteren. Op de korte termijn wordt lokalisatie en identificatie ingewikkelder voor de politie. Met de komst van 5G (het 5^{e} generatie mobiele netwerk) vervalt het gebruik van het IMSI-nummer en wordt meer encryptie toegepast. Daarmee is het voor de politie niet meer mogelijk om middels de IMSI een precieze locatie vast te stellen, waardoor ook het identificeren van personen nog lastiger gaat worden. Een voordeel is dat het voor criminelen ook moeilijker wordt om communicatie af te luisteren.

Wat betreft het ontsleutelen van data, vertellen politiemensen dat de encryptie zelf niet per se beter is geworden, maar dat de sleutel steeds beter wordt en beter wordt verstopt. Hierdoor is informatie, bijvoorbeeld bij internettaps, minder inzichtelijk voor de politie. Een andere geïnterviewde zegt echter dat er geen duidelijke verandering zichtbaar is: *"Ik werk nu vijf jaar bij de politie en binnen die jaren kwamen we het [encryptie] vanaf het begin al tegen, het verandert niet. […] Tor zagen we altijd al, VeraCrypt en TrueCrypt zien we ook. Luks is denk ik wel nieuwer, dat heeft meer te maken met dat verdachten vooral op Windows zaten maar we zien nu verdachten die op Linux bezig zijn. Daar lijkt een verschuiving in te zitten."*

[36] IMSI staat voor International Mobile Subscriber Identity.

Een andere verandering die geïnterviewden zien is dat de politie vóór het ontsleutelen van Ennetcom en PGP 2.0 kansloos was. Toen konden alleen 'reguliere' telefoons ontsleuteld worden en was het intelligencebeeld fragmentarisch. Sinds de toegang tot verschillende cryptodiensten, is er meer een totaaloverzicht van criminele netwerken. Dit zegt vanzelfsprekend meer over de interne ontwikkelingen binnen de politie (opsporingsmethoden), dan over de aard van encryptie. Het is echter de vraag in hoeverre deze ontwikkeling blijft. Immers, criminelen lijken zich hier ook in toenemende mate bewust van te zijn.

De toekomstige ontwikkeling van kwantumencryptie zal naar de verwachting van een geïnterviewde de rol van encryptie in de opsporing doen veranderen. Het beveiligen van informatie en communicatie is hedendaags relatief eenvoudig met gebruiksvriendelijke technologie, maar hij verwacht dat deze encryptie makkelijk te kraken is zodra kwantumcomputers zijn geïntroduceerd.[37] Tevens verwacht hij dat *'kwantumcomputing-as-a-service'* aangeboden zal worden. Defensief zou dat kunnen leiden tot het kraken van communicatie bij de politie. Offensief gezien zal de politie waarschijnlijk geen beschikking hebben over kwantumcomputers in de beginfase. De politie zal het technisch kraken van kwantumencryptie moeten uitbesteden. Dit kan leiden tot problemen op juridisch vlak en in de architectuur (om iets offshore te ontgrendelen en veilig terug te krijgen).

4.2 Encryptie en het verloop van opsporingsonderzoeken

Wat de rol van encryptie is in het verloop van opsporingsonderzoeken wordt in deze paragraaf toegelicht. In dit onderzoek wordt met 'verloop' gedoeld op de slagingskans om binnen opsporingsonderzoeken encryptie te kraken, te omzeilen of alternatieve opsporingsmiddelen in te zetten. Maar ook wat dit betekent in termen van de inzet van mensen en middelen, zoals doorlooptijd, menskracht, expertise en de aanschaf van soft-/hardware.

4.2.1 Factoren die van invloed zijn op het verloop van opsporingsonderzoeken

We vroegen de respondenten welke rol encryptie speelt in het verloop van opsporingsonderzoeken, zie tabel 4.3 op de volgende pagina. Wat volgens hen in meer dan de helft van de gevallen veel of altijd een rol speelt zijn de betrouwbaarheid van gevonden data, de kans op het vinden van aanknopingspunten voor nieuwe zaken en mogelijkheden om verdachten aan te dragen bij het OM.

Op de vraag in hoeverre encryptie een rol speelt in het verloop van opsporingsonderzoek wordt in de interviews verschillend gereageerd. Enerzijds speelt encryptie een belemmerende of negatieve rol, omdat het door criminelen gebruikt wordt om uit het zicht van opsporingsdiensten te blijven. Criminelen kunnen bijvoorbeeld met anonieme communicatienetwerken, zoals het Tor-netwerk, hun IP-adres verhullen en hun communicatie afschermen met satelliettelefoons en encrypte applicaties zoals Telegram en WhatsApp. Een respondent zegt hierover het volgende: *"Het gebruik door criminelen is toegenomen, hierdoor is steeds minder inzichtelijk waar zij zich mee bezig houden."* Een andere respondent geeft aan: *"Encryptie is gebleken een enorme invloed te hebben op opsporingsonderzoeken in de afgelopen jaren. Het bemoeilijkt opsporingsonderzoeken. Alleen specialistische teams zijn in staat bij de berichten te komen. Dat is niet voor elk team weggelegd."*

[37] Kwantumcomputers zijn computers die informatie opslaan en bewerken "door de eigenschappen te gebruiken van deeltjes die nog kleiner zijn dan een atoom. De kwantumcomputer kan heel veel sneller rekenen dan gewone computers" (Cybersecurity Alliantie & Cyberveilig Nederland, 2021, p.46).

Tabel 4.3: Rol encryptie in het verloop van opsporingsonderzoeken (N=177)

	Niet	Weinig	Niet weinig/ Niet veel	Veel	Altijd	Weet niet
De betrouwbaarheid van gevonden data	0,6%	4,5%	26,6%	23,7%	33,3%	11,3%
De kans op het vinden van aanknopingspunten voor nieuwe zaken (restinformatie)	2,8%	10,2%	18,1%	28,2%	32,8%	7,9%
De mogelijkheden om verdachten aan te dragen bij het OM	2,3%	15,8%	22,0%	26,0%	24,9%	9,0%
De kans om een zaak succesvol af te ronden	1,7%	24,3%	23,2%	19,8%	24,3%	6,8%
De kans om een opsporingsonderzoek voort te zetten	2,3%	23,2%	32,8%	21,5%	11,3%	9,0%
De inzet van middelen	5,1%	22,0%	32,2%	20,3%	10,7%	9,6%
De doorlooptijd van een opsporingsonderzoek	10,2%	44,1%	14,7%	12,4%	11,3%	7,3%
De inzet van mensen (capaciteit)	6,2%	33,3%	31,6%	11,3%	9,0%	8,5%

Nagenoeg alle apparaten en digitale communicatie zijn tegenwoordig encrypted (o.a. vingerafdruk, patronen, pincodes, gezichtsherkenning en E2EE). Dit maakt het voor de politie bijvoorbeeld arbeidsintensiever om in de communicatie van (mogelijke) verdachten te komen. Hierdoor mist de politie potentieel veel interessante informatiebronnen. Een respondent illustreert dit als volgt: *"Door encryptie mist er vaak essentiële informatie. Informatie die nodig is om voldoende bewijs aan te leveren. Daardoor heeft encryptie een negatieve rol in opsporingsonderzoeken."*

De respondenten op de vragenlijst dragen vooral aan dat encryptie zijn weerslag kent op de inzet van expertise, capaciteit en doorlooptijd. Ter illustratie: *"Logischerwijs beperkt encryptie de (snelle of zelfs gehele) toegankelijkheid tot potentieel cruciale informatie/bewijs. Dit vergt investering in (specialistische) capaciteit, zowel in- als externe (Team/TDO/NFI/extern)[38] […]. Daarnaast vertaalt het zich veelal in langere doorlooptijden."* Een andere respondent gaat in op de beschikbare tools: *"Zet meer in op betaalde tools die we kunnen gebruiken binnen bijvoorbeeld OSINT onderzoeken i.c.m. forensische onderzoeksoftware.[39] Een politieagent stuur je ook niet de straat op zonder vuurwapen en handboeien, internetrechercheurs moeten eigenlijk alles met gratis tools doen terwijl daar veel winst te behalen valt."*

Wanneer geen toegang verkregen wordt tot een digitale bron, is de kans groot dat tevens geen toegang verkregen wordt tot alternatieve digitale bronnen omdat deze hoogstwaarschijnlijk ook versleuteld zullen zijn. Het onderscheppen van communicatie is in sommige gevallen zelfs onmogelijk volgens een geïnterviewde. Een respondent zegt hierover: *"Heel veel [bij mensenhandel/uitbuiting] gaat middels WhatsApp. Slachtoffers moeten berichten wissen, medeverdachten worden niet of nauwelijks bekend. Niet te tappen, waardoor we veel missen."*

De opsporing is hierdoor steeds afhankelijker van het begin- en eindpunt van de communicatie. Dit leidt ertoe dat het binnendringen in devices een belangrijkere rol krijgt. Dit belemmert de opsporing echter wel, omdat het veel tijd, rekenkracht en capaciteit kost om dit te realiseren. Een voorbeeld waarbij de beperking tot het onderscheppen van communicatie een grote rol speelt is in heimelijk onderzoek. Dit is erop gericht om door middel van tappen verdachten en hun

[38] TDO staat voor Team Digitale Opsporing.

[39] OSINT staat voor Open Source INTelligence, ofwel: open bronnen onderzoek.

communicatie en strafbare feiten in beeld te krijgen. Doordat criminelen communicatiediensten gebruiken met E2EE is het volgens geïnterviewden vrijwel onmogelijk geworden om die communicatie op de traditionele manier te tappen.

Daarnaast geven andere geïnterviewden en respondenten juist aan dat de aanwezigheid van encryptie ook bijdraagt aan het bevorderen van de snelheid van een opsporingsonderzoek. "*Vroeger deden we drie maanden tot een jaar over een zaak en nu hebben we het rond in vier á vijf weken.*" Hoewel het enkele jaren heeft geduurd om EncroChat te kraken, konden daarna zaken bij het bewijsmateriaal worden gezocht. Er was zoveel belastend bewijsmateriaal dat er zaken gemaakt moesten worden bij het bewijsmateriaal. Ook het kraken van EnnetCom en PGP heeft bruikbare informatie opgeleverd, waarmee de rol van encryptie in het verloop van opsporingsonderzoeken groot is. Bij EncroChat, Ennetcom en Sky ECC zijn miljoenen berichten buitgemaakt. Twee respondenten zeggen daarover tot slot: *"Gedecrypte communicatie levert bewijs op; vergroot de slagkracht in heterdaad situaties; beïnvloedt capacitaire inzet in positieve zin; identificeert subjecten die voorheen buiten schot bleven; identificeert blinde vlekken; geeft inzicht in MO's door informatie van binnenuit; geeft informatie over crimescripts; en rollen van subjecten; etc."* En: *"Door cryptohacks bewijs op presenteerblaadje. Zonder dit was onderzoek naar ondermijning / zware criminaliteit eigenlijk vaak te tijdrovend en niet zo kansrijk."*

Encryptie kan naast vertraging dus ook zorgen voor een versnelling in de doorlooptijd van opsporingsonderzoeken. Een geïnterviewde vat dit als volgt samen: *"Het is een dubbelzijdig zwaard."* Als de encryptie niet ontsleuteld wordt zal het onderzoek langer duren, als het wel ontsleuteld wordt zal het onderzoek sneller gaan. Deze nuance kregen we vaker terug in interviews en zagen we ook terug in de survey resultaten. In sectie 4.2.4 staan we hier nadrukkelijker bij stil.

4.2.2 Voortzetten en stopzetten van opsporingsonderzoek

We vroegen respondenten welke criteria volgens hen het meest van belang zijn voor het *voortzetten* van een opsporingsonderzoek waarin encryptie een rol speelt. Daarbij konden de respondenten maximaal drie opties aanvinken, zie tabel 4.4. Om een opsporingsonderzoek waarin encryptie een rol speelt voort te zetten, wordt voornamelijk gekeken naar het criterium prioriteit van de zaak/misdrijf, waarna ook de geschatte kans van slagen om toegang te krijgen tot informatie achter encryptie als belangrijk criterium wordt aangemerkt.

Tabel 4.4: Criteria voortzetten opsporingsonderzoek (N=177)

Antwoordcategorie	Percentage aangevinkt
Prioriteit van de zaak / het misdrijf	85,9%
Kans van slagen om toegang te krijgen tot data achter encryptie	54,8%
Geen andere optie om tot bewijs te komen	32,8%
Benodigde expertise	32,2%
Hoeveel tijd het ontsleutelen of omzeilen van de encryptie vermoedelijk kost	31,6%
Beschikbare capaciteit	27,1%
(Toekomstige) schade voorkomen	7,9%
Anders	7,3%

Een greep uit de antwoorden die onder 'anders, namelijk' zijn ingevuld omvat: de verwachte opbrengst uit de data, ondermijning/georganiseerd verband, maatschappelijk belang en het belang voor de

bewijsvoering. Deze opties zijn meerdere malen benoemd. Hoewel er overlap lijkt te zijn met de antwoordcategorieën zien de respondenten dit toch anders. Hierna worden enkele elementen uit tabel 4.4 nader besproken aan de hand van interviewresultaten. Tevens wordt ingegaan op het *stoppen* van opsporingsonderzoeken.

Om de rol van encryptie in de opsporing in kaart te brengen is onder andere gekeken naar de rol van het OM. Het OM, net als de politie, ontwikkelt zich als organisatie op het gebied van digitale opsporing, en dus ook op het gebied van zaken waarin encryptie voorkomt om deze zodoende beter te behandelen, aldus een politiemedewerker. Het OM heeft als één van de hoofdtaken om leiding te geven aan de politie bij het opsporen van strafbare feiten.[40] In de oriënterende interviews komt het beeld naar voren dat encryptie invloed lijkt te hebben op de keuze voor de voortzetting van opsporingsonderzoeken. Door encryptie zijn er bijvoorbeeld geen andere mogelijkheden om tot bewijs voor strafbare feiten te komen. *"Dat is een groot argument om proportioneel steeds een stapje verder te gaan in bevoegdheden."* Het OM bepaalt bijvoorbeeld of capaciteit en tijd van de Nationale Politie of het NFI wordt ingezet om versleutelde data te kraken*. "Overal is schaarste dus niet alle zaken kunnen ingediend worden."* Deze keuze wordt beïnvloed door prioriteit, de kans van slagen en de wens (toekomstige) schade te voorkomen. Dit laatste criterium wordt door respondenten het minst vaak genoemd (zie tabel 4.4). Een geïnterviewde geeft in dit verband aan nog nooit te hebben meegemaakt dat een onderzoek enkel en alleen niet werd uitgevoerd omdat de encryptie te moeilijk zou zijn.

Er is prioriteit als het opsporingsonderzoek in het belang is van de Nederlandse samenleving. Het is bijvoorbeeld in het Nederlandse belang om in te zetten op bescherming van de vitale infrastructuur en zaken met vele slachtoffers met ernstige schade aan te pakken. Een OvJ legt de link met bepaalde opsporingsbevoegdheden die kunnen worden ingezet als aan een aantal criteria van strafvordering is voldaan; meestal in het geval van zware zaken. *"Als dan vervolgens sprake is van encryptie die door ons niet doorbroken kan worden, dan is zo'n opsporingsmiddel minder effectief, omdat je niet alle informatie meekrijgt."*

Team High Tech Crime (THTC) prioriteert bijvoorbeeld zaken die veel schade veroorzaken voor Nederland. Ze gaan bijvoorbeeld na hoeveel slachtoffers er zijn gemaakt, hoeveel geld er is verdiend, en of vitale infrastructuur en anderszins essentiële infrastructuur zoals ziekenhuizen en overheidsinstellingen zijn getroffen. Uit de interviews komt naar voren dat met name kinderporno en zedenzaken bijna altijd worden opgepakt vanwege de ernst van de zaak. Digitale experts vertellen dat het kraken van digitale devices met kinderporno regelmatig veel digitaal bewijs oplevert. Bij andere typen zedenzaken is minder sprake van digitaal bewijsmateriaal en/of is het digitaal bewijsmateriaal niet de doorslaggevende factor voor het opsporingsonderzoek.

Een geïnterviewde die werkzaam is bij de politie beschrijft hoe THTC heeft ingezet op een groep van ongeveer twintig personen die ransomware verspreidden. In drie jaar tijd heeft deze groep 100 miljoen euro verdiend aan slachtoffers. De groep was volledig afgeschermd via VPN, Tor en proxies, en daarmee bleven de daders anoniem. THTC heeft deze groep drie jaar lang achternagezeten, omdat het Nederlands belang groot is. In dit tijdsbestek heeft THTC nieuwe technieken uitgevonden om het gebruik van VPN te deanonimiseren. "*Als we nu diezelfde zaak zouden mogen draaien met de*

[40] De andere twee hoofdtaken zijn: (i) strafbare feiten vervolgen en verdachten voor de rechter brengen en (ii) afdoen van strafbare feiten zonder tussenkomst van een rechter. Zie: https://www.om.nl/organisatie/openbaar-ministerie/het-werk-van-het-om

nieuwe technieken, dan duurt het vier weken voor je weet wie er achter een computer zit in plaats van drie jaar." Gebruik van een VPN komt volgens geïnterviewden steeds vaker voor in zaken.

Een OvJ vult aan dat prioriteit of belang van een onderzoek breder is dan alleen het vergaren van bewijs. Zij stelt dat het essentieel is om in ieder geval de identiteit van de dader te achterhalen, de locatie en de verblijfplaats. *"Als we weten dat iemand beroofd is van zijn telefoon, dan zou je die telefoon kunnen afluisteren, vanuit de gedachte dat die in handen van de dader zou zijn. Daar kun je dan achter komen wie het is en waar diegene zich bevindt en dat kan helpen om iemand te gaan aanhouden. Dat we überhaupt weten waar we moeten zijn in het land en op welke plekken we eventueel een doorzoeking moeten doen om bewijsmateriaal te vergaren of het een gevaarlijk iemand is, waardoor een speciale politie-eenheid de aanhouding moet verrichten in plaats van gewoon de wijkagent. Al dat soort informatie kun je verkrijgen door de inzet van opsporingsmiddelen en als je niet alles meekrijgt [wanneer encryptie niet doorbroken wordt], mis je dus dingen. Dat betekent dat je soms meer moet doen om uiteindelijk hetzelfde beeld te krijgen; dat je meer opsporingsmiddelen moet inzetten om uiteindelijk toch het beeld dat nodig is, voor de gewenste vervolgstappen in onderzoek op verantwoorde wijze te kunnen uitvoeren."*

Soms kan dat ertoe leiden dat zwaardere middelen ingezet moeten worden, zoals de hackbevoegdheid (mits [technisch] mogelijk). Een voorbeeld daarvan is dat de groep/omgeving waar naar gekeken wordt groter wordt gemaakt om op die manier een beeld te krijgen. *"Een goede informatiepositie is van belang om zorgvuldige, proportionele afwegingen te kunnen maken in een onderzoek. Het is lastig om, als je niet weet wat je mist, om weten wat je mist; je weet alleen dat je iets mist."* In de volgende sectie komt de hackbevoegdheid nadrukkelijker aan bod.

Een uitkomst kan ook zijn dat een opsporingsonderzoek wordt stopgezet. Dit is het geval als er te weinig bewijsmateriaal is en de encrypte data niet ontsleuteld kunnen worden. Een OvJ beschrijft dat jaren geleden diverse lopende onderzoeken van geweldsmisdrijven, liquidaties en drugsonderzoeken zijn gestopt omdat gebruik werd gemaakt van Ennetcom-telefoons. Het tappen van de versleutelde Ennetcom-telefoons leverde de opsporingsinstanties niets op. Verder vertelt hij dat na twee jaar besloten is om te kijken naar de rol van Ennetcom in deze zaken. Dit heeft lang geduurd vanwege privacy overwegingen. Diverse onderzoeken zijn volgens meerdere geïnterviewden gestopt omdat het vanwege deze encryptie de politie niet lukte om een informatiepositie te krijgen. In de volgende sectie gaan we dieper in op het toegang krijgen tot encrypte informatie.

Een aanvullend nadeel van het stoppen van opsporingsonderzoek is dat de ontoegankelijke informatie ook niet gebruikt kan worden als aanleiding voor een nieuwe zaak, als bijvoorbeeld nieuwe verdachten in beeld komen. Door encrypte data mist de politie potentiële intelligence om andere daders of strafbare feiten op het spoor te komen. Op de vraag hoe vaak een opsporingsonderzoek stopt door encryptie is volgens een OvJ niet te zeggen. *"Sommige zaken los je op en andere niet, en daar kan een heel palet aan redenen voor zijn. Als je stuit op devices die je niet kunt openen, weet je niet wat erin staat. Het had het verhaal helemaal kunnen vertellen en daarmee, met één telefoon, de zaak opgelost, dat weet je niet. Afhankelijk van de zaak, kan je kijken of je op andere plekken bewijs kan vinden; soms lukt dat wel en soms niet. […] Als je stuit op een telefoon die je niet open krijgt, is dat het enige wat je weet; dat je hem niet open krijgt."*

4.2.3 Toegang tot encrypte data en communicatie

Er zijn vier mogelijkheden om de inhoud van een digitaal account veilig te stellen. De eerste is met toestemming van de verdachte op grond van art. 32 onder b van het cybercrimeverdrag. De tweede is door middel van een netwerkzoeking op grond van art. 125j Sv. De derde is door middel van een vordering aan de aanbieder op grond van art. 126ng lid 2 Sv. En de vierde is tot slot met toepassing van de hackbevoegdheid als bedoeld in art. 125nba Sv. Een rc typeert de rol van encryptie als hooguit een 'decryptieprobleem'. *"Meestal is encryptie geen juridisch issue, maar een praktisch probleem voor de opsporing. Het levert soms juridische hoofdbrekers op hoe je er anders bijkomt. Bij versleutelde communicatie is het probleem dat er niet bij gekomen kan worden. Dat wordt nu opgelost met 'hacken light', de Innovatiewet en de hackbevoegdheid."* In deze sectie gaan we dieper in op het 'praktische probleem'.

De slagingskans om achter encrypte informatie te komen zodanig dat het bruikbaar is voor het opsporingsonderzoek is niet te kwantificeren. Geïnterviewden is gevraagd om te beschrijven hoe vaak het lukt om toegang te krijgen tot voor de opsporing relevante informatie in zaken waarin encryptie voorkomt. De schattingen uit interviews variëren van een paar procent, naar 25% tot 75%. Ook in de vragenlijst stuitten we op tegenstrijdigheden. Ter illustratie, een respondent geeft bijvoorbeeld aan dat: *"We kunnen steeds meer gegevens die encrypted zijn toch inzichtelijk maken […]"*, maar een andere respondent zegt bijvoorbeeld: *"Veelal komen we niet achter de versleutelde gegevens."*

Een OvJ geeft aan dat het mede afhangt van over welke fase in de opsporing wordt gesproken. Hij geeft aan dat vooral in de heimelijke fase encryptie een belemmerende rol speelt. Dit komt volgens hem vooral door de encryptiemethodieken van de aanbieders. Ter illustratie noemt hij Signal die chatberichten niet eens opslaat en ProtonMail waarbij e-mails versleuteld worden opgeslagen. Daarbij zegt hij dat van de 100 zaken er 90 geraakt worden door 'encryptieproblematiek'. De vraag is dan in hoeveel van die 90 zaken in de heimelijke fase toch informatie veilig gesteld kan worden? De OvJ denkt dat de slagingskans daarvoor – middels methodieken waaronder juridische grondslagen liggen – momenteel drie à vier zaken is. Mogelijk in de nabije toekomst iets meer, maar lang niet alle 90. In de niet-heimelijke fase betreft het vooral telefoons. Tevens geeft de OvJ aan dat zeker bij de nieuwste telefoons het niet lukt om deze te kraken. *"Elke aanpassing die een hardware fabrikant maakt 'van je mag maar zes keer je code invoeren en daarna is het klaar', of er wordt een vertraging ingebouwd, die maakt het voor de opsporing heel erg moeilijk om toegang te krijgen."*

Andere geïnterviewden kunnen of willen hier geen inschatting van geven, omdat dit afhangt van meerdere factoren. Geïnterviewden vragen zich af onder welke voorwaarden kraken 'succesvol' is. Is kraken 'succesvol' als de gevonden data niet nuttig zijn voor de zaak? Of wat als slechts een deel van de data wordt ontsleuteld? Een OvJ zegt hierover *"Dit is een typische vraag die ons heel vaak gesteld wordt. Hoe veel zaken hebben jullie niet kunnen oplossen, omdat er geen dataretentie is? Geen idee, want je kan nooit zeggen wat je niet hebt en in hoeverre dat wel of niet tot de oplossing van de zaak had geleid."*

Een geïnterviewde OvJ draait de vraag om en denkt na hoe vaak het niet is gelukt. Hij vertelt dat het slechts een aantal keer niet gelukt is. In die gevallen ging het om hightech criminaliteit. De betreffende criminelen hadden hun devices dusdanig versleuteld dat het niet lukte om erin te komen. Verder stelt hij: *"Heel vaak lukt het ons met een hoop huidige gegevensdragers van verschillende fabrikanten om binnen een versleuteld apparaat te komen en om die te kunnen ontsleutelen. Daar hebben we wat minder problemen, het duurt alleen wat langer."*

We vroegen de respondenten ook een schatting te maken van hoe vaak zij denken dat het gemiddeld genomen binnen een opsporingsonderzoek lukt om toegang te krijgen tot versleutelde communicatie en versleutelde data (anders dan communicatie), zie tabel 4.5. De antwoorden moeten voorzichtig worden geïnterpreteerd, omdat een precies antwoord lastig is te geven zoals eerder is benoemd door geïnterviewden.

Tabel 4.5: Succesvol toegang tot versleutelde communicatie (N=169) en data (N=156)

	0 tot 25% van de gevallen	25 tot 50% van de gevallen	50 tot 75% van de gevallen	75 tot 100% van de gevallen	Weet niet / niet van toepassing
Versleutelde communicatie	22,6%	30,5%	34,5%	7,9%	4,5%
Versleutelde data	23,2%	34,5%	26,0%	4,5%	11,9%

Een aanvullende analyse is uitgevoerd om te onderzoeken of het type delict van invloed is op het succesvol toegang verkrijgen tot versleutelde communicatie en data. Omdat er een redelijk hoge correlatie blijkt te zijn tussen het succesvol toegang verkrijgen tot communicatie en tot data (*Pearson correlatie = .67, p* < .01) zijn deze in deze analyse samengevoegd. Uit deze analyse blijkt dat het succesvol toegang verkrijgen tot versleutelde communicatie en data als groter wordt ingeschat wanneer respondenten dagelijks vaker te maken hebben met georganiseerde criminaliteit, gedigitaliseerde criminaliteit en cybercrime (zie tabel VI.2 in bijlage VI). Daarnaast is ook onderzocht of de verschillende toepassingen van encryptie van invloed zijn op het succesvol verkrijgen van toegang tot communicatie en data. Hier bleken geen significante relaties te zijn (*p* > .05).

Vervolgens vroegen we op welke wijze toegang verkregen wordt tot versleutelde informatie die in opsporingsonderzoeken een rol spelen. Hieruit ontstaat het volgende beeld, zie tabel 4.6. Wat opvalt is dat er geen duidelijke uitschieters zijn. De gevallen die in meer dan de helft van de gevallen worden benoemd als veel en altijd betreffen: uitbesteding aan andere afdeling of partij, technisch kraken, omzeilen en alternatieve opsporingsmiddelen inzetten. De opties ‘decryptiebevel’ en ‘hackbevoegdheid’ zijn weinig genoemd door de respondenten.

Tabel 4.6: Wijze van toegang tot encrypte data/communicatie (N=177)

	Niet	Weinig	Niet weinig/ niet veel	Veel	Altijd	Weet niet
Via uitbesteding aan een andere politieafdeling of partij (bijv. NFI)	2,3%	11,9%	17,5%	53,1%	8,5%	6,8%
Encryptie technisch kraken (bruteforce)	2,3%	7,9%	17,5%	50,8%	7,9%	13,6%
Encryptie omzeilen (bijv. de sleutel vinden of raden)	3,4%	11,3%	26,0%	42,2%	7,9%	9,0%
Alternatieve opsporingsmiddelen inzetten (bijv. verhoren, observeren, huiszoekingen)	3,4%	13,6%	22,6%	43,5%	10,7%	6,2%
Aanhouding met open devices (zodat encryptie geen rol meer speelt)	3,4%	15,8%	31,1%	36,7%	5,1%	7,9%
Meewerken verdachte (die bijv. de sleutel vrijwillig afgeeft)	10,2%	28,2%	29,4%	23,2%	4,0%	5,1%
Middels het decryptiebevel (art. 126nh lid 1)	31,6%	35,6%	10,7%	1,1%	0%	1,1%
Middels de ‘terughackwet’ (art. 126nba)	32,2%	30,5%	14,1%	2,3%	0%	20,9%

Respondenten konden via een open invoerveld ook andere mogelijkheden noemen. Twee respondenten benoemen: een vordering doen bij versleutelende partij en gebruik maken van sleutels afkomstig uit andere onderzoeken. Aan het einde van deze sectie gaan we dieper in op vorderen en rechtshulpverzoeken. Een derde respondent gaf aan: *"Het toepassen van dwang bij de aanhouding van de verdachte om de toestellen te ontgrendelen."*

In meerdere interviews met rechters en rc'en ging het ook over dat verdachten soms worden gedwongen om hun telefoon te openen. Een rechter stelt dat enige tijd geleden door de Hoge Raad is geoordeeld dat iemand de telefoon moest openen met gebruik van vingerafdruk, zonder dat diegene dit wilde.[41] Er moet dan wel een verdenking zijn en toestemming van de rc om in iemands telefoon te komen. Een rc licht toe aan de hand van dezelfde uitspraak van de Hoge Raad dat er lichte dwang toegepast mag worden en dat dit hoort bij de inbeslagname bevoegdheid. Een andere rc geeft aan dat ook wel eens sprake is geweest van 'fors geweld' tijdens een netwerkzoeking. In dat geval oordeelde de rechtbank dat het geweld proportioneel was. Proportionaliteit is volgens deze rc afhankelijk van het delict en onderzoeksbelang, maar ook als er veel verzet is kan meer geweld dat wordt toegepast ook als proportioneel worden gezien.

Inmiddels codificeert de Innovatiewet Strafvordering dit onder art. 558 Sv. De Innovatiewet – nu nog een pilot – bevat een paar nieuwe cyberbevoegdheden, die uiteindelijk terecht zullen komen in het nieuwe Wetboek van Strafvordering. In deze pilot wordt gekeken hoe de bevoegdheden bevallen en of er aanscherpingen nodig zijn. Bij art. 558 Sv kan de officier bevelen dat iemand – eventueel tegen zijn wil in – moet meewerken aan de ontgrendeling van de telefoon door middel van een vingerafdruk of gezichtsscan (biometrische gegevens). In de praktijk is dit soms lastig bijvoorbeeld als een verdachte gekke gezichten trekt. Er mag lichte dwang gebruikt worden, maar het moet proportioneel zijn.

Een OvJ noemt de doorzoeking na inbeslagname als heel belangrijke ontwikkeling voor de opsporing, en dat het ook fijn is dat die in de Innovatiewet gekomen is. *"Daarmee maak je mogelijk dat je op die manier encryptie doorbreekt nadat je doorzoeking hebt afgesloten of niet eens na doorzoeking, maar dat je het in beslag hebt genomen. En het afvangen van inkomende berichten de eerste periode na inbeslagname, met goedkeuring van de rc. Eigenlijk zijn dat de twee dingen waar de praktijk echt tegenaan liep."* Het afgeven van een vingerafdruk was volgens deze OvJ al wel beslecht, waarbij wordt gerefereerd naar de uitspraak van de Hoge Raad. Daarbij wordt overigens wel aangegeven dat het fijn is dat het nu op papier staat; dat de wetgever nu ook zegt dat het goed is.

Een geïnterviewde rechter geeft aan dat er een verschuiving gaande is naar de bescherming van privacy van de verdachte. Toen telefoons nog minder versleuteld waren, keek de politie vaker in de telefoons, omdat deze makkelijker toegankelijk waren. Dit kan nu niet meer zomaar. Bij cryptotelefoons en het internet ziet hij dezelfde verschuiving. Tevens geeft deze rechter aan zowel redelijk vaak te zien dat verdachten deels toestemming geven om in de telefoon te komen, maar ook best vaak dat ze dat niet doen.

Uitbesteding en encryptie technisch kraken. De politie kan volgens meerdere geïnterviewden op technische wijze het wachtwoord ontsleutelen door het inzetten van BOB-middelen[42] (internettap of telefoontap) en bruteforcen, waarbij een programma systematisch wachtwoorden en encryptiesleutels uitprobeert. Bruteforcen wordt zowel door de politie als het NFI ingezet. Deze methode wordt vaak ingezet als de andere tactieken onvoldoende bewijs hebben opgeleverd

[41] De betreffende uitspraak is te lezen in: ECLI:NL:PHR:2020:927

[42] BOB staat voor Bijzondere Opsporingsbevoegdheden.

(aanhouding met open devices, meewerkende verdachte en encryptie omzeilen). In onderzoeken waarin reguliere telefoons een rol spelen, worden codes vaak gekraakt door TDO, aldus een respondent.

Om op technische wijze het wachtwoord te ontsleutelen worden verschillende methoden ingezet. THTC gebruikt onder andere *side channel attacks*, dit is een type aanval gebaseerd op informatie van de implementatie van een computersysteem in plaats van op de kwetsbaarheden in een systeem. Daarnaast gebruikt THTC volgens een geïnterviewde *keyboard logging* – het monitoren van welke toetsen worden aangeslagen door de verdachte – of zetten ze verborgen camera's in die de verdachte filmt terwijl het wachtwoord wordt ingevoerd. Ook wordt OSINT ingezet om bijvoorbeeld te controleren of een gevonden e-mailadres eerder is gebruikt.

De slagingskans om middels bruteforce toegang te krijgen tot voor de opsporing relevante informatie is volgens geïnterviewden afhankelijk van de beschikbare tijd. Ter illustratie, een geïnterviewde geeft aan dat vanaf het moment dat de eerste EncroChat telefoon in beeld was tot het moment dat het NFI in staat was om die te ontsleutelen daar zo'n twee à drie jaar overheen is gegaan. In de tussentijd hebben de daders vrij spel gehad op het platform. Bovendien zit er vaak op dergelijke toestellen een *burntime*, waardoor berichten na een bepaalde periode automatisch worden verwijderd. Met als gevolg dat na het kraken beperkte communicatie getoond wordt. Het kraken van versleutelde gegevens kan *"weken, maanden of jaren duren … Bijna alles is te kraken, het heeft gewoon tijd nodig."*

Het NFI wordt ingeschakeld bij zaken met encryptie die de politie niet kan kraken (of geen capaciteit voor heeft). Het NFI krijgt een concrete opdracht van de politie. Volgens enkele geïnterviewden is de capaciteit van digitaal specialisten bij de politie en bij het NFI beperkt. Anderen geven aan dat gebrek aan capaciteit overal in de strafrechtketen een rol speelt. Bij het NFI komen meer zaken binnen dan kunnen worden opgepakt en daarom maakt het NFI een selectie. Bij bruteforce-opdrachten zoeken ze meestal drie maanden en als er niets is gevonden nemen ze contact op met de opdrachtgever; de politie. Enkele geïnterviewden geven aan dat voor het toepassen van bruteforce veel capaciteit en adequate soft-/hardware nodig, zoals zware grafische kaarten. De politie en het NFI schaffen deze apparatuur niet altijd zelf aan. Sommige van de eerdergenoemde grafische kaarten betreffen in beslag genomen apparatuur van *bitcoin miners*.

De slagingskans van het ontsleutelen is ook afhankelijk van het type encryptie en de sterkte van het wachtwoord. *"Over het algemeen geldt, hoe langer de sleutel is, hoe lastiger deze is te kraken."* En zelfs als er geen lange sleutels worden gebruikt, dan is het moeilijk om encryptie op technische wijze te kraken, vanwege de vele mogelijke combinaties, aldus geïnterviewden. Wat daarbij helpt is dat de opsporing zoekt naar *"briefjes, schriftjes, namen van de kat en hond"* die aan een wachtwoordlijst toegevoegd kunnen worden wat het bruteforcen kan vergemakkelijken.

Ook kunnen daders volgens geïnterviewden speciale beveiligingsinstellingen inzetten om het kraken voor de politie te bemoeilijken. Bij het programma VeraCrypt kan bijvoorbeeld een dubbel wachtwoord worden gebruikt of een alternatief wachtwoord worden ingesteld om alle data te wissen of toegang te geven tot een ruimte waar geen (strafbare) bestanden op staan. Een geïnterviewde politiemedewerker heeft één keer een door de verdachte verstrekt wachtwoord gebruikt waardoor er geen inhoud meer op de schijf was. Op basis van de grootte van het bestand met encryptie werd verwacht dat er (meer) data op de gegevensdrager zouden staan. De verdachte geeft vervolgens aan meegewerkt te hebben en er kan niet bewezen worden dat de verdachte een alternatief wachtwoord

heeft gegeven. Deze medewerking van de verdachte zonder opbrengst brengt de politie in een lastig parket, aldus een geïnterviewde.

Hoe goed de encryptie is ingezet is afhankelijk van de technische capaciteiten van de daders (zie ook sectie 4.1.3). Een geïnterviewde beschrijft verschillende typen van encryptie aan de hand van daders in kinderpornozaken. Hij stelt dat in kinderpornozaken daders onder te verdelen zijn in de volgende categorieën (in piramidevorm): *"een persoon met technische capaciteiten, de misbruiker, de downloader en de kijker."* Op de onderste lagen van de piramide (misbruiker, downloader en kijker) worden applicaties gebruikt zoals WhatsApp en Skype. Opsporingsinstanties hebben een relatief grote slagingskans om tot relevante versleutelde informatie te komen bij devices en programma's waar encryptie is ingebouwd (zoals een mobiele telefoon, WhatsApp, Skype). Een politiemedewerker bevestigt dat zijn afdeling in de meeste gevallen telefoons behandelt met standaard versleuteling (pincode, vingerafdruk, gezichtsherkenning): *"Daar kunnen we altijd wel bij."*

Hoe hoger de dader in de piramide zit, hoe moeilijker de dader te lokaliseren is en hoe moeilijker het is om de encryptie te kraken. De daders met technische vaardigheden gebruiken hoogwaardige vormen van encryptie zoals versleuteling van gestolen telefoons, het dark web (Tor Browser) en crypto containers. Daders die dergelijke encryptie gebruiken vertragen het verloop van het opsporingsonderzoek aanzienlijk, aldus een geïnterviewde.

Een laatste redmiddel om toegang te krijgen tot encrypte data is het inzetten van de hackbevoegdheid. Deze speciale bevoegdheid mag alleen ingezet worden door Digital Intrustion Team (DIGIT) van de politie, dat is opgericht in 2019 na de invoering van de wet Computercriminaliteit III. De hackbevoegdheid heeft met deze wet een grondslag gekregen in het Wetboek van Strafvordering (Van Uden & Van den Eeden, 2022). Het gaat daarbij om artt. 126nba, 126uba en 126zpa Sv. De wet Computercriminaliteit III staat ook wel bekend als de 'hackwet' of 'terughackwet'. De hackbevoegdheid is bedoeld om heimelijk en op afstand in een geautomatiseerd werk in te breken of te tappen als deze versleutelde data verstuurt. Een geïnterviewde politiemedewerker geeft aan dat de capaciteit beperkt is en het geen standaard middel is dat ingezet kan worden. Een OvJ zegt in het kader van bevoegdheden dat het belangrijk is om goed na te blijven denken waar informatie nog in niet-versleutelde vorm aanwezig is en hoe daar rechtmatig toegang tot te krijgen.

Resumerend, de slagingskans van het kraken van encrypte informatie is op basis van de interviews niet te kwantificeren. De kans voor de politie om in de opsporing tot relevante informatie te komen wordt vergroot door encryptie te omzeilen (zie hierna). Dit wordt gedaan door intensief vooronderzoek en de verdachte aan te houden met open devices. Mocht dit niet lukken dan kan om medewerking (wachtwoorden) worden gevraagd of op zoek gegaan naar de sleutel (hopen op slordig sleutelbeheer). Het kraken (bruteforcen) van encrypte data is moeilijk en kost veel tijd, rekencapaciteit en menskracht, maar is zeker niet onmogelijk.

Het kraken van encryptie leidt overigens ook tot een dilemma binnen de opsporing. Een OvJ benoemt de mogelijke toepassing van zero-days door de politie, althans zo wordt het volgens hem soms gepositioneerd. De OvJ geeft toe dat in de opsporing tools worden gebruikt, zoals het commerciële Cellebrite, waarvan de exacte werking onbekend is. Het voert volgens hem echter te ver om dat te kwalificeren als zero-days en vervolgens te zeggen: *"De politie gebruikt dat elke dag."* Er worden overigens meerdere tools gebruikt binnen de politie, maar daar gaan we in dit rapport niet dieper op in. Een ander dilemma dat naar voren kwam is dat door het niet kunnen ontsleutelen van informatie, (sterke) vermoedens van criminaliteit niet bewezen kunnen worden. *"Wordt bijvoorbeeld*

een toestel waar zeer waarschijnlijk, maar niet bewijsbaar, kinderporno op staat weer teruggegeven aan de verdachte?"

Encryptie omzeilen. Als een verdachte niet meewerkt is het aan de opsporingsinstanties om de encrypte devices te ontgrendelen of encrypte informatie te ontcijferen. Een van de geïnterviewden schat ruwweg in dat 25% van de zaken waar encrypte data worden ontsleuteld de politie afhankelijk is van de bewijsvoering van een weigerachtige verdachte. Een geïnterviewde schat in dat 5-10% van de (kinderporno) zaken encryptie succesvol wordt ontsleuteld.

Als de verdachte niet meewerkt en er geen toegang is tot de benodigde informatie, dan moet de politie zelf de sleutel zien te bemachtigen. Hiervoor zijn meerdere mogelijkheden. De politie kan de encryptie omzeilen door te zoeken naar slordig sleutelbeheer bij verdachten. "*Daar moeten we het van hebben; van mensen die fouten maken."* Ze zoeken op usb-sticks, het dark web en in bestanden op de computer om gericht de sleutel te raden zoals een geboortejaar. *"Soms geeft de toegang tot een laptop hints voor de toegangscode van de telefoon en soms kom je geeltjes tegen met aanwijzingen. Denk aan een geeltje waar een wachtwoord op is geschreven of een 'open' bestand waar alle wachtwoorden van verschillende accounts in staan."* De politie zet ook technische middelen in zoals een keyboard logger. *"Daar [slordig sleutelbeheer] behalen we de meeste successen mee. Maar bij de slimmere, scherpe verdachten lukt het minder goed."*

Een geïnterviewde benoemt dat de minder technisch onderlegde criminelen bij het gebruik van encryptie sneller fouten maken. Het inspelen op deze gemaakte fouten stelt de politie in staat om makkelijk toegang te verkrijgen tot belastende informatie. Een voorbeeld gegeven door een geïnterviewde is het per ongeluk koppelen van een encrypte telefoon aan een minder goed beveiligde cloud-omgeving: "*Waar we zien dat ze soms de fout ingaan, vooral bij de niet zo handige gebruiker, is dat ze om de zoveel tijd een nieuwe telefoon kopen en dan kennen ze de instellingen niet meer en dan gaat er iets mis want dat apparaat is automatisch gekoppeld aan een cloudopslag."*

Ook worden soms creatieve manieren ingezet om de encryptie te omzeilen. In een interview werd verwezen naar de rechtsuitspraak: ECLI:NL:RBDHA:2021:8421.[43] Het OM heeft hierbij aan een rc gevraagd om een nieuwe simkaart aan te vragen om zodoende bij WhatsApp gesprekken te komen van een slachtoffer. De telefoon van het slachtoffer is nooit teruggevonden en twee andere telefoons die vermoedelijk van het slachtoffer waren zijn beide niet recent actief geweest en bevatten geen WhatsApp data. Ze willen vervolgens het wachtwoord resetten van het Google account om op die manier toegang te krijgen tot de WhatsApp back-up die mogelijk in het Google account staat. Dit verzoek is afgewezen. Het lijkt op de hackbevoegdheid – die alleen ingezet mag worden bij een verdachte en niet bij een slachtoffer – en het verzoek was bovendien niet goed onderbouwd.

In een ander geval dat werd genoemd mocht dit wel: ECLI:NL:RBDHA:2022:4288. In dit geval was het slachtoffer overleden. Het OM vraagt om via een nieuw aangevraagde simkaart bij het Google account te komen en vervolgens in de WhatsApp back-up te komen. Een geïnterviewde noemt dit 'hacken light'. Dit verzoek is aangevraagd op grond van art. 181 juncto 177 Sv met analyse toepassing van art. 126ng SV. Een rechter oordeelt over deze niet-rechtstreekse wijze van toegang verschaffen: er is geen sprake van omzeiling van de hackbevoegdheid (art. 126nba Sv). Er mogen berichten van

[43] Alle uitspraken krijgen een Europees identificatienummer (ECLI). Dit is een unieke codering voor gerechtelijke uitspraken in de EU. Een ECLI-nummer bestaat uit de onderdelen: landcode, afkorting van instantie, jaartal en volgnummer. Zie: https://www.rechtspraak.nl/Uitspraken/Paginas/Hulp-bij-zoeken.aspx#1ab85aa0-e737-4b56-8ad5-d7cb7954718d77a998be-3c73-40e3-90f7-541fceeb00fd4

maximaal elf dagen veiliggesteld worden. Met de Innovatiewet is onder art. 556 Sv lid 1 vastgesteld dat berichten die de eerste drie dagen na inbeslagname van een device binnen komen, gelezen mogen worden.

Aanhouding met open devices. Geïnterviewde politiemensen geven aan dat het tijdens een opsporingsonderzoek lastig is om in kaart te brengen of er versleutelde bestanden zijn en zo ja, welke bestanden dat zijn ('hidden in plain sight', zoals een versleutelde container). Om te achterhalen of er überhaupt versleutelde devices of data zijn bij de verdachte kan de politie de telefoon of het internetverkeer van een verdachte tappen. Door een internettap kan communicatie worden onderschept. De politie kan zo achterhalen welke devices en data relevant zijn voor het opsporingsonderzoek.

Een techniek om toegang te krijgen tot versleutelde bestanden dat door meerdere geïnterviewden is genoemd is om verdachten aan te houden terwijl de devices nog open staan. Als de devices open staan, en de verdachte ingelogd is op relevante accounts, heeft de politie geen sleutel nodig om de data te ontsleutelen. Als een verdachte bijvoorbeeld is ingelogd op een dark web account waar drugs worden verkocht, kan een klantenlijst toegankelijk zijn of een andere server met bewijsmateriaal. Of als een verdachte tijdens de aanhouding een cryptotelefoon of een communicatie-app zoals WhatsApp open heeft staan, dan is communicatie van de verdachte beschikbaar voor de politie. Op deze wijze heeft de politie – niet op technische wijze maar tactische wijze – toegang verkregen tot een heel netwerk, aldus een geïnterviewde. Het OM moet regelmatig heftige maatregelen nemen om iemand achter een open device aan te houden. *"Het aanhouden van een cyber verdachte in een volle collegezaal, daar deinzen we niet meer voor terug, omdat het anders niet te doen is."* De maatregelen die genomen worden zijn zwaarder geworden om het probleem van encryptie te omzeilen.

Een rc legt uit wat in sommige zaken gebeurt is dat er een IP-tap loopt, om te kijken wanneer iemand online is, zodat het apparaat bij de aanhouding open is. In sommige gevallen komt er dan een arrestatieteam aan te pas. De extreme manier van aanhouding met een arrestatieteam met het oog op een open device komt een aantal keer per jaar voor. Een rc is betrokken bij de doorzoeking die volgt op de aanhouding. Een rc kan een doorzoeking soms eerder openen, zodat de politie direct op de apparaten af kan en deze kan veiligstellen. Dat is een bevriezingsmogelijkheid; de technici gaan naar binnen en zorgen ervoor dat niks meer met de apparaten kan gebeuren. Op het moment dat een apparaat versleuteld is en de gedwongen ontgrendeling valt binnen de doorzoeking, dan heeft de rc ook de verantwoordelijkheid dat het geweld wat toegepast wordt binnen de perken blijft.

De slagingskans op een succesvolle aanhouding met open devices is grotendeels afhankelijk van de investering in het vooronderzoek. Door de eerdergenoemde telefoon- of internettap kan de politie informatie vergaren over de relevante bestanden en om voorbereidingen te treffen bij de aanhouding. De tap kan bijvoorbeeld blootleggen dat de gebruikte computer een automatische schermbeveiliging heeft; waarbij de computer na een poosje wordt vergrendeld. Door deze informatie voorafgaand aan de arrestatie te achterhalen, kan de politie voorbereidingen treffen om ervoor te zorgen dat de computer niet automatisch vergrendelt na de arrestatie. De politie heeft steeds vaker te maken met bluetooth devices die automatisch afsluiten als een persoon op een bepaalde afstand is van het device. Er worden ook devices aangetroffen op een plaats delict die op afstand worden gewist. Hoewel dit geen encryptie betreft, is het wel verlies van data. Met een grote investering vooraf lukt het in 80% van de zaken om open devices aan te treffen, aldus een geïnterviewde.

Een aanhouding met open devices vergt een andere strategie en planning van een opsporingsonderzoek. Er wordt veel tijd en capaciteit geïnvesteerd in de informatieverzameling van een verdachte om een succesvolle aanhouding met open devices te garanderen. Het opsporingsonderzoek gericht op het vinden van bewijs voor strafbare feiten in digitale informatie verschuift vervolgens naar de staart van het onderzoek (na de aanhouding). Inzicht in strafbare feiten komen pas na de aanhouding. De gevonden informatie kan vervolgens niet getoetst worden aan andere bronnen en er zijn weinig mogelijkheden om in de fysieke wereld informatie te toetsen. Als het niet lukt om belastende of ontlastende informatie te achterhalen dan kan dat ook impact hebben op het wel of niet langer en rechtmatig kunnen vasthouden van verdachte handlangers, aldus geïnterviewden.

Om in te kunnen spelen op encryptie in opsporingsonderzoeken is volgens een geïnterviewde meer mankracht nodig. Om een succesvolle aanhouding te garanderen is volgens politiemensen *"inzicht nodig in de leefgewoonte van een verdachte en dat vreet veel capaciteit."* Ook bij de ondersteunende teams zoals de Dienst Speciale Interventies (DSI) is meer mankracht nodig. De DSI is een antiterrorisme eenheid die voor team TBKK dergelijke specialistische aanhoudingen verzorgt.

Meewerken verdachte. Om de kans te vergroten om tot voor de opsporing relevante informatie te komen is een meewerkende verdachte nog belangrijker dan het type encryptie wat is gebruikt, aldus een geïnterviewde. De slagingskans om tot voor de opsporing relevante informatie te komen is afhankelijk van het type verdachte en of de verdachte meewerkt bij het toegang verschaffen tot de versleutelde systemen. Op device niveau moet de politie een meewerkende verdachte hebben die het device moet openen. Een politiemedewerker heeft vier zaken gehad waarin een verdachte mens-gedreven encryptie heeft toegepast, zoals VeraCrypt en BitLocker. In drie van de vier zaken heeft de politie toegang gekregen tot voor hen relevante informatie, omdat verdachten hun wachtwoord hebben afgegeven. Slimme criminelen zullen volgens geïnterviewden niet snel voor cloudopslag kiezen omdat het eindstation dan niet in eigen handen is en er daardoor risico is op meekijken door anderen, zoals de politie. Echter worden volgens geïnterviewden wel steeds meer bestanden opgeslagen in de cloud, zoals Dropbox en MEGA.nz.

Als een verdachte meewerkt in een opsporingsonderzoek is het van belang dat de politie kan aantonen dat de medewerking vrijwillig is. Volgens het nemo tenetur-beginsel mag niemand gedwongen worden om mee te werken aan zijn eigen veroordeling. Dit is verankerd in art. 6 EVRM. Dat betekent dat de politie een verdachte niet mag dwingen om zijn/haar wachtwoord af te geven in Nederland. Uitzondering hierop is de eerder beschreven Innovatiewet, waarin dat onder specifieke omstandigheden wel mag. Geïnterviewde OvJ's geven aan dat de Innovatiewet niet in strijd is met dit beginsel. Een OvJ licht dit toe: *"Het wetboek van Strafvordering kent al heel lang de bepaling dat je ook mee moet werken aan het afscheren van je haar, correcte fotoconfrontatie te laten plaatsvinden, vingerafdrukken en DNA onder omstandigheden moet afstaan, daar is dit er een van."*

Ook zijn er zaken bekend – die zich voor de Innovatiewet afspeelden – waarin dit werd gedaan en waarbij de rechter oordeelde dat dit rechtmatig was. In een zaak heeft de politie de verdachte gevraagd om samenwerking en het ontgrendelen van zijn telefoon. Na het bieden van weerstand heeft de politie geprobeerd om zijn duim op zijn telefoon te plaatsen, waarop hij meewerkte en zijn toegangscode heeft verstrekt. De rechter oordeelde dat er geen sprake was van een overtreding van artt. 3, 6 of 8 van het Europees Verdrag voor de Rechten van de Mens. De verdachte werd verdacht van serieuze vergrijpen, waaronder het vasthouden van twee vermiste jonge kinderen. Ten tijde van

het verzoek van de politie om mee te werken, was de locatie nog onbekend. De locatie van deze kinderen was dringend nodig. In een dergelijke situatie is een bepaalde mate van dwang toegestaan en noodzakelijk. De politie leek niet buitenproportioneel te hebben gehandeld.

Hoewel een verdachte niet hoeft mee te werken aan zijn/haar eigen veroordeling, wordt in meerdere interviews aangehaald dat verdachten dit soms wel doen door over de daden te spreken of door wachtwoorden af te geven. Een geïnterviewde beschrijft dat verdachten in kinderpornozaken in 80-90% van de gevallen vrij spreken over hun daden, maar slechts een enkeling (5%) een wachtwoord afgeeft. Om medewerking van verdachten te krijgen zijn goede rechercheurs nodig die in gesprekken hen ertoe brengen om hun devices en wachtwoorden af te geven. Een OvJ geeft in het kader van medewerking aan dat dat veel gebeurt in minder ernstige zaken. Bijvoorbeeld omdat men vindt dat zijn of haar rol anders is geweest, of daarmee wil aantonen iets niet te hebben gedaan; dat ze de verkeerde hebben. Deze OvJ stelt ook dat hoe georganiseerder de criminaliteit, hoe minder de medewerking.

Middels een analyse op de vragenlijstdata hebben we gekeken in hoeverre het meewerken van een verdachte opsporingsonderzoeken gerelateerd is aan het type delict. Voor het belang van deze analyse is het antwoord 'weet ik niet' niet meegenomen. Uit deze analyse blijkt dat het meewerken van een verdachte vaker een rol speelt in opsporingsonderzoeken rond geweldsdelicten, vandalisme en milieucriminaliteit (zie tabel VI.3 in bijlage VI).

We hebben in de analyse van rechterlijke uitspraken ook gekeken op welke manier encryptie is omzeild of gekraakt. In de meeste gevallen is niet bekend hoe achter de encryptie is gekomen of is de rol ten aanzien van de strafrechtelijke vervolging onduidelijk. In gevallen waarin het wel bekend is, komt veelal de EncroChat-zaak en/of andere grote zaken voorbij waarbij encryptiesleutels zijn gebroken door politie van servers die in het buitenland staan. Daardoor zijn berichten leesbaar geworden voor opsporingsdiensten waarnaar dit als bewijs is gebruikt in rechtszaken.[44]

Verder is een aantal keer benoemd dat het NFI de encryptiesleutels heeft gebroken en dat door de Ennetcom-hack of via buitenlandse opsporingsdiensten bewijs is verkregen. Wat slechts eenmaal naar voren kwam is het vinden van een wachtwoord in de woning, het verkrijgen van een wachtwoord via toetsaanslagen op een computer en dat middels art. 126ng Sv toegang is verkregen tot versleutelde chatberichten.[45] Onder art. 126ng wordt verstaan dat de OvJ een vordering mag doen op communicatie bij een aanbieder van een communicatiedienst en gebruiker daarvan. Ook lazen we een aantal keer dat het in sommige rechtszaken niet is gelukt om de encryptie te ontsleutelen. Dit kan verschillende redenen hebben zoals dat er toegang werd gevraagd tot het betreden van een WhatsApp account maar dit verzoek is afgewezen door de rechtbank.

We willen deze paragraaf besluiten met een quote van een van de geïnterviewde OvJ's. *"Mijn grootste zorg zit niet zo zeer in dat encryptie de opsporing zo moeilijk maakt. Mijn grootste zorg zit er denk ik in dat we met elkaar ons moeten realiseren om encryptie te doorbreken, of we dat nou doen met wachtwoorden of met vingers of andere manieren, dat we daarvoor bestaande opsporingsbevoegdheden soms in dat licht uitleggen. En ik zou van de politiek of van de minister zo graag eens een keer in nota's, in discussies in de kamer, willen horen 'natuurlijk mag je methodieken inzetten om te komen tot inhoudelijke informatie'. Want daarmee wordt mijn werk een stuk*

[44] Ter illustratie, zie: ECLI:NL:PHR:2021:565 en ECLI:NL:RBAMS:2018:8698

[45] ECLI:NL:RBROT:2019:2712

makkelijker; om uit te leggen aan collega's hoe je techniek gebruikt om alsnog tot de versleutelde informatie te komen."

Vorderen en rechtshulpverzoeken. Een geïnterviewde vertelt dat het kraken van versleutelde data veel tijd kost. Volgens hem ligt dat onder andere aan de internationale rechtshulpverzoeken die gestuurd moeten worden naar buitenlandse bedrijven. Veel zedenonderzoeken lopen vertraging op door het opvragen van informatie over bijvoorbeeld een *subscriber*. De politie vraagt dan bij techbedrijven naar enige herleidbare persoonsgegevens die gekoppeld kunnen worden aan een bepaalde bijnaam (*nickname*). Bij grootbedrijven lukt het opvragen van de informatie, maar: *"Bij kleine bedrijven in exotische landen, zoals Telegram, is dat heel moeilijk."* Zonder deze informatie kan het onderzoek ernstig vertragen. Deze geïnterviewde stelt dat in 10-20% van de zaken waar de doorlooptijd is vertraagd encryptie een bepalende rol speelde.

Een respondent geeft in het kader van rechtshulpverzoeken aan: *"[…] Het wordt steeds makkelijker om (ogenschijnlijk) vanuit het buitenland criminele activiteiten uit te voeren. Omdat rechtshulpverzoeken lang duren en veel werk zijn worden deze op districtelijk niveau vrijwel nooit ingezet. Daardoor leidt een IP-adres of bankrekeningnummer uit het buitenland bijvoorbeeld al snel tot het niet oppakken van een zaak."* Een rc legt een link met de Telecomwet, ofwel een aftapverplichting. Hij geeft aan dat in bijvoorbeeld Nederland telecommunicatiediensten moeten meewerken en ervoor dienen te zorgen dat telefoongesprekken en sms-berichten afgetapt kunnen worden. WhatsApp valt daar niet onder en kan door E2EE niet getapt worden. Wel kan in sommige gevallen worden meegelezen in een groepsapp van WhatsApp. Dit is toegestaan door de rc en gebeurt op basis van 126m Sv of 181 & 177 Sv (zie ook ECLI:NL:RBDHA:2019:14245). Een rc maakt een vergelijking met de telefoontap: *"Verschil in tappen of meelezen is niet wezenlijk te noemen."*

In andere interviews met OvJ's en rc'en werd ook gesproken over rechtshulpverzoeken. In twee interviews wordt aangegeven dat het indienen van rechtshulpverzoeken in verband met een vordering aan bijvoorbeeld Google vaak lang duurt; minimaal een half jaar, soms wel twee jaar. Amerikaanse autoriteiten stellen hieraan hoge eisen (*probable cause*). Het moet dus een zaak zijn die zich daarvoor leent (m.n. zwaardere zaken). De rc moet dan eerst toestemming geven. Het is voorzienbaar dat het niet, of niet binnen afzienbare tijd, tot enig resultaat leidt.

Ook kan het vorderen misgaan, bijvoorbeeld als er een procedurele fout wordt gemaakt. In een interview werd verwezen naar een gerechtelijke uitspraak (ECLI:NL:RBDHA:2021:8421) waarbij een officier een vordering indiende om WhatsApp communicatie in te zien waarvan mogelijk een back-up op het Google account opgeslagen stond. Omdat in de betreffende vordering stond dat de politie toegang zou krijgen tot het WhatsApp account en daar de communicatie zou veiligstellen is dit niet gehonoreerd. In de vordering had moeten staan dat dit via het Google account zou gebeuren.

Een OvJ ziet ook de internationale dimensie – aanbieders die zich in het buitenland begeven, of waar het beheer van data in het buitenland zit – als een van de grootste obstakels voor de opsporing. Dit gaat niet alleen over kwesties rondom vorderen, maar heeft ook impact op de inzet van alternatieven, zoals het opvragen van logbestanden. Een andere complexiteit die door een OvJ wordt genoemd is wanneer servers in verschillende landen staan. De uitdaging waar dan tegen aan wordt gelopen is dat men zegt niet te weten waar de data staan, of dat ze op het ene moment de ene kant uitwijzen en op het andere moment de andere. *"Ook in die gevallen vonden – en vinden – wij dat je met machtiging van een rc data kunt vorderen, maar dan dus met een analoge vordering; 181 jo 177 jo 126ng (2) Sv."*

Los van de wijze van encryptie spelen ook zaken als het wel of niet hebben van rechtshulprelaties. Het Budapest-verdrag, ook bekend als het cybercrimeverdrag, biedt de mogelijkheid om met spoed gegevens te laten bevriezen in landen die daarbij aangesloten zijn. Echter, lang niet alle landen zijn dat. Daarbij wordt ook aangegeven dat soms lastig is te achterhalen welk bedrijf nou precies toegang heeft tot welke data. *"Dan zou je wel ergens een vordering aan iemand kunnen richten, maar dan weten we niet aan wie. Of dan richten we het aan iemand en die zegt 'dan moet je niet bij mij zijn'. Dan sta je met lege handen en dan kun je wel wedervragen stellen, maar ondertussen tikt de teller door. De data zijn vluchtig, die verdwijnen."* Een kleine nuance volgde op het einde van het interview: *"Het lukt gelukkig vaak ook wel, maar dit zijn wel belemmeringen bij het uitvoeren van de voor de hand liggende alternatieven en bevoegdheden."* Ook een andere OvJ benadrukt dit: *"Er wordt altijd naar een weg gezocht om ergens bij te kunnen."*

Een respondent zegt hierover: *"[…] Ik heb gemerkt dat we er helemaal gestoord van worden, dat we bij het opvragen van informatie in het buitenland tegen allerlei problemen aanlopen. Lange wachttijden en papierwinkel waar je 'u' tegen zegt. Dat komt de doorlooptijd van onderzoeken niet ten goede en is in de digitale wereld te zot voor woorden."* Een respondent ziet een oplossing in betere wetgeving; *"Wettelijke mogelijkheden om medewerking af te dwingen bij providers ontbreekt. Capaciteit is te vaak gelabeld aan grote onderzoeken en/of bepaalde afdelingen, waardoor lange doorlooptijd aanvragen of geen inzet. Wettelijke regels beperken m.i. ook de creativiteit van medewerkers m.b.t. encryptie."* Een OvJ geeft aan dat sinds de kwestie FBI-Apple (zie hoofdstuk 1) de discussie is beslecht door hardware fabrikanten; 'we werken gewoon niet meer mee'. De OvJ noemt dit spijtig en vraagt zich hardop af *"[…] waarom kan je ons geen rechtmatige toegang geven als we een rechterlijke machtiging hebben."* Deze zienswijze hoorden we vaker: "*Ik ben positief over encryptie, maar op het moment dat je een heel duidelijke verdenking hebt en aan alle waarborgen wordt voldaan, vind ik het van belang dat je de stap kunt zetten om er in die gevallen achter te komen wat gecommuniceerd wordt en wat er op een gegevensdrager staat."* Een nuance is hier op zijn plaats. Immers, soms kunnen fabrikanten geen toegang geven. In een dergelijk geval betreft het geen gebrek aan medewerking, maar een gebrek aan mogelijkheden.

4.2.4 Duiding encryptie op het verloop van opsporingsonderzoeken

Zoals te lezen in voorgaande secties binnen paragraaf 4.2 wordt de rol van encryptie in de opsporing door geïnterviewden en respondenten zowel negatief als positief ervaren. In het merendeel van de interviews wordt de nadruk gelegd op de negatieve rol die encryptie zou spelen. De vragenlijstresultaten geven een wisselend en genuanceerd beeld in de duiding van de rol van encryptie in opsporingsonderzoeken. Twee op de vijf politiemensen (37,8%) beschouwt de rol van encryptie in opsporingsonderzoeken als positief, twee op de vijf politiemensen (42,4%) beoordeelt de rol van encryptie als negatief en een op de vijf (19,8%) is niet positief, maar ook niet negatief ten aanzien van de rol van encryptie in de opsporing. Zij zijn neutraler en/of geven een genuanceerd beeld van wat de rol van encryptie betekent in hun werk.

Het genuanceerde beeld over de rol van encryptie heeft vaak te maken met de fase waarin een onderzoek zit; in de encryptie of decryptie fase. De volgende drie tekstovernames van respondenten illustreren dit: *"In principe is encryptie zeer negatief voor de opsporing, we moeten veel meer middelen inzetten om achter de encryptie te komen. Het voordeel is echter als een encryptie gekraakt is, dit weer een schat aan informatie oplevert en dat is weer positief." "Het gebruik van*

encryptie werkt in zijn algemeenheid negatief op de meeste veel voorkomende criminaliteit waarin deze wordt gebruikt. Het breken van encryptie (Sky, Encro, etc.) heeft veel bewijs opgeleverd waardoor zaken konden worden opgepakt of succesvol konden worden afgerond." "D.m.v. EncroChat, Sky en Anom hebben we inzage gekregen in gegevens die we met klassieke methoden niet hadden verzameld. In die zin heeft het kraken van deze diensten ons veel gebracht. Echter zien we ook dat het in de actualiteit belemmerend werkt als gebruik wordt gemaakt van cryptotelefoons."

Hoewel sommige geïnterviewden de 'wapenwedloop' tussen de opsporing en criminelen ervaren als een negatief aspect van encryptie, wordt dit tegelijkertijd door een aantal andere geïnterviewden als positief aspect benoemd. Deze wapenwedloop zorgt juist ook voor dat de politie in de opsporing scherp blijft, inventiever moet worden en gedwongen wordt *out of the box* te denken. En, zoals een geïnterviewde aangeeft: *"Op een gegeven moment wordt het heel erg moeilijk, maar we blijven het kunnen.*" Ook geven enkele respondenten dit aan. "*Vaak is encryptie een belemmering van de eenvoudige weg. Uiteindelijk wordt de belemmering weggenomen, of gekozen voor een moeilijkere weg. Zelden zijn er geen alternatieven en dan kan encryptie het einde van dat bewijs in een zaak betekenen." "In geval van ontsleuteling is veelal sterk bewijs voor handen. Maar bij uitblijven van decryptie is een zaak niet persé verloren."*

Ook geven respondenten aan dat het op voorhand onduidelijk is wat ontsleutelen oplevert: *"Op het moment dat versleutelde data niet ontsleuteld kan worden, dan is er ook niet bekend wat het ontsleutelen hiervan had opgeleverd en zou je dat als negatief kunnen zien, maar is het feitelijk onbekend."* En in ander verband wordt encryptie gezien als iets wat zich nu in de maatschappij afspeelt en daarnaar gehandeld moet worden: *"Encryptie wordt gebruikt om iets te verhullen. Bij CT [contraterrorisme] is opgeven geen optie en dus ook niet relevant. Encryptie of niet. Het maakt de uitdaging des te groter. Je kunt dat niet positief of negatief noemen. Encryptie is er en we hebben het te begrijpen. De samenwerking met Hightech en digitaal is van groot belang."*

Ook OvJ's, rechters en rc'en zien encryptie niet per se als iets negatiefs of positiefs. Zij lijken op de lijn te zitten van dat het een fenomeen is dat nu speelt. Sommige vinden het lastig er een antwoord op te geven omdat het totaalbeeld ontbreekt. Een rc en een OvJ noemen het een uitdaging. De betreffende rc geeft aan: "*Het levert bepaalde belemmeringen op en ik denk dat we met zijn allen hier op een juridisch verantwoorde wijze het hoofd aan moeten bieden."* De OvJ benoemt het voorbeeld dat als je weet dat een verdachte gebruik maakt van encryptie hoe ervoor gezorgd kan worden dat deze wordt aangehouden met open device. *"Daar zijn tig manieren voor te bedenken. Dat maakt het er niet eenvoudiger op, maar er zijn wel mogelijkheden. Hetzelfde geldt voor de encryptie in communicatie. […] Het zijn uitdagende tijden, maar daar worden wel oplossingen voor gevonden."*

Ook in deze gesprekken zijn de antwoorden dus genuanceerd; het is nadelig op het moment dat het niet gekraakt of omzeild kan worden. De kans op een kansrijke vervolging c.q. veroordeling door het OM wordt geringer. Ook wordt als negatief effect aangemerkt dat het arbeidsintensief is; *"het slokt aardig wat capaciteit op door de hele keten."* Zodra de informatie wel bekend is speelt een positieve rol in het kansrijk vervolgen. *"Als je eenmaal de hobbel van rechtmatigheid van het bewijs hebt genomen is het in een aantal zaken makkelijker om tot de inhoud te komen. Sommige zaken krijg je bij wijze op een presenteerblaadje, de kernvraag, heeft de verdachte het gedaan is dan makkelijker te beantwoorden."* Een ander positief effect is dat de mogelijkheden om de encryptie te doorbreken er veel meer zicht is gekomen op en om een beeld te krijgen van wat er speelt. Door het combineren van data en andere gegevens wordt het criminaliteitsbeeld veel beter.

Er is geen duidelijk patroon te ontdekken in de duiding van encryptie. Wel blijkt uit nadere analyse dat opsporingsmedewerkers die in hun dagelijks werk vaker met gedigitaliseerde criminaliteit te maken hebben (zoals online oplichting), de rol van encryptie als licht negatiever duiden (zie tabel VI.4 in bijlage VI). Voor alle andere type delicten heeft het delict geen invloed op de duiding van de rol van encryptie. Let op dat de resultaten mogelijk beïnvloed kunnen zijn omdat er veel politiemensen uit de digitale opsporing in de sample zitten. De verdere analyses die zijn uitgevoerd – op achtergrondkenmerken, type functie, werkgebied en affiniteit met digitalisering – laten geen significante verschillen voor wat betreft de duiding van de rol van encryptie.

4.3 Encryptie en de opbrengst van opsporingsonderzoeken

Encryptie speelt ook een rol in de opbrengsten die in opsporingsonderzoek verkregen worden. In de volgende drie secties wordt daarop ingegaan (4.3.1-4.3.3).

4.3.1 Bewijs

Een positief aspect dat door meerdere geïnterviewden beschreven wordt is de schijnveiligheid die encryptie met zich meebrengt. Doordat criminelen zich veilig wanen voor het meelezen door de overheid, communiceren ze opener dan ze zouden doen zonder encryptie. Wanneer de politie dan toegang krijgt tot deze informatie, is de opbrengst groter. Het zorgt voor een schat aan data en daarmee kansen voor de opsporing. Een geïnterviewde OvJ geeft als voorbeeld het duiden van plannen en opzet, zoals bij EncroChat en Sky ECC het geval was.

Door het ontsleutelen van bovengenoemde diensten, is het intelligencebeeld van de opsporing verschoven van slechts een globaal en fragmentarisch beeld van criminele samenwerkingsverbanden naar een veel vollediger beeld van (internationale) netwerken. Dit heeft ook gezorgd voor een andere werkwijze in het vinden van zaken en bijbehorend bewijs. Of zoals een politiemedewerker het beschrijft: "*Vroeger zochten we naar een naald in een hooiberg en nu hebben we een hooiberg van naalden.*" Anders gezegd, vroeger werd bewijs gezocht voor een strafbaar feit van een zaak en nu heeft de politie ontzettend veel bewijs voor strafbare feiten waar de zaken nog bij gezocht moeten worden.

Twee respondenten op de vragenlijst vatten dit treffend samen: *"Gekraakte encryptie (PGP, SKY, ANOM, Ennetcom) heeft al zo veel bewijs opgeleverd, dat dit onmogelijk alleen met andere opsporingsmiddelen had kunnen gebeuren. Ook hebben de onderzoeken een kortere doorlooptijd. Daarnaast geeft het veel meer zicht op criminele netwerken, de rollen daarin. (Dit geldt ook voor gekraakte losse cryptodevices van verdachten in onderzoeken waar andere opsporingsmiddelen lopen)."* En: *"Encryptie biedt ook kansen, verdachten wanen zich heel veilig achter encryptie. Als je daar doorheen komt heb je vaak een hele mooie open tijdlijn, of in ieder geval veel (extra) bewijs. Het identificeren van daders en slachtoffers, of het lokaliseren van servers, is door encryptiegebruik lastig. Maar niet onmogelijk :)."*

De vraag is in hoeverre dergelijke successen in de toekomst herhaald kunnen worden nu het bekend is dat de politie ook toegang heeft gekregen tot dergelijke cryptodiensten. Een geïnterviewde ziet dit langzaam veranderen: *"Niemand vertrouwt zijn criminele cryptotelefoon meer, omdat de politie een paar keer succesvol de aanbieder heeft aangepakt met een schat van informatie. De criminelen leren daarvan. De criminelen verdelen communicatie over meerdere systemen en versluieren communicatie."*

Bovendien geeft een respondent aan: *"Mooi als er veel data beschikbaar komt door het ontsleutelen van geëncrypte data, alleen jammer dat er tactisch veruit te weinig capaciteit is om dit succesvol op te volgen."* En andere respondent zegt: *"[…] doordat er zoveel communicatie (bijv. Sky, Encro) ontsleuteld is worden we bedolven onder het bewijsmateriaal. De grootste uitdaging die ik nu zie is hoe we deze hoeveelheid data zo efficiënt mogelijk kunnen analyseren en verwerken met de beperkte capaciteit die we hebben."* Een rc nuanceert de waarde van grote hoeveelheden data. Hij geeft aan dat het erom gaat *welke* data beschikbaar zijn en dat weinig data ook veel kunnen opleveren.

Dat de politie toegang heeft weten te krijgen tot de communicatie uit een aantal cryptodiensten, betekent niet dat niet nog een onbekend aantal cryptodiensten is waar de politie geen toegang toe heeft, en criminelen dus vrij kunnen communiceren. Althans, op dit moment. Dat een bepaalde dienst nu niet te kraken is wil niet zeggen dat dit over een tijd niet alsnog lukt. Encryptie wordt in een interview dan ook beschreven als een '*wapenwedloop met tanks en antitankwapens'.* Criminelen verzinnen steeds nieuwe manieren om hun criminele activiteiten uit te voeren en uit het zicht van de opsporing te blijven en de politie moet steeds nieuwe en inventievere methoden bedenken om verdachten te identificeren, lokaliseren en bewijs te verzamelen.

Geïnterviewden geven tevens aan dat de bewijswaarde van de ontsleutelde informatie sterk is. De kans dat de ontsleutelde data zijn aangepast door een willekeurige derde is klein, omdat data alleen kunnen worden aangepast met de juiste sleutel die moeilijk toegankelijk is. Ter illustratie, de data van Ennetcom, PGP-safe, EncroChat en Sky ECC zijn ontsleuteld met de juiste encryptiesleutels. Normaal gesproken is er één iemand die de sleutel heeft, zijnde de gebruiker dan wel in sommige gevallen het bedrijf. Dat de betrouwbaarheid van ontsleutelde data groter is moet nog doordringen in de strafrechtketen, aldus een landelijke OvJ. Bij een geïnterviewde rechter is deze bewustwording er in ieder geval wel. Hij geeft aan: *"Als je digitaal bewijs hebt wat ontsleuteld is, dan voelt dat voor mij sterker dan een getuige. Over getuigen zijn veel boeken geschreven dat die zich kunnen vergissen. In mijn ogen is de data, als deze eenmaal is ontsleuteld, ook betrouwbaar. De bewijswaarde is in die zin vrij groot."* Een andere OvJ beaamt dit ook. Hij legt dat uit met een voorbeeld over een drugszaak. Daarin werd communicatie gevonden over de handelingen om drugs te maken waarin tevens een afbeelding werd meegestuurd van het lab waar men bezig was alsook van de drugs zelf. Het gaat dan om 'real evidence'. Digitaal bewijs kan ook worden gebruikt bij het weerleggen van een alibi, wanneer bijvoorbeeld een verdachte wordt geconfronteerd met digitale sporen, zoals locatiedata.

Encryptie leidt volgens geïnterviewden tot een vermindering van directe toegang tot bewijs. Eén geïnterviewde beschrijft het als: *"Ik zie encryptie als iets dat ons iets heeft afgenomen, waardoor we nu daarin moeten zoeken. Vroeger kon dat makkelijker, zoals verdachten lokaliseren. Het is niet anders dan vroeger, maar er is een extra drempel waar we overheen moeten."* Zo is er minder directe toegang tot bijvoorbeeld WhatsApp data (behalve metadata) en tot de cloud. *"Aanbieders geven aan dat ze zelf de data versleutelen, dus ze kunnen zelf de data ook niet lezen. Dat betekent dat er geen alternatief is om encrypte data in handen te krijgen, omdat de aanbieder zelf ook geen leesbare inhoud heeft. Dat begint zich langzaam te verspreiden naar meer metadata, dus ook locatie gegevens. Dus waar we nu nog wel kansen zien, anders dan inhoudelijke inhoud om mensen te identificeren en lokaliseren, verwachten we dat die kansen in de toekomst ook minder worden."*

De vermindering van de opbrengst in opsporingsonderzoeken zorgt ervoor dat het moeilijker wordt om bewijs te verzamelen. *"In elke zaak is wel één gegevensdrager die niet open is geweest. Dat zorgt ervoor dat je vanuit je onderzoek minder informatie genereert. Dit speelt niet alleen een rol in je*

eigen onderzoek maar ook binnen de opbrengst van nieuwe onderzoeken." Een andere geïnterviewde geeft aan: *"Soms ben je afhankelijk van data uit verzegelde containers en dan heb je niks voor een rechtszaak. Dat is pech hebben. Het kan soms je zaak maken of breken."* Een andere geïnterviewde is er zeker van dat verdachten zijn vrijgekomen omdat het niet is gelukt encrypte data te kraken of anderszins toegang te krijgen. Dan was er te weinig ander bewijsmateriaal en leunde de zaak uitsluitend op ontsleutelde data die tot een veroordeling konden leiden.

We vroegen de respondenten ook welke rol encryptie speelt in de opbrengst van opsporingsonderzoeken, zie tabel 4.7. Zoals is te zien speelt encryptie overal een rol. Het is te context-specifiek om hier harde conclusies aan te verbinden. Wel zien we dat voor een aantal onderdelen de scores op 'veel' en 'altijd' hoger is. Dit betreffen: het verkrijgen van informatie, het onderscheppen van communicatie (tappen) en de mogelijkheden om bewijsmateriaal te vergaren.

Tabel 4.7: Rol encryptie in opbrengst opsporingsonderzoeken (N=177)

Terreinen	**Niet**	**Weinig**	**Niet weinig/ Niet veel**	**Veel**	**Altijd**	**Weet niet**
Het verkrijgen van communicatie/data	0,6%	2,8%	9,6%	62,7%	21,5%	2,8%
Het onderscheppen van communicatie (tappen)	0,6%	7,9%	9,6%	53,7%	23,7%	4,5%
De mogelijkheden om bewijsmateriaal te vergaren	1,1%	3,4%	16,4%	62,7%	13,6%	2,8%
De mogelijkheden om criminele samenwerkingsverbanden vast te stellen	1,7%	5,1%	16,4%	57,6%	14,1%	5,1%
De mogelijkheden om criminele activiteiten vast te stellen	0%	9,0%	15,3%	58,8%	12,4%	4,5%
Het verkrijgen van toegang tot data, anders dan communicatiedata	0%	5,6%	24,9%	50,3%	13,0%	6,2%
De mogelijkheden om relaties tussen personen, goederen en locaties vast te stellen	1,7%	5,6%	27,1%	53,7%	7,9%	4,0%
De kans om relevante personen te identificeren	0,6%	7,9%	27,7%	50,8%	9,6%	3,4%
De kans op relevante personen te lokaliseren	1,1%	16,4%	37,9%	33,9%	6,2%	4,5%
De kans op relevante goederen te lokaliseren	0,6%	16,4%	39,0%	29,9%	6,2%	7,9%
De kans om relevante goederen te identificeren	1,1%	15,8%	39,5%	31,1%	5,6%	6,8%

We vroegen de respondenten vervolgens naar hoe vaak zij inschatten dat hun team een opsporingsonderzoek succesvol kan afronden in het geval de encryptie van een potentieel bewijsstuk niet is te kraken of omzeilen (bijv. omdat andere bewijslast voldoende is). Daarop antwoorden zij als volgt, zie tabel 4.8. Ook hier is sprake van een wisselend beeld bij de respondenten.

Tabel 4.8: Afronden opsporingsonderzoek zonder toegang door encryptie (N=177)

	0 tot 25% van de gevallen	25 tot 50% van de gevallen	50 tot 75% van de gevallen	75 tot 100% van de gevallen	Weet niet / niet van toepassing
Succesvol afronden	13,0%	30,5%	37,3%	12,4%	6,8%

De opbrengst in opsporingsonderzoeken kan opgedeeld worden in vier grotere categorieën: (i) het identificeren en/of lokaliseren van relevante personen, (ii) het vaststellen van

samenwerkingsverbanden of relaties tussen personen, goederen en locaties, (iii) de mogelijkheid om criminele activiteiten vast te stellen en (iv) het vergaren van bewijsmateriaal. De rol van encryptie op deze vier categorieën komen nu aan bod, waarbij is geput uit de interviews.

Identificeren en/of lokaliseren van relevante personen. Het is technisch en tactisch soms ingewikkeld om personen te identificeren. De werkelijke gebruiker van de gegevensdrager moet achterhaald worden op basis van onder andere nicknames, nummers en identiteiten die verstrekt worden door een provider, aldus geïnterviewde politiemensen. Hoewel het identificeren en lokaliseren van relevante personen door encryptie lastiger is geworden is het niet ondoenlijk. Het uitlezen van een telefoon, het verkrijgen van een locatie, data of een globaal beeld om vervolgens daarmee iemand te identificeren is in veel gevallen nog wel mogelijk, bijvoorbeeld met de metadata die beschikbaar zijn. *"Als je metadata hebt en je op IMEI-nummer van de telefoon gaat kijken zie je bij welke telefoonpalen die telefoons zich vaak bevinden. Als die telefoon elke dag om twaalf uur 's nachts zich op een bepaalde locatie bevindt kun je op een gegeven momenten gaan aannemen dat die persoon de telefoon daar neerlegt omdat hij daar waarschijnlijk slaapt. En dan heb je een aanwijzing om daar te gaan kijken. Als je dan nog meer metadata hebt dat hij elke dag of wekelijks op de A4 langs een paal rijdt richting Amsterdam, dan heb je nog meer aanwijzingen en kun je met die metadata wel tot de identificatie van een verdachte komen."* Een OvJ geeft aan dat door metadata – patroonherkenning, meereizende telefoons – identificatie blijft kunnen. Sommige applicaties geven bijvoorbeeld locatiegegevens onversleuteld weer via de tap. Een andere geïnterviewde geeft aan dat door de uitrol van 5G het identificeren van personen lastiger gaat worden.

Daarnaast kan een combinatie van gegevens gebruikt worden, bijvoorbeeld door de locatiegegevens van de telefoon en informatie vanuit het netwerk (bijv. Vodafone en KPN) te combineren. Ook bij het verkrijgen van een IP-adres kan verder onderzoek worden gedaan naar de identificatie van een persoon. Als een IP-adres uit een ander land komt wordt het lastig om het aan een persoon te koppelen omdat andere landen vrijwel geen gegevens omtrent IP-adressen bewaren.

Het succesvol identificeren en lokaliseren van verdachten is afhankelijk van de zwaarte van encryptie en technische capaciteiten van de verdachten. Zo wordt verteld dat het identificeren van een persoon die gebruik maakt van het internet en daar meerdere versleutelings- of afschermingsprotocollen voor gebruikt, vrijwel ondoenlijk is en ongelofelijk veel moeite kost. *"De succesratio als we het hebben over echt goede criminelen, ligt denk ik zeer laag. Ik doe een slag in de lucht. Ik denk dat de succesratio onder de 5% ligt om iemand te identificeren en lokaliseren."*

Zoals al eerder is beschreven kan encryptie ook een positieve rol spelen in de opbrengst van het identificeren van personen. Er wordt door geïnterviewden verteld dat de identificatie van een persoon technisch lastiger is geworden, maar dat door het ontsleutelen van cryptodiensten het identificeren tegelijkertijd bij bepaalde zaken op bulkwijze kan. *"Met PGP et cetera hebben we ook allerlei data achter elkaar gelegd. Bij de eerste hadden we veel moeite om te identificeren, bij de tweede hadden we al een heleboel mensen geïdentificeerd die Ennetcom gebruikten, en die zeiden massaal we gaan naar Sky [ECC]. Zelfde gebruikersnamen, zelfde paallocaties, die metadata kan je over elkaar heen leggen en dan weet je veel meer. Dus identificatie, ja, we draaien nu dossiers in elkaar zonder dat we de verdachte getapt, gevolgd of gezien hebben. Bij wijze van spreken kunnen we met een druk op de knop de gespreksdata van een boef binnenhalen."* Een nuancering van een andere geïnterviewde is dat het bewijs uit cryptodiensten vaak niet realtime is: *"De politie kon maximaal twee maanden meekijken*

bij live communicatie van EncroChat, buiten die twee maanden weten wij niet waar EncroChat gebruikers mee bezig zijn."

Vaststellen van samenwerkingsverbanden/relaties tussen personen. Wat betreft het vaststellen van samenwerkingsverbanden of relaties kan een onderscheid gemaakt worden tussen 'reguliere' opsporingszaken en cryptodienstzaken. Bij reguliere zaken speelt encryptie een negatieve rol. Het wordt moeilijker omdat je als politie minder weet, en die kennis het uitgangspunt is voor een zaak. Dit leidt volgens een geïnterviewde tot minder bewijs over het netwerk. Waar normaal gesproken een sneeuwbaleffect optreedt van informatie op basis van bewijs uit de data, is hedendaags veel afhankelijk van medewerking van verdachten die iemand noemen of buiten de omgeving slordig zijn omdat ze bijvoorbeeld iemand gebeld hebben. Daarnaast is een positief aspect van encryptie, zoals eerder beschreven, dat door het ontsleutelen van cryptodiensten het intelligencebeeld van de betreffende criminelen veranderd is van fragmentarisch naar meer een totaal netwerkoverzicht. Voorwaarde is hier dus wel dat eerst de data achter encryptie inzichtelijk moeten zijn.

Mogelijkheid om criminele activiteiten vast te stellen. Geïnterviewden geven aan dat encryptie een rol speelt in het vaststellen van criminele activiteiten. Hierbij gaat het vooral om de eerder beschreven 'mens-gedreven' encryptie. *"Mensen die willens en wetens met verkeerde dingen bezig zijn, zijn over het algemeen bewust met encryptie bezig."* Zo wordt PGP telefoongebruik waarbij hoge kosten gemaakt worden bijvoorbeeld wel als verdacht gezien voor een reguliere gebruiker. Dan wordt de vraag gesteld waarom de verdachte zoveel privacy nodig heeft. Er wordt verteld dat op ontsleutelde of open gegevensdragers met encryptie vaak belangrijke zaken zijn aangetroffen die als bewijs kunnen gelden in een strafzaak. Op het gebied van kinderpornozaken kan bijvoorbeeld worden gedacht aan notulen van vergaderingen van forumbeheerders en foto's waar ook andere mensen op staan. Ook als een platform gevonden wordt welke voor criminele doeleinden gebruikt wordt dan gaat er een 'doos van Pandora' open wanneer deze ontsleuteld wordt. Wat betreft 'technologie-gedreven' encryptie is het lastiger om criminele activiteiten vast te stellen. Het is moeilijk te zeggen dat iemand die WhatsApp gebruikt criminele activiteiten uitvoert. Hoe meer van die applicaties en devices standaard geencrypt zijn hoe minder dat als indicator voor criminele activiteit geldt.

Vergaren van bewijsmateriaal. De rol van encryptie op het vergaren van bewijsmateriaal wordt door de geïnterviewden voornamelijk als negatief beschreven. Ten eerste is het door versleuteling in veel zaken moeilijker en tijdrovender geworden om bewijs te vergaren. De toegang tot de inhoud van gegevensdragers en het vorderen van informatie is beperkter geworden. Op het gebied van kinderporno is dit voor eenvoudigere delicten een minder groot probleem dan voor zwaardere delicten: *"Dan wordt de computer gewoon geopend door de verdachten en vinden we het bewijs uit downloaden en bezit."* Deze beperking tot het verkrijgen van informatie wordt door een geïnterviewde als volgt beschreven: *"Waar we vroeger keuze hadden aan gegevensdragers die inhoud hadden, die worden allemaal minder. Je gaat voor die ene computer waar je de verdachte achter aantreft en daar moet je het van hebben. De versleuteling blijft sterk en kunnen we heel weinig mee. De opbrengsten die je in handen krijgt, die nemen af. Hetzelfde met het vorderen van gegevens, we krijgen geen inhoud via andere wegen dan via interceptie."*

Ook al is de bewijslast van zaken vaak niet enkel afhankelijk van data, de data kunnen in een zaak uiteindelijk wel van doorslaggevende factor zijn. *"Als je niet genoeg bewijs hebt gaat de rechter daar niet in mee. Dit bewijs kan in deze data zitten. Er zijn sowieso verdachten die niet veroordeeld zijn,*

alleen omdat het bewijs niet rond is gekomen (ze zouden wel veroordeeld zijn als er toegang was tot de versleutelde data).” Een ander zegt: *“De waarde van de [ontsleutelde] berichten is heel hoog.”*

Een OvJ noemt een voorbeeld van een onderzoek waar de inzet van opsporingsbevoegdheden, zoals een tap en observatie, niets opleverde, maar wel veel tijd in beslag nam. Op het moment dat de versleutelde data ontsleuteld waren, viel op dat de verdachte diverse drugslabs aanstuurde. Dit was cruciaal bewijs dat als dat niet voorhanden was geweest de zaak ook niet opgelost had kunnen worden. De OvJ zegt hier verder over: *“Dat soort zaken wordt veel bij ondermijning gedraaid. Eigenlijk zijn die ontsleutelde cryptodata waar wij beschikking over hebben, de bron van gigantisch veel zaken en ook heel veel [van de zaakdossiers] is bijna, voor 70%, gebaseerd op die ontsleutelde communicatie.”* Verder wordt gesteld dat wanneer op geprioriteerde wijze wordt omgegaan met die grote hoeveelheden data dat veel tijdswinst oplevert. Hij onderbouwt dit met een voorbeeld van moordzaken. Daarbij kan veel tijd gaan zitten in bijvoorbeeld het opsporen van mensen die aanwezig waren in de omgeving om getuigenverklaringen te verkrijgen en vervolgens die personen te verhoren. *“Op het moment dat je de communicatie net voorafgaand aan het overlijden hebt, en je hebt dat decrypted, in combinatie met een moordwapen of iets anders, dan is dat een zaak die je veel sneller afrondt.”*

4.3.2 Strafrechtelijke vervolging

In de interviews is gevraagd naar de mogelijke rol van encryptie in de strafrechtelijke vervolging van zaken. Het Voorziening Crypto Analyse Team (VCAT) van de Nederlandse Politie faciliteert het landelijk netwerk van crypto analyse teams om te zorgen dat decrypte data op een rechtmatige manier in onderzoeken terechtkomen en als bewijs kunnen dienen. Ze analyseren zichtbaar gemaakte data en adviseren bij opsporingsonderzoeken waar gebruik wordt gemaakt van crypto-communicatiedata en de specifieke voorwaarden die gelden voor het gebruik ervan. VCAT is het enige contactpunt in het land over decrypte data richting het OM.

Encryptie kan, net als in de opsporing, een negatieve en positieve rol hebben op de strafrechtelijke vervolging. Encryptie kan enerzijds ook hier voor vertraging zorgen. Allereerst omdat de data of devices ontsleuteld moeten worden, wat tijd kost. Maar ook het vast stellen van identiteiten kan lastig zijn, bijvoorbeeld door gebruik van *“VPN-diensten, wegwerp e-mails en simkaarten die continu worden gewisseld.”* Ook het opvragen van gegevens bij (technische) bedrijven kost veel tijd, vooral als gewerkt wordt met internationale rechtshulpverzoeken.

Door de complexe internationale wet- en regelgeving maken buitenlandse rechters de keuze wie deze ontsleutelde data mogen gebruiken en onder welke voorwaarden. Eén geïnterviewde trekt het breder door te stellen dat al het digitaal bewijs zorgt voor vertraging, omdat gegevens beperkt bewaard mogen worden. De bewaartermijn is afhankelijk van dataretentie (bewaren van gegevens) wetgeving per land. Niet elk land heeft retentie wetgeving, waardoor het bewaren en ophalen van informatie lastig is. Hoewel het langer kan duren voordat men toegang heeft tot de data, zijn er altijd andere bewijzen nodig om het delict voltooid te krijgen.

De ene geïnterviewde vindt ontsleutelde data slechts bijvangst, terwijl het voor een andere een belangrijke bron is voor de bewijslast. In de verdiepende interviews gingen we nader in op bijvangst versus essentieel belang van ontcijferde informatie. De OvJ’s waarmee is gesproken zien het als essentieel en niet als bijvangst. Ook kan het zijn dat het bewijs niet rond wordt gekregen omdat simpelweg niet bij de gegevens kan worden gekomen. Als de politie niet bij belastende gegevens kan

komen, kan het zo zijn dat er niet tot vervolging wordt overgegaan omdat de zaak niet te bewijzen is. Echter, het is nooit helemaal duidelijk welke gegevens er ontbreken omdat deze versleuteld zijn.

Een aantal rechters nuanceert het beeld van de belemmerende rol van encryptie enigszins. Een van hen stelt dat versleutelde informatie 'best vaak' een rol speelt, maar niet altijd. Zo zijn bijvoorbeeld regelmatig WhatsApp gesprekken onderdeel van strafzaken. Die zijn in principe versleuteld, maar dergelijke gesprekken worden door verdacht vaak door henzelf geopend en gegeven voor de strafzaak, waardoor encryptie dan geen rol meer speelt. *"Uiteindelijk gaat het over bewijs. Er zijn heel veel zaken waarbij het enige bewijs de onversleutelde informatie is."*

Anderzijds heeft encryptie ook een positieve rol op de strafrechtelijke vervolging. Als een telecomdienst, zoals EncroChat, is ontsleuteld ontstaat er zoveel bewijs dat de zaken erbij moeten worden gezocht. *"We hebben nu in die hooiberg van naalden ontzettend veel kansen om boeven aan te houden en binnen te halen."* Criminelen krijgen levenslange gevangenisstraf voor liquidaties die op basis van ontsleutelde data zijn bewezen. Een geïnterviewde geeft aan dat er te weinig capaciteit is om alle zaken goed af te ronden bij de politie, justitie en bij de rechtbank. Een ander positief aspect van encryptie op de strafrechtketen is dat de doorlooptijd sneller kan gaan en de kwaliteit van de bewijsvoering hoger is. Een potentieel nadeel schuilt erin dat de ontsleutelde data niet altijd compleet hoeven te zijn volgens een rc, bijvoorbeeld dat slechts van één partij de communicatie inzichtelijk is. Een andere rc geeft aan dat dit vooral ook een kwestie was bij de Ennetcom-zaak. Dat is echter het niveau van bewijswaardering.

Er is geen goed beeld van de doorstroom van zaken met encryptie in de strafrechtketen. Wel lijkt encryptie een grote rol te spelen in de doorstroom van zaken op het moment dat er nog geen toegang is tot de versleutelde data. Een OvJ benoemt in het kader van encryptie het volgende: *"Leidt dat er nou toe dat er mensen vrijuit omdat we daar geen toegang tot hebben? Ja, dat leidt daar toe. Betekent het dat we die mensen wel hadden kunnen vervolgen en kunnen veroordelen als we toegang hadden gehad? Dat kunnen we niet zeggen, omdat we niet weten of daar bewijs was."* Een andere OvJ benadrukt het belang van een goede voorbereiding op een klapdag (aanhouding) om bewijs in onversleutelde staat in beslag te nemen. Als het niet lukt om achter de encrypte informatie te komen kan het zijn dat de verdachte niet wordt vervolgd. Twee andere geïnterviewden hebben het gevoel dat er meer encryptie voorkomt in de doorstroom van kinderpornozaken dan bij bijvoorbeeld inbraken.

In de interviews met rechters en rc'en wordt vooral gewezen dat encryptie vertragend werkt. Vooral bij de eerste zaken zou het hebben geleid tot 'enorm oponthoud', en hoewel er nu betere kaders zijn, is het voor een deel nog steeds vertragend. Een van de rechters benoemt dat alle grote strafzaken die gebaseerd zijn op ontsleutelde data van cryptotelefoons 'stroperig' zijn worden. Dit komt vooral doordat in de afgelopen tijd een discussie heeft gespeeld over de rechtmatigheid van de ontsleutelde data van cryptotelefoons. De rechtmatigheidsdiscussie – dat vooral in het teken staat van het recht op een eerlijk proces – komt in elk interview met de rechtspraak terug. De vraag voor de strafrechter is dan: Hoe kom je bij de inhoud? Is het rechtmatig verkregen? Wie kan de integriteit van de data garanderen? Dat vergt van de strafrechter dat ze zich in technische details moeten verdiepen, omdat er nieuwe rechtmatigheidsvragen komen. Dit geldt overigens ook voor de rc.

Er wordt in de interviews gesteld dat er nog veel onduidelijkheden zijn over de rechtmatigheid van ontsleuteld bewijs. Bijvoorbeeld in hoeverre de politie in een telefoon mag kijken zodra deze ontsleuteld is. Moet dit altijd via een rc, of alleen bij ernstige zaken? Bij het dark web of telefoons is het de vraag in hoeverre er sprake is van bulkdata en hoe zich dat verhoudt tot de rechtspraak. *"Als er*

geen verdachte op het oog is en gezocht wordt op een woord zoals stash of loods in de ontsleutelde dataset, is dat dan rechtmatig?" Een rc benoemt ook dat dit momenteel een discussie is. Immers: *"[…] want in de telefoon staat je hele leven."* Een andere rc zegt: *"Er gaat geen rechter-commissaris toestemming geven om heel WhatsApp binnen te halen. Dat zou disproportioneel zijn."* In relatie tot rechtmatigheid van bulkvergaring door ongericht gegevens binnen te halen zijn in het geval van Sky ECC en EncroChat prejudiciële vragen gesteld bij de Hoge Raad.

Een geïnterviewde rc noemt nog twee nieuwe bevoegdheden die raken aan encryptie. Deze kennen hun oorsprong in de Innovatiewet. *"De eerste: Wat doe je als een telefoon in beslag is genomen en er komen nog nieuwe berichten op binnen? Mag je daar dan kennis van nemen?"* Daar was tot nu toe nog geen wettelijke bevoegdheid voor. Soms werd het gezien als bijvangst. De Innovatiewet biedt de mogelijkheid dat als na bijvoorbeeld negen maanden de telefoon open is de berichten van de eerste twee weken na inbeslagneming bekeken mogen worden, om het proportioneel te houden. De tweede nieuwe bevoegdheid is de netwerkzoeking na inbeslagneming. Nu mag deze alleen plaatsvinden tijdens de doorzoeking. *"Dit kan lang duren als je bijvoorbeeld een hele Google take-out wil doen. Dat duurt soms dagen. Dat is een enorme inbreuk voor mensen die daar wonen."* Met de Innovatiewet kan een apparaat in beslag worden genomen en mag buiten de doorzoeking om een netwerkzoeking worden gedaan. Hier zitten strenge regels aan vast; er komt altijd een rc aan te pas en er moet kritisch worden gekeken van welke periode de gegevens worden vastgelegd en van welke applicaties of servers. De bevoegdheid tot netwerkzoeking valt onder art. 557 Sv.

Het gebruik van informatie uit ontsleutelde encryptie zorgt ook voor een andere tactiek van advocaten, aldus geïnterviewden. Bij de strafzaken waarin het bewijs uit EncroChat wordt gebruikt proberen de advocaten aan te voeren dat de opsporingsinstanties de informatie op niet rechtmatige wijze hebben verzameld. Advocaten hebben dit bij het kraken van Ennetcom (een aantal jaar eerder) ook geprobeerd. Volgens een geïnterviewde is in hoger beroep geoordeeld dat het kraken van Ennetcom legitiem was, daarmee bleven de strafzaken ook valide. Bij de EncroChat-strafzaken proberen advocaten de legitimiteit van de kraak onderuit te halen. Het is nog onzeker of de legitimiteit van de EncroChat kraak bewezen kan worden. Dit is nog niet in hoger beroep geweest.

Voor het VCAT is het daarom belangrijk om in elk deelonderzoek aan de hand van dezelfde procedures en processen te werken, zoals eenduidige processen verbaal. Daarin wordt uitgelegd hoe de data zijn verkregen, hoe de telefoon heeft gewerkt, hoe het team de data hebben benaderd en welke toestemmingen er zijn gegeven door de rechter. Zodra in hoger beroep besloten wordt dat de op EncroChat achterhaalde informatie niet legitiem is verzameld, dan heeft dat gevolgen voor alle strafzaken waarin bewijs is aangevoerd uit de EncroChat-databases. Dat zorgt ervoor dat het OM en de advocaten deals sluiten, om er zeker van te zijn dat de verdachte een straf krijgt. Als besloten wordt door de Hoge Raad dat de data op onrechtmatige wijze zijn verkregen dat heeft dat waarschijnlijk grote gevolgen voor de andere 1.200 tot 1.300 zaken waar informatie uit dezelfde dataset is gebruikt, aldus politiemedewerkers.

4.3.3 Rechterlijke afdoening

Op basis van de oriënterende interviews lijkt encryptie een minimale rol te spelen in de rechterlijke afdoening van strafzaken in tegenstelling tot de uitkomsten uit de verdiepende interviews. Om de resultaten van deze specifieke paragraaf in een accuraat perspectief te plaatsen is het belangrijk om

deze vraag ook aan de doelgroep te stellen die rechtstreeks betrokken is bij de rechterlijke afdoening. Daarom hebben we vanuit RM perspectief een vijftal interviews afgenomen.

We vroegen aan de geïnterviewde rechters en rechter-commissarissen (rc) om kort hun rol te duiden. De rechter moet met name een beslissing nemen, alle argumenten aanhoren en wegen en de rechtmatigheid en de basiswaarde van de rechtstaat in de gaten houden. Het is op grond van art. 6 EVRM en het EU-verdrag essentieel om te kijken of het dossier als geheel betrouwbaar en evenwichtig is en er geen grondrechten zijn geschonden op een wijze die valt buiten de bestaande bevoegdheden op dit punt. Een ander zegt over de rol: het onderzoeken van de aantijgingen van het OM jegens een subject/verdachte en dan beslissen of het al dan niet strafbaar is en of daar een straf voor moet komen. Een rc heeft een meer toezichthoudende rol; een soort 'poortwachter'-functie in het opsporingsonderzoek om te toetsen of alles volgens de regels verloopt, waaronder ook digitale opsporingsbevoegdheden.

Daarna vroegen we door op in hoeverre encryptie in zaken iets betekent voor die rol. Daarop worden verschillende antwoorden gegeven. Encryptie speelt wel degelijk een rol in strafzaken. Een rechter geeft aan dat encryptie een rol speelt zodra de politie dingen gaat ontsleutelen. Meestal heeft die rol volgens hem betrekking op cryptotelefoons. Wanneer encryptie op dergelijke telefoons is versleuteld komen grote hoeveelheden data aan het licht. *"In hoeverre dat onderzocht mag worden en hoe dat mag, heeft te maken met rechtmatigheid. De rechter beoordeelt de rechtmatigheid van het onderzoek en de waardering of het klopt wat eruit is gekomen."* Hoewel rechters niet zozeer kijken naar hoe encryptie technisch ontsleuteld wordt, kijken ze wel in hoeverre data onderzocht mogen worden.

Rechters en rc'en geven aan dat encryptie in principe niet bijzonder is voor hun werk, met uitzondering van de grote hoeveelheden data die eruit voort kunnen komen. Dit kan soms leiden tot capaciteitsproblemen. Als er veel informatie voorhanden is, bijvoorbeeld in de zaken van EncroChat en Sky ECC, dan duurt het lang door de rechtmatigheid verweren en pro forma beslissingen.

Capaciteit kan soms ook worden uitgespaard. In een kleine zaak kan bijvoorbeeld jaren onderzoek worden gedaan, maar 'soms is genoeg', want er zijn ook andere zaken die liggen te wachten, aldus een geïnterviewde rc. Bij encryptie speelt capaciteit zo een rol, om te kijken of er nog tijd in een apparaat gestopt moet worden of dat er al genoeg bewijs is verzameld. *"Als een verdachte na een maand bekent en de telefoon is nog versleuteld, dan kan je beter stoppen met dat onderzoek en de capaciteit op een andere zaak inzetten."*

Rc'en geven aan dat de hackbevoegdheid is ontstaan omdat er minder wordt gebeld en omdat er encryptie is. Taps leveren weinig op en IP-taps meestal versleuteld materiaal. Met de hackbevoegdheid wordt getracht vóór de versleuteling op het apparaat zitten, zodat er geen hinder wordt ervaren door encryptie. *"Het is meer dat er encryptie is en daarvoor bepaalde bevoegdheden in het leven zijn geroepen dan dat encryptie een andere beoordeling geeft."* Volgens deze rc wordt de hackbevoegdheid steeds vaker ingezet. Een rechter geeft hierbij aan dat voordat een machtiging kan worden verleend aan zware eisen moet worden voldaan. Hierbij speelt ook het aspect subsidiariteit; dat zwaardere bevoegdheden pas worden inzet als minder zware bevoegdheden geen soelaas bieden. Als verdachten geen medewerking verlenen moeten andere manieren worden verzonnen *"om binnen de grenzen van wet en recht met vrucht onderzoek te doen."*

Een geïnterviewde OvJ geeft aan dat de hackbevoegdheid, op het moment van het interview, 28 keer is ingezet. *"Ten opzichte van de duizenden zaken waarin we dit tegenkomen, is dat natuurlijk*

bijzonder weinig." Volgens hem is dat onder andere te wijten aan een gebrek aan bekendheid van deze mogelijkheid binnen het OM. Het belangrijkste probleem is echter het niet mee kúnnen werken van degene die het in bezit heeft, omdat de informatie niet door een partij zelf ontsleuteld kan worden. Omdat zo'n partij dat niet kan hoeft er ook niet meegewerkt te worden aan een decryptiebevel. Een OvJ die veelal met cyberzaken aan het werk is geeft aan dat de bevoegdheid in die hoedanigheid wel wordt ingezet, maar zich ook kan voorstellen dat deze in andere typen zaken minder wordt gebruikt. Het vereist enige technische kennis en de 'papierwinkel' die ermee gemoeid is kan afschrikken. Deze OvJ wijdt het niet zozeer aan de onbekendheid ervan binnen het OM, maar ziet vooral winst in het praktischer uitleggen ervan; voor welke type zaken kan het worden ingezet en wat is ervoor nodig om dat te doen.

Een andere rc zet zijn vraagtekens bij de houdbaarheid van deze bevoegdheid. *"Het is een vergaande bevoegdheid, want je neemt het apparaat over en een privéleven van een persoon. Het wordt tot nog toe sporadisch ingezet. Uiteindelijk komt het denk ik allemaal neer op een proportionaliteitstoets: is het voor het onderzoek voldoende van belang als je het afzet tegen privacy schending."* Ook zegt hij dat de inzet van de hackbevoegdheid veel geld kost, omdat de politie daarvoor eenmalige licenties moet kopen. Daarnaast is zijn observatie dat de inzet van de bevoegdheid vaak niet tot direct bewijs heeft geleid, met uitzondering van PGP-telefoons, maar vooral sturingsinformatie heeft opgeleverd.

Tevens wordt aangegeven dat collega-rechters het wellicht ingewikkeld vinden om encryptie te bevatten en het in een juridisch kader te plaatsen. Een rc geeft aan dat technische basiskennis wel nodig is bij rechters. Een rechter moet kunnen beslissen of een middel goedgekeurd is en integer is ingezet. Een andere rechter stelt dat het de kunst is voor rechters om zich niet te laten afschrikken op het gebied van technologie. *"Het is fijn om iets te begrijpen. Je moet willen begrijpen hoe dingen werken, hoe er met WhatsApp omgegaan wordt en wat een dark web is, maar je hoeft niet alles te weten om juridisch te kunnen oordelen. Die basiskennis is er wel, als je je niet laat afschrikken door de computertermen."* Bovendien geeft hij aan dat over het algemeen goede uitleg wordt gegeven over bijvoorbeeld de werking van harde schijven in kinderpornozaken. Een rc geeft daarbij een uitdaging aan: *"Je moet kennis vergaren, deels door het OM te vragen, en tegelijkertijd kritisch en onafhankelijk blijven."*

Een andere rc meldt in dit verband dat er een cursus 'cyber voor rechter-commissarissen' is waarbij wordt getracht ervoor te zorgen dat iedereen de basis op orde heeft en doorsnee beslissingen kan nemen. In deze cursus komen zaken aan de orde als doorzoekingen, netwerkzoekingen, cryptovaluta, bijzondere opsporingsbevoegdheden, zoals het vorderen van gegevens, en de hackbevoegdheid. Deze onderwerpen worden als 'doorsnee' omschreven omdat ze in elke zaak voorkomen. Bijvoorbeeld bij grootschalige onderzoeken, zoals moord- en doodslagzaken, proberen ze deze bevoegdheden allemaal in te zetten.

Een andere geïnterviewde benadrukt dat de zaken technisch complexer worden en het daarom van belang is dat politie, justitie en de rechtbank meer mensen aannemen met digitale affiniteit. Bovendien zijn er zoveel zaken met een encryptie element (de hooiberg met naalden), waar te weinig capaciteit voor is. Daarom is het van belang dat de rechtbank en het OM uitbreiden om de zaken op te pakken. We zagen in een open invoerveld in de vragenlijst ook een hulpvraag op dit thema. *"Ondanks veel discussie is er nog niemand in Nederland die mij heeft geholpen met het rechercheren binnen de crypto bestanden in algemene zin."* Niet alleen complexiteit speelt een rol, ook moeten ontwikkelingen

worden bijgehouden. Zo stelt een van de geïnterviewden dat jeugdige daders minder gebruik maken van WhatsApp en bijvoorbeeld meer op Snapchat zitten.

Een OvJ vat dit als volgt samen: *"Politie en OM zullen zich moeten aanpassen aan een nieuwe en blijvende andere vorm van opsporen en vervolgen. Nu blijft men bij de opsporing nog te veel in het oude karrespoor en wordt te weinig de data benut. Bij het wel benutten wordt nog te veel teruggegrepen naar de extra inzet van gebruikelijke middelen terwijl het bewijs al aanwezig is. De strategische laag zal zich moeten aanpassen aan de nieuwe omstandigheden die decryptie biedt. Dat geldt niet alleen voor het keuzemodel maar ook de inzet van personeel en efficiënt opsporen."* Deze OvJ voorziet dat door de hoeveelheid en snelheid waarmee zaken worden aangedragen voor een 'verstopping in het systeem' zal zorgen. Hij geeft tevens aan dat met alleen het uitbreiden van capaciteit het probleem niet wordt opgelost.

Ook kan verslaglegging een rol spelen; wanneer wordt gehint op encryptie in het dossier kan daarop worden doorgevraagd door rechters. Ter illustratie, als er alleen 'informatie uit de telefoon' in het dossier staat, dan zal de rechter vaak niet de wijze van ontsleuteling laten onderzoeken. Als niemand hier iets over zegt dan wordt hier ook niet moeilijk over gedaan. Als er wordt opgeschreven 'we hebben een telefoon ontsleuteld', dan slaan rechters daar eerder op aan. Er kunnen vragen worden gesteld zoals 'waarom eigenlijk' en 'op welke basis'?

Door encryptie is de kans groter dat een groot deel van belastbare informatie niet toegankelijk is. En er kan niet veroordeeld worden als er onvoldoende bewijs is geleverd. Als voorbeeld: drie leden van een motorclub worden verdacht van moord en uit de communicatie blijkt niet wie het heeft gedaan. *"Als drie personen het gedaan kunnen hebben, dan kunnen we daar niet één persoon voor veroordelen."* Geïnterviewden denken dat het niet kunnen omzeilen of kraken van encryptie ervoor zorgt dat vervolging eerder uitblijft of lagere straffen worden gegeven. *"Gevoelsmatig worden lagere straffen gegeven omdat er minder zicht is op wat er is gebeurd",* aldus een geïnterviewde. Aan de andere kant leiden succesvolle onderzoeken (zoals EncroChat) tot nieuwe veroordelingen. De rol van encryptie op de rechterlijke afdoening is dus onder andere afhankelijk van de hoeveelheid informatie die is onderschept.

Rechters geven ook aan dat encryptie een rol speelt in de berechting. Als de politie succesvol kan ontsleutelen, krijgen ze toegang tot (soms veel) bewijs. Als dit ontsleutelde bewijs niet voorhanden was geweest dan kunnen bij veel zaken verdachten niet vervolgd worden. Een voorbeeld is een strafzaak op het terrein van de georganiseerde misdaad waar ontsleutelde data uit cryptotelefoons als bewijs zijn opgenomen. *"In het juridisch proces zijn er verschillende stappen. Eerst of het bewijs rechtmatig is verkregen, daarna of de verdachte de juiste persoon is en tot slot de inhoud van de berichten. In dergelijke strafzaken gaat het niet vaak over de inhoud van de berichten, maar richten advocaten zich op het voorproces; hoe de informatie in het dossier is gekomen."*

Er wordt geen hogere straf gegeven bij het vermoeden van meer versleuteld belastend materiaal. *"Dat is een discussie die in andere landen wel speelt en wat in Nederland nog niet aan de orde is."*[46] Een andere geïnterviewde geeft aan dat er eerder geen vervolging is, omdat het bewijs mist. Wel kan encryptie iets zeggen over de professionaliteit waarmee iemand te werk gaat (zie ook sectie 4.1.3). Als iemand professioneel informatie heeft afgeschermd dan kan dat meegenomen worden.

[46] Uit de literatuurverkenning blijkt dat landen zoals Groot-Brittannië en Ierland een strafmodaliteit kennen als een verdachte geen wachtwoord geeft aan de politie. In de VS zijn er vervolgingen voor 'contempt of court' als een verdachte het wachtwoord wel weet maar niet wil geven.

Denk bijvoorbeeld aan een drugsdealer die een cryptotelefoon gebruikt versus een die met een simpele Nokia werkt. Of aan een kinderpornozaak waarbij een verdachte zelf iets heeft gebouwd om het ver weg te houden. Dat kan iets zeggen over de bewustheid en professionaliteit, wat dan weer van invloed kan zijn op de straf.

Sommige geïnterviewden denken dat de proceshouding van een verdachte (bijv. meewerken, openheid geven en spijt betuigen) ook een rol speelt in het strafrechtelijk proces. *"Als iemand zijn wachtwoord niet geeft wordt het hem aangerekend dat hij niet voldoende meewerkt. Het is juridisch niet strafbaar, maar heeft wel zijn uitwerkingen op officieren en rechters. Dat heeft niet alleen met encryptie te maken maar met respect tonen aan de rechtbank."* Iemand kan meewerken door zijn eigen harde schijf te geven en/of te ontsleutelen. Echter, als er bijvoorbeeld nog twintig andere versleutelde harde schijven zijn, is dat geen bewijs. Een rc geeft aan dat meewerken niet per se wordt beloond, maar dat het omgekeerd wel nadelig is wanneer een verdachte niet coöperatief is. *"Dat zou zijn weerslag kunnen krijgen in de strafmaat."* Een andere geïnterviewde zegt: *"Als een verdachte niet meewerkt om toegang te geven tot zijn harde schijf waar geen kinderporno op zou staan, maar vervolgens wel vraagt om de harde schijf terug te krijgen, dan geeft de rechter aan dat de harde schijf wordt vernietigd."*

Door de tijd die nodig is om encryptie te kraken komt in veel zaken voor dat op een later moment extra (ontsleuteld) bewijsmateriaal wordt toegevoegd. *"Laatst hebben we daardoor een gegevensdrager open gekregen en wordt er nu met terugwerkende kracht gekeken of we extra strafbare feiten hebben waar we eerder geen bewijs van hadden. […] Het delict moet wel anders zijn dan waarvoor de verdachte is veroordeeld. Bijvoorbeeld als de verdachte is veroordeeld voor bezit van kinderpornografie, maar misschien is er nu bewijs dat de verdachte het ook verspreid heeft."* Dit komt overigens naar eigen zeggen niet vaak voor.

De discussie over rechtmatigheid (zie ook sectie 4.3.2) heeft ertoe geleid dat een aantal rechtbanken op een gegeven moment procesafspraken heeft gemaakt, omdat het zo lang duurt. Een rechter zegt hierover: *"In het begin was iedereen bezig met het wiel uitvinden, nu begint het zich langzaam uit te kristalliseren. Het liep vast omdat het nieuw was, er kwam een bulk aan informatie uit de telefoons. Het OM kwam steeds met een klein stukje bewijs en weinig uitleg over hoe dit bewijs tot stand was gekomen. De advocatuur ging hier vol op in en heeft documenten opgevraagd. Stapje voor stapje kwam er meer uitleg bij. Advocaten werken nu internationaal samen en vragen gezamenlijk documenten op (bijv. uit Parijs). Er komt steeds meer informatie en het OM wordt opener met het delen van informatie, maar het gaat in kleine stapjes."* Een geïnterviewde rc geeft bijvoorbeeld aan dat hij in een zaak waarin encryptie een rol speelde het OM heeft uitgenodigd om uit te leggen hoe de data achterhaald zijn. *"Ik wil weten dat de data reproduceerbaar en controleerbaar is en wil weten welke techniek overheden in kunnen zetten om door beveiliging heen te breken. Ik wil daar zicht op hebben zonder een techneut te worden om daarover te kunnen oordelen en ook voor de controle van de zittingsrechter achteraf."*

Een andere geïnterviewde geeft aan: *"Er wordt nu vaak geschikt omdat er veel bewijs te vinden is."* Bij een schikking wordt meestal afgedwongen dat men niet in hoger beroep kan gaan. Een rechter geeft aan dat hierover op landelijk niveau wordt gesproken, omdat een aantal rechtbanken dit wel goed vindt en een aantal niet. *"Procesafspraken zijn normaal gesproken meer voor individuele zaken."* Procesafspraken zijn strikt genomen geen schikking, maar het speelt volgens een rc in sommige zaken wel een rol. De principiële vraag die speelt is: In hoeverre kan akkoord worden gegaan met de

afspraken tussen het OM en een verdachte? Het is de bevoegdheid van de rechter om te beslissen. Het is een moeilijke vraag. In hoeverre mag de privacy worden geschonden van mensen die nog geen verdachte zijn? In hoeverre mag de overheid een hoop data doorzoeken ter voorkoming van georganiseerde criminaliteit?

Wat opvallend is en in meerdere interviews aan bod kwam is dat bij cryptotelefoons/PGP-zaken de advocatuur zich heeft georganiseerd en dat gebeurt niet vaak volgens een rechter. Een andere rechter geeft ook aan dat een deel van de Nederlandse advocaten samen hebben gewerkt aan het rechtmatigheidsvraagstuk in PGP-zaken.[47] Door de verdediging wordt bijvoorbeeld de schending van art. 8 van het EVRM naar voren gebracht. In hun zienswijze staat het recht op privacy van alle burgers onder druk. *"We hebben gezegd dat de machtigingen van de rc voor die schending een afdoende wettelijke basis is, dus dat er geen sprake is van een schending van art. 8 EVRM. De grondrechten zijn objectief bezien wel geschonden; er is immers sprake van kennis nemen van vertrouwelijke communicatie, maar door de rechterlijke machtiging is het onderzoek wel rechtmatig. Er hing veel van af in heel veel strafzaken."* Een strafrechter zegt hierover: *"Bij Ennetcom zag je dit minder, maar misschien is het daar wel begonnen."*

Het bewijs an sich lijkt heel weinig verweer op te leveren. Inhoudelijk zijn er veel gesprekken over interpretatie, maar dit levert weinig verzoeken op om getuigen te horen. Het kan dat in de toekomst alsnog allerlei getuigen worden opgegeven. Het is evident dat wanneer bewijs onrechtmatig is verkregen dat consequenties heeft. Dat kan gaan van niet ontvankelijkheidverklaring van het OM, bewijsuitsluiting, strafvermindering of geen vervolging. Als een telefoon ontsloten is in de tijd dat de regels nog niet duidelijk waren en dat het gebeurde zonder toestemming van rc dan heeft het geen consequenties (het bewijs mag gebruikt worden). Want als het nu was aangevraagd bij de rc, dan had deze zeker toestemming gegeven. Er wordt wel op gelet dat de verdachte niet in zijn belangen is geschaad.

[47] Op de dag van het laatste interview met de RM werd een brandbrief gestuurd vanuit de strafrechtadvocatuur. Deze brief is hier te vinden: https://vanboomadvocaten.nu/brandbrief-strafrechtadvocatuur/

5. Conclusie, discussie en beperkingen

In dit hoofdstuk staan we ten eerste stil bij de conclusies en bediscussiëren we de belangrijkste resultaten (par. 5.1). Ten tweede bespreken we de beperkingen van het onderzoek (par. 5.2). Tot slot beschouwen we het onderzoek als geheel (par. 5.3).

5.1 Conclusies en discussie

In deze paragraaf beantwoorden we de onderzoeksvragen. De deelvragen worden beantwoord in secties 5.1.1-5.1.3. De beantwoording van de hoofdvraag staat centraal in sectie 5.1.4. Hoewel we geen onderzoeksvraag hebben opgesteld die gaat over de omvang-vraag, en dus geen onderwerp was van onderzoek, hebben we daar niettemin wel informatie over gevonden. Deze informatie behandelen we kort in sectie 5.1.1.

5.1.1 Wat is de aard van encryptie in opsporingsonderzoeken?

Encryptie kan op verschillende wijzen naar aard worden ingedeeld. Een eerste indeling is technologie-gedreven versus mens-gedreven. Dit is een soort poging tot 'classificatie' (vgl. Yar, 2006). Encryptie die standaard op apparaten aanwezig is noemen sommige politiemensen technologie-gedreven encryptie en bewust toegepaste encryptie noemen zij mens-gedreven encryptie. In deze tweedeling kan technologie-gedreven encryptie worden vertaald naar 'algemeen gebruik'. Verschillende geïnterviewden beschouwen mens-gedreven encryptie als indicator voor criminaliteit wanneer zij dit tegenkomen in hun werk. Dat dit in de interviews naar voren komt wil niet zeggen dat wij een verbinding willen leggen tussen encryptiegebruik en criminaliteit. Immers, het is op zich niet verboden om gebruik te maken van cryptotelefoons en derhalve moeten daar ook niet allerlei negatieve conclusies aan worden verbonden. Bovendien gaat het om een classificatie en niet om een definitie.

Een tweede indeling is aan de hand van de encrypte gegevens: opgeslagen of stromende gegevens. De classificatie kwamen niet alleen terug tijdens de interviews, maar is algemeen geaccepteerd in de literatuur. In het geval van opgeslagen gegevens gaat het bijvoorbeeld om afbeeldingen van seksueel kindermisbruik. Bij stromende informatie bijvoorbeeld om een lopende conversatie tussen criminelen.

Een derde indeling classificeert verschillende vormen van encryptie aan de hand van het apparaat of toepassing dat encrypt is. Dat encryptie gemeengoed is geworden in de opsporing is voor een belangrijk deel te wijten aan mobiele telefoons die in beslag worden genomen en waar vrijwel altijd een vorm van encryptie op zit, met een sleutel in de vorm van een wachtwoord, een patroon, een vingerafdruk, et cetera. Andere vormen van encryptie, naast versleutelde mobiele telefoons, waarmee de opsporing geconfronteerd wordt, zijn op volgorde van meest voorkomend: versleutelde chatdiensten, versleutelde devices anders dan mobiele telefoons (zoals laptops en desktop computers), versleutelde e-maildiensten en cryptotelefoons.

Een opmerking die we hier willen maken is dat niet iedereen die we hebben gesproken hetzelfde beeld heeft van encryptie. Sommigen betrekken encryptie vooral op cryptotelefoons. Anderen zien encryptie als het bewust ontoegankelijk maken van informatie. En weer anderen zien encryptie als iets dat überhaupt afschermend werkt, zoals authenticatie op een mobiele telefoon. Het is belangrijk om in de discussie die wordt gevoerd, duidelijk te maken wat precies onder encryptie wordt geschaard en wat niet.

Vervolgens kijken we naar het verband tussen vorm van encryptie en soort criminaliteit. Op het niveau van delictscategorieën komt encryptie volgens de geïnterviewden het meest voor bij ondermijning en in vrij grote mate bij high impact crimes (HIC). Encryptie is weliswaar aanwezig bij veel voorkomende criminaliteit, maar in mindere mate. Wanneer we in ogenschouw nemen dat mobiele telefoons in verschillende delicten – waaronder VVC – een rol spelen, dan is het opmerkelijk dat encryptie voor deze delictscategorie minder vaak voorkomt. Een alternatieve verklaring kan zijn dat encryptie minder als een probleem wordt ervaren, omdat verdachten bijvoorbeeld vaker meewerken. Met andere woorden, het is overal aanwezig, maar de rol is hier kleiner. Vervolgonderzoek zal moeten uitwijzen hoe dit precies zit.

Als we nader inzoomen op type criminaliteit, dan zien we encryptie het vaakst voorkomen bij drugsmisdrijven, kinderporno en cybercrime (in ruime en enge zin). Hoewel niet expliciet een vorm van criminaliteit, komt encryptie in zeer grote mate voor in de georganiseerde misdaad. Ondermijning en georganiseerde criminaliteit hangen nauw met elkaar samen, waarbij ondermijning vooral verwijst naar de effecten van georganiseerde criminaliteit.[48]

Op basis van correlaties zien we dat 'cryptotelefoons' en 'versleutelde berichtendiensten' vaker gezien worden bij drugsmisdrijven, georganiseerde criminaliteit en wapendelicten en juist minder bij seksuele misdrijven/zeden en kinderporno (en versleutelde berichtendiensten bij vandalisme). Cryptocontainers zijn in opsporingsonderzoeken naar vermogensdelicten, cybercrime en milieucriminaliteit vaker aan de orde. Versleutelde gegevensdragers komen vaker voor in kinderpornozaken. Verder komen versleutelde chatdiensten, gelockte mobiele telefoons, gelockte devices anders dan mobiele telefoons, bulletproof hosting en Tor niet vaker of minder vaak bij een bepaald type delict voor.

Over de omvang van encryptie kunnen we op basis van het onderzoek, zoals eerder aangegeven, geen concrete uitspraken doen. Dit was geen expliciet doel van het onderzoek en laat zich daarnaast lastig vaststellen. Naast dat geïnterviewden aangeven dat het overal een rol speelt, geven ze ook aan in hun werk dagelijks met encryptie te maken te hebben. De omvang hangt volgens geïnterviewden sterk af van type misdrijf, type toepassing en type verdachte. Hoewel de omvang niet exact is vast te stellen is de perceptie van de meeste geïnterviewden en respondenten dat de omvang van encryptie in de opsporing in de afgelopen vijf jaar is toegenomen. In de literatuur wordt ook gesteld dat de omvang-vraag zich lastig laat beantwoorden. In sommige rapportages worden dergelijke uitspraken wel gedaan. In het EMCDDA & Europol-rapport (2017) wordt bijvoorbeeld genoemd dat in meer dan drie kwart van de cybercrime-onderzoeken in de EU in 2017 een vorm van encryptie voorkwam om data te beschermen. Daarbij wordt overigens niet vermeld om hoeveel onderzoeken het gaat en wat precies onder cybercrime wordt verstaan. Overigens is niet alleen van belang wat de frequentie is dat iets voorkomt, maar ook juist hoe vaak iets een probleem is. Dit zijn twee verschillende dingen. In sectie 5.1.2 gaan we dieper in op het tweede.

Het laatste onderdeel van deze onderzoeksvraag gaat over de recentste ontwikkelingen. Over hoe de aard van encryptie is veranderd in de afgelopen vijf jaar, wordt aangegeven dat de encryptie zelf niet per se beter is geworden, maar dat vooral de sleutel beter wordt verstopt. Een andere trend is dat encryptie steeds meer geïntegreerd is in hard- en software, en installatieprocessen. Daarmee wordt encryptie steeds meer (standaard) toegepast en gebruikt. Biometrie en 5G worden genoemd als

[48] NCTV (z.d.). *Stevige programmatische aanpak criminele ondermijning.* Verkregen via: https://www.nctv.nl/onderwerpen/nationale-veiligheid-strategie/versterkte-aanpak-van-risicos-en-dreigingen/criminele-ondermijning

belangrijke veranderingen van de afgelopen tijd. 5G verschilt van de vorige generaties mobiele netwerken met betrekking tot bepaalde kwaliteiten, met name het potentiële vermogen van snelle gegevensoverdracht en gelijktijdig gebruik van meerdere gegevensbronnen. Maar het bevat ook een nieuw encryptieniveau, wat directe gevolgen kan hebben voor strafrechtelijke onderzoeken, bijvoorbeeld voor het vaststellen van locaties. Ook maakt de komst van 5G het voor de opsporing lastiger om devices van gebruikers af te tappen (Europol, 2019). Niet alleen is gekeken naar de afgelopen jaren, ook blikken enkele respondenten alvast vooruit. Dit bespreken we in sectie 5.1.4.

Tot slot wordt door geïnterviewden en respondenten aangegeven dat criminelen anders zijn gaan communiceren. De reden daarvoor ligt met name aan de recent behaalde successen met enkele grote encryptiezaken. Criminelen zijn zich daardoor bewuster geworden van de gevaren die alsnog kunnen schuilen in het gebruik van encryptie. Dit kan betekenen dat deze successen lastig te evenaren zijn. Echter, voor verschillende criminaliteitsvormen blijft communicatie een essentieel onderdeel van de uitvoering, dus dat blijft kansen bieden. Zo heeft de politie begin 2023 42 verdachten uit verschillende landen opgepakt nadat zij vijf maanden konden meelezen met versleutelde communicatie via Exclu Messenger.[49] De verdachten worden onder andere verdacht van drugshandel, witwassen en verboden wapenbezit.

5.1.2 Encryptie en het verloop van opsporingsonderzoeken

In dit onderzoek wordt met 'verloop' gedoeld op de slagingskans om binnen opsporingsonderzoeken één van de volgende routes te bewandelen: encryptie omzeilen, encryptie technisch kraken of alternatieve opsporingsmiddelen inzetten. De rol van encryptie in het verloop van een opsporingsonderzoek omvat ook wat een bepaalde route betekent in termen van de inzet van mensen en middelen, zoals doorlooptijd, menskracht, expertise en de aanschaf van soft- en hardware, en wat een bepaalde route betekent in termen van extra opbrengsten. Hierna komen achtereenvolgens aan bod: (i) het omzeilen van encryptie, (ii) het kraken van encryptie en (iii) het inzetten van alternatieve opsporingsmiddelen. Tot slot gaan we ook in op (iv) de (extra) inspanningen die hiermee gepaard gaan.

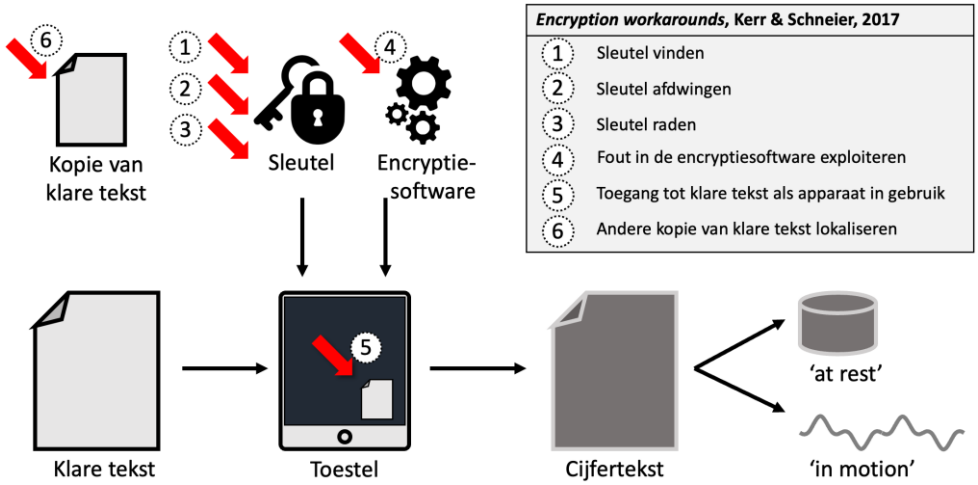
(i) Eerste route: het omzeilen van encryptie. In het geval van omzeilen kan de opsporing dit doen via het vinden van de sleutel, het raden van de sleutel, het afdwingen van de sleutel, het exploiteren van een lek in de encryptiesoftware, het verkrijgen van toegang tot leesbare tekst (klare tekst) als het apparaat wordt gebruikt en het lokaliseren van een kopie van de leesbare tekst (zie figuur 5.1 op de volgende pagina voor een grafisch overzicht).

De eerste tactiek is de sleutel vinden. Dit kan alleen als deze ergens beschikbaar is (bijv. fysiek op een post-it of digitaal op de computer). Daarnaast moet de sleutel vindbaar en leesbaar zijn. Als laatste moeten de opsporingsinstanties op rechtmatige wijze toegang krijgen tot de sleutel.

De tweede tactiek is om de sleutel af te dwingen van iemand die de sleutel heeft of kent. In de ideale situatie biedt de verdachte de sleutel aan. Een belangrijke voorwaarde is om binnen het juridisch geldende kader te blijven om de sleutel op rechtmatige wijze te verkrijgen. In 2020 zijn er in totaal vijf Europese landen met een wettelijke bepaling om een verdachte te dwingen om de politie te assisteren in de toegang van de data of de sleutel te geven. Deze landen zijn België, Kroatië, Frankrijk, Ierland en het Verenigd Koninkrijk. Met ingang van de Innovatiewet mag een verdachte ook in Nederland tot op zekere hoogte worden gedwongen om de sleutel af te geven. Het afdwingen van een sleutel lijkt op

[49] NOS (2023). *Politie leest vijf maanden mee met versleutelde berichten, 42 arrestaties.* Verkregen via: https://nos.nl/artikel/2462344-politie-leest-vijf-maanden-mee-met-versleutelde-berichten-42-arrestaties

het eerste oog misschien in strijd met het nemo tenetur-beginsel; dat niemand mag worden gedwongen om aan zijn eigen veroordeling mee te werken (Europol & Eurojust Public Information, 2020b). Volgens geïnterviewden is daar echter geen sprake van. Daarbij wordt verwezen naar een uitspraak van de Hoge Raad (ECLI:NL:PHR:2020:927) alsook het feit dat deze wetgeving (pilot Innovatiewet) er nu ligt. Bovendien kent het wetboek van Strafvordering al langere tijd de bepaling dat in omstandigheden materiaal moet worden afgestaan (bijv. DNA), daar is dit er een van.



Figuur 5.1: Wijzen om encryptie te omzeilen (gebaseerd op Kerr & Schneier, 2017)

De derde tactiek is het raden van de sleutel. Dit is een realistischere optie dan het vinden van een sleutel, maar is ook uitdagender daar het veel capaciteit en tijd vraagt. De opsporing kan bij het raden van wachtwoorden onder andere gebruik maken van informatie van de verdachte. Naast persoonlijke of sociale informatie dat vaak onderdeel is van een wachtwoord, kennen de meeste wachtwoorden ook een specifieke volgorde.

De vierde tactiek is het exploiteren van fouten in de encryptiesoftware. Hierover hebben we voor wat betreft *omzeilen* van encryptie geen nadere informatie opgehaald. Wel wordt hier iets over gezegd in relatie tot het *kraken* van encryptie. Dit komt dus verderop aan bod.

De vijfde tactiek is om toegang te krijgen tot leesbare tekst als het apparaat wordt gebruikt. Hiervoor kan zowel op afstand toegang worden verkregen (bijv. via een keylogger) als fysiek (bijv. aanhouding met open device). De opsporing kan in theorie gebruik maken van het decryptiebevel (art. 126nh lid 1) en de hackbevoegdheid (art. 126nba). We zien dat hier weinig gebruik van wordt gemaakt. Dit is te verklaren doordat deze bevoegdheden niet zomaar mogen worden ingezet. Inmiddels is een eerste evaluatie afgerond naar de hackbevoegdheid (Van Uden & Van den Eeden, 2022). Zij beschrijven dat in de periode maart 2019-2021 in 26 opsporingsonderzoeken bevelen zijn afgegeven hiervoor. Zij geven daarbij aan dat deze bevoegdheid vooral is ingezet bij de zwaardere vormen van traditionele criminaliteit, zoals (poging tot) moord, drugscriminaliteit, zeden en terrorisme, en slechts eenmaal bij cybercrime (in enge zin).

De zesde techniek is het lokaliseren van een kopie van de leesbare tekst. Deze tactiek omzeilt encryptie volledig. Opsporingsinstanties kunnen sleutels en/of informatie opvragen bij derde partijen. De meeste EU-lidstaten hebben een specifieke of algemene wettelijke bepaling waarin deze derde partijen kunnen worden verplicht om een sleutel of informatie over te dragen (Europol & Eurojust Public Information, 2019). Bij rechtshulpverzoeken is het onder andere afhankelijk van wet- en

regelgeving of opgevraagde data (tijdig) geleverd worden, maar ook of ze bruikbaar zijn voor het opsporingsonderzoek. In dit kader wordt soms helemaal geen informatie opgevraagd omdat opsporingsinstanties verwachten dat de informatie niet bruikbaar is of te laat zal komen.

(ii) Tweede route: het technisch kraken van encryptie. In het geval van kraken gebruikt men binnen de opsporing een zogenoemde brute force aanval. Vaak als laatste redmiddel wordt getracht om encryptie op technische wijze te ontsleutelen. Dit kost de meeste tijd en capaciteit en is onzeker in uitkomst. Hoewel achter encryptie komen altijd tijd vergt is voor het kraken naast capaciteit ook adequate soft- en hardware nodig (zie ook Council of the European Union, 2017; Ilbiz & Kaunert, 2022).

In de praktijk zien we dat het technisch kraken van encryptie veelal wordt uitbesteed aan een andere afdeling of partij, zoals het NFI. In het geval van een internationale samenwerking kan ook Europol mogelijk worden verzocht tot het kraken van encryptie. Zo beschikt Europol over een decryptie platform. Hoewel we geen medewerkers van Europol hebben gesproken, lezen we in documentatie terug dat de vraag van EU-lidstaten naar forensische ondersteuning van Europol 'aanzienlijk' is toegenomen, zowel qua volume als qua complexiteit (Europol, 2020b). Wel lijkt het erop dat het percentage zaken waarbij een beroep op Europol kan worden gedaan beperkt is, omdat het platform zich primair lijkt te focussen op terrorisme, HIC en georganiseerde criminaliteit, waaronder online seksueel kindermisbruik (Europol, 2020a). Ook is niet geheel duidelijk in hoeverre de EC3 in staat is om te reageren op alle verzoeken vanuit de lidstaten (Ilbiz & Krauner, 2022).

De belangrijkste technische aspecten aangaande encryptie zijn het toegepast cryptografische algoritme en de sleutellengte. Daarbij geldt in algemene zin; hoe langer de sleutel hoe lastiger te kraken. Naast de interne factoren die te maken hebben met encryptie – de encryptiemechanismen en sleutellengten – zijn externe factoren belangrijk in het kraken van een systeem.

In een van de interviews kwam het gebruik van zero-days naar voren; bij het gebruik van applicaties van derden voor ontsleuteling. Deze zero-days zijn bekend bij de aanbieders van de betreffende applicaties, maar niet bij de politie. Er is verder weinig bekend over of en hoe overheden deze tactiek gebruiken (Europol & Eurojust Public Information, 2019). Het lijkt erop dat de meeste leden van de EU geen duidelijk juridisch kader hebben betreffende het omgaan met kwetsbaarheden in software. Wel wordt in 2015 door het Europees Agentschap voor Netwerk- en Informatiebeveiliging (ENISA) benadrukt dat overheden transparant en open moeten zijn over het gebruik van softwarekwetsbaarheden. ENISA kan ook een rol spelen in het adviseren en assisteren van lidstaten in het ontwikkelen en implementeren van een Government Disclosure Decision Process (GDDP).

Voor de Nederlandse situatie wordt wel iets over zero-days gezegd. "Indien politie of justitie – al dan niet binnen het bestek van de uitoefening van de bevoegdheid ex artikel 126nba Sv – op de hoogte komt van een (tot dan toe onbekende) kwetsbaarheid of lek in de beveiliging van hardware of software, wordt dit gemeld bij de producent van die hardware of software met het oog op het beëindigen of dichten daarvan" (Aben & Luining, 2022, p.46). De procedure van art. 126ffa Sv stelt de OvJ in staat om – met een vereiste machtiging van de rc – de bekendmaking van een onbekende kwetsbaarheid tijdelijk uit te stellen op grond van een 'zwaarwegend opsporingsbelang'.

(iii) Derde route: alternatieven. Als het niet lukt om encryptie te omzeilen of te kraken zijn er volgens diverse geïnterviewden en respondenten vaak voldoende alternatieven aanwezig om in te zetten om toch bewijs te vergaren dat nodig is in een zaak. Er kan namelijk ook (ander) bewijs worden vergaard op andere manieren, waardoor het toch kan lukken om iemand te veroordelen. Niet alleen bewijs zelf is gewichtig, maar ook de identiteit van een verdachte, diens verblijfplaats en de locatie van

een misdrijf. In dat kader wordt door verschillende deelnemers een belangrijke link gelegd met metadata. Metadata kunnen daarin namelijk een belangwekkende rol spelen. Geïnterviewden voorzien echter dat de waarde van metadata (in ieder geval voor mobiele telefonie) mogelijk onder druk komt te staan door technologische ontwikkelingen, zoals 5G. Dit kan zijn weerslag hebben op de mate waarin het lukt om relevante personen te lokaliseren.

(iv) Inspanningen. Op de vraag of, en zo ja hoe, encryptie een rol in de voortzetting en/of doorlooptijd van opsporingsonderzoeken speelt is geen eenduidig antwoord mogelijk. Om een opsporingsonderzoek waarin encryptie een rol speelt voort te zetten, wordt voornamelijk gekeken naar het criterium prioriteit van de zaak/misdrijf. Er is prioriteit als het opsporingsonderzoek in het belang is van de Nederlandse samenleving. Het tweede criterium dat door respondenten veelal wordt benoemd is de kans van slagen om toegang te krijgen tot data achter encryptie. Wat de geschatte kans van slagen is om achter encryptie te komen loopt erg uiteen. Er is geen duidelijk peil op te trekken, en derhalve niet te kwantificeren. Antwoorden variëren van een paar procent tot aannemelijk. Het is contextafhankelijk waardoor een uitspraak hierover niet te doen is. Daarbij moet ook worden gezegd dat op voorhand niet altijd duidelijk is welke informatie zich achter encryptie begeeft. Op het moment dat de encryptie omzeild of gekraakt is, en er geen bruikbare informatie aanwezig is dat als bewijs kan dienen of aanknopingspunten biedt, in hoeverre is het dan succesvol? Of als slechts een deel van de data worden ontsleuteld?

Qua doorlooptijd zien we dat encryptie in principe altijd vertragend werkt. Het kost immers een handeling (of meerdere) om achter de versleutelde informatie te komen. Het beeld ontstaat dat wanneer criminelen geprofessionaliseerd en/of technisch vaardig zijn, zij eerder geneigd zijn om hoogwaardige encryptie te gebruiken. Encryptie die bewust is toegepast door criminelen lijkt op basis van de data een aanzienlijke vertraging op te leveren. Dit ten opzichte van standaard toegepaste encryptie op bijvoorbeeld mobiele telefoons. Wat uit onze data niet duidelijk wordt is hoeveel vertraging precies wordt opgedaan. Een respondent geeft aan dat het weken, maanden of jaren kan duren. Het is erg contextafhankelijk. Ook de gekozen strategie speelt een rol. Denk bijvoorbeeld aan de tijd die in het voorbereiden van een aanhouding met open device gaat zitten, of aan de doorlooptijd van rechtshulpverzoeken die minimaal een halfjaar duren en waarvan de uitkomst onzeker is. Rechtshulpverzoeken – of de internationale component in bredere zin – worden gezien als een belangrijke belemmering. Dat dergelijke verzoeken langdurige processen betreffen weten we ook uit eerder onderzoek (o.a., Veenstra e.a., 2016; Zuurveen & Stol, 2020). Wellicht kunnen daar op internationaal niveau betere afspraken over worden gemaakt.

De andere kant van de medaille is dat zodra de encryptie doorbroken of omzeild is, de doorlooptijd van opsporingsonderzoeken juist sneller kan gaan. Een respondent illustreert dat na decryptie een zaak in een aantal weken rond kan zijn waar vroeger maanden tot een jaar over werd gedaan. Daarnaast wordt aangemerkt dat encryptie niet altijd een rol speelt, omdat verdachten deze ook in gevallen zelf ontgrendelen. Tot slot speelt het lerend vermogen van de politieorganisatie een belangrijke rol alsook die van gelieerde partijen als het NFI, het OM en de RM. Met het ontwikkelen van kennis en opdoen van ervaring kan het kraken en omzeilen – of het inzetten van alternatieven – positief bijdragen aan de doorlooptijd van zaken waarin encryptie aanwezig is (zie ook par. 5.4).

Daarnaast speelt nog wat anders. Veel van de issues die betrekking hebben op het verloop van opsporingsonderzoeken zijn niet uniek voor encryptie. Het is belangrijk om hierover na te blijven denken. Denk bijvoorbeeld aan de capaciteits- en expertisevraagstukken en belemmeringen op

internationaal vlak. Dergelijke issues spelen op verschillende terreinen binnen de gehele politieorganisatie een rol. Maar ook het moeten stopzetten van een onderzoek omdat op encryptie wordt gestuit waar niet omheen gewerkt kan worden is niet uniek. Een zaak kan ook stranden omdat bijvoorbeeld geen getuigen worden gevonden. Kortom, zodra dergelijke problemen direct worden geprojecteerd op het fenomeen encryptie, kan dat ervoor zorgen dat men denkt dat deze problematiek nieuw is. Met andere woorden, een dergelijke focus op encryptie kan ertoe leiden dat het beeld ontstaat dat de politie nu met een probleem te maken heeft dat ze nooit eerder bij de hand had, en dat is dus niet het geval. Het lijkt erop dat in veel gevallen alleen het type drempel anders is.

We hebben in deze paragraaf besproken: drie routes die de politie hanteert in het oplossen van encryptie als hindernis, en welke nadelen (investering) en voordelen elke route voor de opsporing heeft. Alles overziend, lijkt ons dat het kunnen kraken van encryptie niet de eerste investering is waar de politie breed op zou moeten inzetten. De kunst van het oplossen van delicten is vooral gebaat bij het ontwikkelen van het vermogen om encryptie te omzeilen of het inzetten van alternatieve opsporingsmiddelen. Het vermogen om technisch te kraken zou met name voor cruciale zaken centraal belegd kunnen worden bij het NFI, en bij specifieke zaken bijvoorbeeld bij Europol. De politie is voor de bulk van haar werk vooral gebaat bij de andere twee routes, die niet uitgaan van technologisch geweld maar die uitgaan van slim politiewerk. De vraag waarop de politie moet inzetten – en wat haalbaar is – is belangrijk om te beantwoorden voor (toekomstig) beleid.

5.1.3 Encryptie en de opbrengst van opsporingsonderzoeken

In principe speelt encryptie een belemmerende rol aangaande het identificeren en/of lokaliseren van relevante personen en goederen, van samenwerkingsverbanden of (strafrechtelijk relevante) relaties tussen personen, goederen en locaties, en de mogelijkheid om criminele activiteiten vast te stellen (signaleren). De belemmering ligt vooral in de vermindering van directe toegang tot bewijs. Tevens verschillen ontsleutelde en opgevraagde data in bruikbaarheid voor het opsporingsonderzoek. Daarnaast komen opgevraagde data regelmatig te laat, niet of zijn niet bruikbaar.

Hoewel niet duidelijk is te zeggen wat voor data – en daarmee ook bewijs – worden gemist, en dat er dus gevallen kunnen zijn waarin verdachten onterecht vrijuit gaan, krijgen we in meerdere interviews terug dat niet achter encryptie komen niet het einde van de wereld is. In gevallen waarin het niet lukt, bijvoorbeeld in zaken waarin encryptie bewust is toegepast, zijn er vaak voldoende alternatieven aanwezig om in te zetten om toch bewijs te vergaren dat nodig is in een zaak. En hoewel door encryptie het misschien lastiger en uitdagender is geworden, lukt het bovendien vaak ook wel om achter encryptie te komen. Zo wordt door meerdere geïnterviewden en respondenten aangegeven dat er een relatief grote slagingskans is om informatie te ontsleutelen van werken waarbij de encryptie standaard is ingebouwd. We kunnen dit echter niet staven met cijfers.

Bovenstaande bevinding komt overeen met het onderzoek van Hartel en Van Wegberg (2021). Zij hebben in kaart gebracht in hoeverre end-to-end encryptie een rol speelt bij het aandragen en de uitkomst van strafzaken. Ze vergeleken zaken waarin encryptie voorkomt met zaken waarin geen encryptie voorkomt. Ze concluderen op basis van een analyse van jurisprudentie dat Nederlandse opsporingsinstanties daders die encrypte communicatie gebruikten net zo succesvol strafrechtelijk kunnen vervolgen als daders die geen gebruik maakten van encrypte communicatie.

In de oriënterende fase was een wisselend beeld of ontsleutelde data essentieel zijn voor een zaak of slechts bijvangst waarbij meer informatie nodig is. Wel geeft men aan dat het beeld over

criminele samenwerkingsverbanden volledediger is geworden (na decryptie) in plaats van globaal en fragmentarisch in de situatie voor encryptie. In de verdiepende fase wordt dit beeld bijgesteld naar dat het veelal essentiële informatie betreft, en wordt de waarde van deze data benadrukt. Het wordt over het algemeen gezien als zuiverder dan bijvoorbeeld (getuige)verklaringen. Mogelijk is dit voor een groot deel te wijten aan data die vanaf mobiele telefoons komen. Doordat tegenwoordig dusdanig veel (persoonlijke) informatie op mobiele telefoons staan, vinden mensen het minder prettig deze aan anderen uit te lenen, en is het gebruik van deze devices – en de digitale sporen die daaruit komen – daarmee ook beter te koppelen aan één specifiek persoon. Dit betekent dan ook dat normaal gesproken slechts één iemand de sleutel heeft. Daardoor is de kans kleiner dat deze informatie is aangepast door derden. Ook het vrijer communiceren van verdachten – die zich veilig wanen achter encryptie – draagt daar aan bij.

Wel willen we nuanceren dat bovenstaande niet altijd opgaat voor digitale sporen in zijn algemeenheid. Sommige digitale sporen zijn wel degelijk eenvoudig te manipuleren. Denk bijvoorbeeld aan tijdsaanduidingen, loggegevens, foto's, video's alsook verstuurde berichten. Dit betekent dat politiemensen niet zonder meer ervan uit kunnen gaan dat digitale sporen waarheidsgetrouw zijn (Zuurveen & Stol, 2020). Bewustwording hiervan is belangrijk.

Advocaten lijken in strafzaken te proberen om te bewijzen dat het bewijs op niet legitieme wijze is verzameld door opsporingsinstanties. Eind 2022 is daar een brandbrief over gestuurd. In de verdiepende interviews met het OM en de RM wordt daarnaar gerefereerd. Hoewel men vanuit die perspectieven niet per se meegaan in de argumentatie, vinden de geïnterviewden het waardevol dat discussie blijft bestaan over de wijze waarop data verkregen zijn en of dat past binnen de geldende wettelijke voorschriften en beginselen van proportionaliteit en subsidiariteit. Ten tijde van de oplevering van het conceptrapport heeft de Rechtbank Noord-Nederland prejudiciële vragen gesteld aan de Hoge Raad aangaande onder andere de toepassing van het interstatelijke vertrouwensbeginsel, waarbij EncroChat en Sky ECC worden besproken (zie ook sectie 3.3.2).[50] Ten tijde van het opleveren van dit rapport zijn op deze vragen nog geen antwoorden geformuleerd.

5.1.4 Wat is de rol van encryptie in opsporingsonderzoeken?

Dit onderzoek toont dat de aanwezigheid van encryptie in opsporingsonderzoeken een prominente rol inneemt. Deze rol heeft een tweeledig karakter. Encryptie speelt zowel een belemmerende rol in de opsporing alsook een praktische rol die ten gunste komt aan de opsporingspraktijk.

Enerzijds kan encryptie dus belemmerend werken op de opsporing, bijvoorbeeld doordat extra handelingen uitgevoerd moeten worden om toegang te krijgen tot informatie c.q. bewijslast. Deze extra handelingen kunnen belemmerend werken, omdat ze bijvoorbeeld veel capaciteit vergen, en daarmee de doorlooptijd van een zaak kunnen vertragen. Een aanzienlijk deel van de politiemensen die wij spraken of die de vragenlijst invulden benoemden dan ook dat encryptie daarmee in negatieve zin een rol speelt in de opsporing.

Daarnaast zagen we ook, voornamelijk op het moment dat achter de encryptie wordt gekomen (de fase van decryptie), dat er een schat aan data ligt waarmee de opsporing haar voordeel kan doen. EncroChat en SKY ECC zijn daar sprekende voorbeelden van. Door de ervaren schijnveiligheid van criminelen worden netwerken blootgesteld en wordt communicatie inzichtelijk, waardoor de

[50] https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:RBNNE:2022:4797

bewijslast voor het oprapen ligt. Er zijn voorbeelden waarbij er zoveel data beschikbaar zijn, dat wederom een gebrek aan capaciteit ervoor kan zorgen dat niet alles opgepakt kan worden, maar over het algemeen benoemen de geïnterviewden en de respondenten dit als een positieve rol die encryptie – of eigenlijk decryptie – speelt in de opsporing. Deze bevinding zien we ook terug in de literatuur, waarbij wordt gesteld dat versleuteld digitaal bewijs voor Europese rechtshandhaving instanties leidt tot uitdagingen op het vlak van (i) een gebrek aan voldoende technische capaciteit, (ii) een gebrek aan voldoende financiële middelen en (iii) een gebrek aan voldoende personele capaciteit in de vorm van aantallen en opleiding van personeel (Pisariç, 2021). Om het capaciteitsprobleem voor een deel aan te pakken lijkt een belangrijke rol weggelegd voor de 'tactiek'.

Wij zijn van mening dat we bij het bestuderen van encryptie niet alleen naar de versleuteling moeten kijken, maar dat een holistisch beeld nodig is om tot de kern van het 'probleem' van encryptie te komen, en dat is door ook bewust decryptie in het verhaal mee te nemen. Dat de rol van encryptie in de opsporing daarmee genuanceerder ligt, zagen we ook terug in de respons die we kregen via de verschillende onderzoeksmethoden. Enerzijds gaat dit over het accepteren dat er gedeald moet worden met nieuwe fenomenen en dat daarop geacteerd moet worden. Het zogenoemde kat-en-muisspel dat optreedt tussen politie en criminelen kan dus ook worden gezien als kans voor de politieorganisatie om zich verder te ontwikkelen. Dit laatste is in de steeds verder digitaliserende samenleving zeer van belang (Henseler, 2010; 2017).

Hoewel vraagstukken over encryptie in relatie tot de opsporing niet nieuw zijn (bijv. Henseler, 2010), zijn deze onverminderd actueel en meer aan de oppervlakte komen drijven door de technologische ontwikkelingen van de afgelopen jaren. Hoewel we nu de status quo beschrijven, moeten we ook rekening houden met wat er op ons af gaat komen. Wat betekent bijvoorbeeld een 'nieuwe' digitale ontwikkeling zoals kwantumcomputing in dit verband? Een belangrijke fundamentele vraag voor vervolgonderzoek, maar ook voor de opsporingspraktijk. Door kwantumcomputing zullen de huidige vormen van encryptie waarschijnlijk in onbruik raken (Europol & Eurojust Public Information, 2020b). Echter, met dezelfde technologie kunnen ook weer nieuwe oplossingen worden gevonden. Desalniettemin kan het de politie in de toekomst voor nieuwe uitdagingen stellen en is het dus van belang om hier rekening mee te houden.

Ook op andere zaken die verband houden met de wijze waarop toegang verkregen wordt tot voor de opsporing relevante data – die voor potentiële (en nieuwe) digitale uitdagingen kunnen zorgen, zoals AI (artificiële intelligentie), IoT, robotica en metaverse – moet worden geanticipeerd. Net als bij kwantumcomputing lijkt misbruik van AI door criminelen momenteel beperkt, omdat de technologie nog in ontwikkeling is. Wel kan de toepassing van AI het nog lastiger maken om online vast te kunnen stellen wat echt is en wat nep, en wie wie is; echtheidscomplexiteit (Stol & Jansen, te verwachten; Jansen e.a., 2019). Een concreet voorbeeld waar op moment van schrijven veel discussie over is, is de AI-gebaseerde applicatie ChatGPT, een geavanceerde chatbot, maar ook deepfakes gaan een groter risico vormen.[51,52,53] Volgens Europol (2019) is het van belang dat in de opsporing wordt geïnvesteerd in het begrijpen van AI-technologie en de implicaties daarvan.

[51] Zie: https://openai.com/blog/chatgpt/

[52] Borst, M. de (2023). *De impact van ChatGPT op cybercrime*. Verkregen via: https://numbers.amsterdam/nieuws/de-impact-van-chatgpt-op-cybercrime/

[53] Meijer, E. (2022). *Deepfakes, ransomware en cybercrime-as-a-service grote risico's voor 2023*. Verkregen via: https://www.agconnect.nl/artikel/deepfakes-ransomware-en-cybercrime-service-grote-risicos-voor-2023

Niet alleen is het anticiperen op de toekomstige ontwikkelingen belangrijk, ook moet worden geïnvesteerd in het opdoen van kennis en ervaring omtrent encryptie in relatie tot digitale sporen die nu actueel zijn. Dit geldt zowel voor politiemensen als medewerkers van het OM en de RM. Volgens geïnterviewden draagt dat positief bij aan de doorlooptijd van zaken waarin encryptie aanwezig is. In het werk van Jansen e.a. (2020) en Zuurveen en Stol (2020) wordt gesteld dat – los van de beschikbaarheid van adequate tools en technieken – kennis en vaardigheden aangaande digitale aspecten van politiewerk (incl. het vereiste juridische kader) een belangrijke basis zijn in de steeds verder digitaliserende samenleving, en tegelijkertijd dat die niet overal in voldoende mate aanwezig is. Ook weten waar en/of bij wie deze kennis te halen is, is daarin van cruciaal belang. Beide onderzoeken gaan overigens niet expliciet in op encryptie. In vervolgonderzoek kan daar nader op worden ingegaan. In het werk van Fukami e.a. (2021) wordt gesteld dat forensische vaardigheden met betrekking encryptie vandaag de dag essentieel zijn voor de opsporing.

5.2 Beperkingen

Dit onderzoek beperkt zich tot encryptie in de opsporing. Er is niet gekeken naar andere politiestrategieën, zoals verstoring. Deels is dit een definitiekwestie. Opsporing en verstoring lopen in elkaar over en de definitie ervan is discussiewaardig. In dit onderzoek is daarnaast – bewust – voorbijgegaan aan de algemene voordelen die digitalisering en encryptie opleveren vanuit maatschappelijk perspectief. Onderhavig onderzoek is descriptief en niet prescriptief van aard.

Bij een onderzoek als deze kan op voorhand mogelijk de indruk worden gewekt dat vooral de negatieve aspecten worden benadrukt van encryptie ten aanzien van de opsporing. De onderzoekers hebben getracht zoveel mogelijk weg te blijven van mogelijke negatieve associaties, en zijn zich ook terdege bewust van de politiek-gevoelige aard van het onderzoek. Acties die de onderzoekers daarvoor hebben genomen zijn bijvoorbeeld het toepassen van extra zorgvuldigheid bij formuleringen. Daarom spreken we in dit onderzoek over de ‘rol’ van encryptie, in plaats van meer geladen termen als ‘impact’ en ‘effect’ (zie ook par. 1.3). Bovendien is impact lastig meetbaar aan de hand van de gehanteerde methoden. In die zin gaat het onderzoek meer over percepties van deskundigen in de opsporingspraktijk. Daarnaast kijken de onderzoekers zo objectief mogelijk naar de deze praktijk en zijn dan ook niet ingegaan op het proportionaliteitsvraagstuk en bredere debat. Wel bieden de resultaten input voor dit debat.

Een andere beperking ligt in de gevoeligheid van het onderwerp ten aanzien van de opsporingspraktijk. Hoewel we het debat willen informeren, willen we kwaadwillenden niet onnodig wijzer maken. Immers, als criminelen meer weet krijgen van hoe de politie te werk gaat, kunnen zij daar hun voordeel mee doen. Om die reden hebben we strategieën en werkwijzen van de politie en haar partners zodanig beschreven dat de algemene principes ervan in relatie tot de rol van encryptie duidelijk zijn, zonder daarbij in te gaan op onderliggende details.

Een andere mogelijke beperking zien we in de wijdverbreidheid van encryptie. We merkten in de gesprekken die we voerden dat niet iedereen hetzelfde verstaat onder encryptie. Sommigen interpreteren het in brede zin en verstaan daar bijvoorbeeld ook gelockte mobiele telefoons onder, terwijl anderen encryptie vooral zien als het verhullen van informatie; digitale gegevens en communicatie. Dit kan ertoe hebben geleid dat respondenten op verschillende wijze de vragenlijst hebben ingevuld. We hebben de respondenten vooraf een definitie van encryptie gegeven, en in de verdiepende interviews is expliciet gevraagd wat een geïnterviewde onder encryptie verstaat, om

zoveel mogelijk eenduidigheid te creëren, maar dat er verschillende beelden bestaan bij wat encryptie inhoudt, blijft een factor waarmee rekening moet worden gehouden. Hoe dan ook is het van belang om in vervolgonderzoek en in beleidsvorming daar aandacht aan te besteden.

Het is goed mogelijk dat de politie niet alles ziet wanneer we het hebben over encryptie. Het kan dus zijn dat we in dit onderzoek alleen het topje van de ijsberg raken of dat we specifieke (criminele) toepassingen hebben gemist. Tevens hebben we geen onderzoek gedaan naar de omvang, wat als een beperking van het onderzoek gezien kan worden. Dit was echter nog niet goed mogelijk, omdat de stand van beschikbare kennis op dit onderwerp dat niet toe liet. Daarnaast hebben we verkend wat de mogelijkheden waren om data te verzamelen en analyseren van politiesystemen, maar ook dat bleek niet mogelijk (zie par. 2.5). Een optie voor vervolgonderzoek kan zijn om gedurende een bepaalde periode op systematische wijze bij te houden welke verzoeken tot decryptie binnen komen bij de daarvoor aangewezen politieafdelingen en/of het NFI. Dit kan leiden tot een concreter en kwantitatiever beeld, alsook tot meer inzicht in hoe die zaken worden behandeld en afgehandeld. Ondanks deze beperking hebben we rijke data verzameld aan de hand van de methoden die wel zijn ingezet, zoals de interviews en de vragenlijst, waarbij materiedeskundigen hun kennis en expertoordeel hebben gedeeld.

De ingezette methoden kennen overigens wel enkele beperkingen. Ten aanzien van het literatuuronderzoek kan worden opgemerkt dat relatief weinig literatuur beschikbaar was. De aanwezige literatuur ging bovendien veelal in op de technische aspecten van encryptie. Ons onderzoek helpt om de kennisbasis over dit onderwerp te vergroten. De andere methoden die we hebben ingezet voor deskresearch kennen ook beperkingen. De geanalyseerde rechterlijke uitspraken zijn geselecteerd uit een database waarin slechts een beperkt deel van alle rechterlijke uitspraken zijn ondergebracht. Bovendien kan het zijn dat in een vonnis niet expliciet wordt gerept over encryptie of digitale sporen, terwijl daarvan wel sprake was. Bij de media-analyse is selectiviteit mogelijk nog meer van belang. De media belichten vaak de spraakmakende kwesties en dat zijn kwesties als kinderporno en georganiseerde criminaliteit. Dit zegt niets over de grote berg eronder.

Ten aanzien van de survey kunnen twee kritiekpunten worden geïdentificeerd. Sommige respondenten gaven in de open invoervelden aan de vraagstelling soms onduidelijk te vinden. Dit betreft bijvoorbeeld onduidelijkheid over het begrip ‘rol’ en sommige vonden het lastig om antwoord te geven in vorm van percentages. Een aantal respondenten gaf aan dat niet alle vragen relevant waren. Eén respondent gaf aan dat dit komt door het expertisegebied waarvan uit werd geantwoord, namelijk contraterrorisme. Twee anderen gaven aan dat niet alles relevant was omdat zij uitsluitend werken met ontsleutelde cryptocommunicatie.

Tot slot ligt een beperking in het ontbreken van de politiedoelgroep in de verdiepende interviews. In par. 2.4 gaven we de reden daarvoor. Hoewel we inschatten dat een aantal ertoe doende elementen nader aangescherpt had kunnen worden, en daardoor sterkere uitspraken mogelijk waren geweest, denken we niet dat de het ontbreken hiervan tot (heel) andere conclusies hadden geleid. Dit leiden we af uit het feit dat in de verzamelde data geen doemverhalen rond gingen of alarmbellen werden geluid. Aan de andere kant weten we niet exact wat we hierdoor hebben gemist.

Een mogelijke blinde vlek, maar die wel het benoemen waard is, kwam aan bod tijdens een bijeenkomst met de begeleidingscommissie.[54] Dit is de gedachte dat encryptie ook omzeild kan worden

[54] Persoonlijke communicatie (22 december 2022).

wanneer de politie actief is in online groepen, zoals op Telegram. Dit kan een vorm van werken onder dekmantel zijn, waarbij encryptie geen rol meer speelt zodra de politie toegang heeft tot een groep. Met name wanneer het 'open groepen' betreft kan eenvoudig worden meegekeken (OSINT). Dat zou daarmee een alternatief kunnen zijn voor interceptie. Type zaken waarbij dit voorstelbaar is zijn bijvoorbeeld mensenhandel, (illegale) vuurwerkverkoop en openbare ordeverstoringen c.q. rellen. Vervolgonderzoek naar deze mogelijkheid is aan te raden, waarbij niet alleen van belang is om te kijken of het *kan* en wat het oplevert, maar ook in hoeverre dit *mag*. Hier zitten namelijk ook juridische haken en ogen aan, bijvoorbeeld op het gebied van stelselmatigheid (Zuurveen & Stol, 2020).

5.3 Slotbeschouwing

Dit onderzoek ging over de rol die encryptie speelt in de opsporing. Alles overziend concluderen we dat het niet eenvoudig is om deze rol te omschrijven. We kunnen niet vaststellen hoeveel zaken er niet worden opgelost en/of hoeveel tijd verloren gaat. We kunnen ook niet vaststellen hoeveel zaken er extra worden opgelost en/of hoeveel tijd wordt gewonnen. De opsporing is daarvoor een te complex geheel van feiten, toevalligheden en omstandigheden. Het onderzoek geeft dan ook een genuanceerd beeld over wat de toepassing van encryptie – bewust of onbewust – betekent in termen van de opsporing. Er zitten negatieve kanten aan deze toepassing, maar er zijn ook positieve aspecten te benoemen. De vraag is ook wat de toepassing van encryptie nu echt anders maakt? En daarmee de vraag of we dit dan ook anders moeten behandelen?

De politie heeft altijd al te maken met cruciale informatie over criminaliteit die is opgeslagen in een geheugen waartoe zij niet de sleutel heeft. Dat noemen we het menselijk brein. Omdat de politie dat niet kan uitlezen (geen sleutel heeft) en de crimineel niets wil zeggen, moet zij allerlei manieren bedenken om die beveiliging heen te werken en/of de sleutel te bemachtigen en/of iemand er toe te verleiden de informatie prijs te geven. Nu hebben we een computer die net als de crimineel zegt: je komt er niet in en ik zeg niks. Dan moet je als politie dingen bedenken om daar mee om te gaan. Dat deed de politie altijd al. Dus wat is er nu écht anders?

De neiging kan zijn om de huidige situatie – waarin encryptie dus dagelijks aan bod komt – te vergelijken met de situatie waarin digitale informatie nog niet versleuteld was. De vraag die daar achter ligt is welke norm wordt gevolgd. We kunnen stellen dat ten opzichte van vijf, tien of vijftien jaar geleden de huidige situatie lastiger is geworden voor de politie. We kunnen ook stellen dat in die periode de politie, met (of dankzij) encryptie, beschikt over een informatiepositie die in potentie veel groter is dan voorheen. We maken een vergelijking waarbij de politie een appartement in het vizier heeft waar vermoedelijk criminele activiteiten plaatsvinden. Op het moment dat een dergelijk pand wordt binnengedrongen komt er veel informatie ter beschikking. Met encryptie is er nu niet slechts toegang tot dat ene appartement, maar tot alle appartementen binnen het complex. Dit heeft niet alleen te maken met ontwikkelingen in de opsporing, maar ook met criminele afhankelijkheidsrelaties die voor een belangrijk deel gedigitaliseerd zijn. De principes blijven hetzelfde; wel maakt encryptie het mogelijk dat – in potentie – veel meer gegevens inzichtelijk zijn. Uiteindelijk vergt digitalisering meebewegen en aanpassen aan wat er op ons af komt. Daarin zit de voortdurende uitdaging.

Referenties

Aben, D.J.C., & Luining, E.T. (2022). *Onderzoek in een geautomatiseerd werk: Over de toepassing van opsporingsbevoegdheden als bedoeld in de artikelen 126nba lid 1, 126uba lid 1 en 126zpa lid 1 van het Wetboek van Strafvordering door het Openbaar Ministerie.* Den Haag: Procureur-generaal bij de Hoge Raad der Nederlanden.

Algemene Inlichtingen- en Veiligheidsdienst (AIVD) (2012). *Het jihadistisch Internet: Kraamkamer van de hedendaagse jihad.* Verkregen via: https://www.aivd.nl/documenten/publicaties/2012/02/14/het-jihadistisch-internet-kraamkamer-van-de-hedendaagse-jihad

Algemene Inlichtingen- en Veiligheidsdienst (AIVD) (2022). *Tijdelijke wet verbetert cyberonderzoek van inlichtingendiensten*. Verkregen via: https://www.aivd.nl/onderwerpen/onderzoeksopdrachtgerichte-interceptie-oog/nieuws/2022/04/01/tijdelijke-wet-verbetert-cyberonderzoek-van-inlichtingendiensten

Boerman, F., Grapendaal, M., Nieuwenhuis, F., & Stoffers, E. (2017). *Nationaal dreigingsbeeld 2017: Georganiseerde criminaliteit.* Driebergen: Nationale Politie.

Bloom, M., Tiflati, H., & Horgan, J. (2017). Navigating ISIS's preferred platform: Telegram. *Terrorism and Political Violence, 31*(6), 1242-1254.

Cachet, A. (1990). *Politie en sociale controle*. Arnhem: Gouda Quint.

Conlan, K., Baggili, I., & Breitinger, F. (2016). Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. *Digital investigation, 18*, S66-S75.

Council of the European Union (2016). *Encryption: Challenges for criminal justice in relation to the use of encryption – future steps*. Verkregen via: https://data.consilium.europa.eu/doc/document/ST-14711-2016-COR-1/en/pdf

Council of the European Union (2017). *Final report of the seventh round of mutual evaluations on "The practical implementation and operation of the European policies on prevention and combating cybercrime".* Verkregen via: https://data.consilium.europa.eu/doc/document/ST-12711-2017-INIT/en/pdf

Custers, B. (2018). Nieuwe online opsporingsbevoegdheden en het recht op privacy: Een analyse van de Wet computercriminaliteit III. *Justitiële verkenningen*, *44*(5), 100-117.

Cybersecurity Alliantie & Cyberveilig Nederland (2021). *Cybersecurity woordenboek 2021: Van cybersecurity naar Nederlands.* Verkregen via: https://www.cybersecurityalliantie.nl/ecp_images/2021/12/Cybersecurity-Woordenboek-2021_ZonderSpreads.pdf

Eeden, C.A.J. van den, Berkel, J.J. van, Lankhaar, C.C., & Poot, C.J. de (2021). Opsporen, vervolgen en tegenhouden van cybercriminaliteit. Cahiers.

Emmen, B., Poot C.J. de, & Stol, W.Ph. (te verwachten). *What are they doing in the dark? Police strategies and working methods in fighting crime on the Tor network.*

ENISA (2022). *The EU Cybersecurity act*. Verkregen via: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

Europese Raad (2020). *Versleuteling: Raad neemt resolutie aan over beveiliging dankzij en ondanks versleuteling*. Verkregen via: https://www.consilium.europa.eu/nl/press/press-releases/2020/12/14/encryption-council-adopts-resolution-on-security-through-encryption-and-security-despite-encryption/

Europol (2019). *Do criminals dream of electric sheep? How technology shapes the future of crime and law enforcement.* Verkregen via: https://www.europol.europa.eu/sites/default/files/documents/report_do_criminals_dream_of_electric_sheep.pdf

Europol (2020a). *Europol and the European Commission inaugurate new decryption platform to tackle the challenge of encrypted material for law enforcement investigations*. Verkregen via: https://www.europol.europa.eu/media-press/newsroom/news/europol-and-european-commission-inaugurate-new-decryption-platform-to-tackle-challenge-of-encrypted-material-for-law-enforcement

Europol (2020b). *Europol programming document 2020 – 2022.* Verkregen via: https://www.europol.europa.eu/sites/default/files/documents/europol_programming_document_2020-2022.pdf

Europol (2021a). *800 criminals arrested in biggest ever law enforcement operation against encrypted communication*. Verkregen via: https://www.europol.europa.eu/media-press/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication

Europol (2021b). *European Union serious and organised crime threat assessment (SOCTA) 2021.* Verkregen via: https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021

Europol (2021c). *Internet Organised Crime Threat Assessment (IOCTA) 2021*. Verkregen via: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021

Europol (2021d). *New major interventions to block encrypted communications of criminal networks*. Verkregen via: https://www.europol.europa.eu/media-press/newsroom/news/new-major-interventions-to-block-encrypted-communications-of-criminal-networks

Europol & Eurojust Public Information (2018). *Common challenges in combating cybercrime.* Verkregen via: https://www.europol.europa.eu/publications-events/publications/common-challenges-in-combating-cybercrime

Europol & Eurojust Public Information (2019). *First report of the observatory function on encryption.* Verkregen via: https://www.eurojust.europa.eu/sites/default/files/2019-01/2019-01_Joint-EP-EJ-Report_Observatory-Function-on-Encryption_EN.pdf

Europol & Eurojust Public Information (2020a). *Dismantling of an encrypted network sends shockwaves through organized crime groups across Europe*. Verkregen via: https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe

Europol & Eurojust Public Information (2020b). *Second report of the observatory function on encryption*. Verkregen via: https://www.europol.europa.eu/publications-events/publications/second-report-of-observatory-function-encryption

Europol & Eurojust Public Information (2021). *Third report of the observatory function on encryption.* Verkregen via: https://www.europol.europa.eu/publications-events/publications/third-report-of-observatory-function-encryption

European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) & Europol (2017). *Drugs and the darknet: Perspectives for enforcement, research and policy.* Verkregen via: https://www.emcdda.europa.eu/system/files/publications/6585/TD0417834ENN.pdf

Foucault, M. (1979, oorspr. 1975). *Discipline and punish: The birth of the prison.* NY: Vintage Books.

Fukami, A., Stoykova, R., & Geradts, Z. (2021). A new model for forensic data extraction from encrypted mobile devices. *Forensic Science International: Digital Investigation*, *38*, 301169.

Goodison, S.E., Woods, D., Barnum, J.D., Kemerer, A.R., & Jackson, B.A. (2019). *Identifying law enforcement needs for conducting criminal investigations involving evidence on the dark web*. Santa Monica, CA: RAND Corporation.

Hartel, P., & Wegberg, R. van (2021). Going dark? Analysing the impact of end-to-end encryption on the outcome of Dutch criminal court cases. *Computers and Society.* https://doi.org/10.48550/arXiv.2104.06444

Henseler, J. (2010). *E-discovery: Op zoek naar de digitale waarheid*. Amsterdam: HvA.

Henseler, J. (2017). *De (r)evolutie van digital bewijs*. Leiden: Hogeschool Leiden.

Holt, T.J., Cale, J., Leclerc, B., & Drew, J. (2020). Assessing the challenges affecting the investigative methods to combat online child exploitation material offenses. *Aggression and Violent Behavior*, *55*, 101464. https://doi.org/10.1016/j.avb.2020.101464

Ilbiz, E., & Krauner, C. (2022). Europol and cybercrime: Europol's sharing decryption platform. *Journal of Contemporary European Studies, 30*(2), 270-283.

Jansen, J., Westers, S., Twickler, S., & Stol, W.Ph. (2019). *Aankoopfraude vanuit het buitenland: Alternatieven voor opsporing.* Den Haag: Sdu (reeks Politiekunde).

Jansen, J., Valkengoed, T. van, Veenstra, S., & Stol, W.Ph. (2020). *Level-up! Kennis voor politiewerk in een digitale samenleving*. Leeuwarden: Onderzoeksgroep Cybersafety (NHL Stenden Hogeschool).

Kerr, O.S., & Schneier, B. (2017). Encryption workarounds. *Georgetown Law Journal, 106*(4)*,* 989.

Koomen, M. (2021). *The encryption debate in the European Union: 2021 update*. Verkregen via: https://carnegieendowment.org/files/202104-EU_Country_Brief.pdf

Losavio, M.M., Pastukov, P., Polyakova, S., Zhang, X., Chow, K.P., Koltay, A., … & Ortiz, M.E. (2019). The juridical spheres for digital forensics and electronic evidence in the insecure electronic world. *Wiley Interdisciplinary Reviews: Forensic Science*, *1*(5), e1337.

Manhattan District Attorney's Office (2019). *Report of the Manhattan district Attorney's office on smartphone encryption and public safety: An update to the November 2018 report*. Verkregen via: https://www.manhattanda.org/wp-content/uploads/2019/10/2019-Report-on-Smartphone-Encryption-and-Public-Safety.pdf

Manpearl, E. (2017). Preventing "going dark": A sober analysis and reasonable solution to preserve security in the encryption debate. *University of Florida Journal of Law and Public Policy, 28*(1), 65.

Mevis, P.A.M, Verbaan, J.H.J., & Salverda, B.A. (2016). *Onderzoek aan in beslag genomen elektronische gegevensdragers en geautomatiseerde werken ten behoeve van de opsporing en vervolging van strafbare feiten.* Den Haag: WODC.

Moore, D., & Rid, T. (2016). Cryptopolitik and the darknet. *Survival*, *58*(1), 7-38.

National Center for Missing and Exploited Children (NCMEC) (2020). *2020 CyberTipline reports by electronic service providers (ESP).* Verkregen via: https://www.missingkids.org/content/dam/missingkids/pdfs/2020-reports-by-esp.pdf

Nationale Politie (2021). Bewijs zoekt zaak. *Scherp: Over intelligence gestuurd politiewerk*, 22-24. Den Haag: Nationale Politie.

NCTV (2021). *Dreigingsbeeld Terrorisme Nederland 54.* Den Haag: Nationaal Coördinator Terrorismebestrijding en Veiligheid.

Nogala, D., & Schröder, D. (2019). Innovations In law enforcement. *European Law Enforcement Research Bulletin*, (4 SCE), 7-17.

Odinot, G., Jong, D. de, Leij, J.B.J. van der, Poot, C.J. de, & Straalen, E.K. van (2012). *Het gebruik van de telefoon- en internettap in de opsporing.* Meppel: Boom Lemma (WODC).

Oerlemans, J.J. (2012). Mogelijkheden en beperkingen van de internettap. *Justitiële Verkenningen, 38*(3), 35-49.

Oerlemans, J.J. (2017). *Investigating cybercrime*. Amsterdam: Amsterdam University Press.

Oerlemans, J.J. (2019). *Cybercrime jurisprudentieoverzicht – december 2019*. Verkregen via: https://jjoerlemans.com/tag/bulletproof-hosting/

Oerlemans, J.J. (2022). *Overzicht cryptophone-operaties*. Verkregen via: *https://jjoerlemans.com/2022/11/14/overzicht-cryptophone-operaties/*

Pisariç, M. (2021). Encryption as a challenge for European law enforcement agencies. *Australasian Policing*, *13*(1), 30-34.

PricewaterhouseCoopers (2020). *Doorlichting strafrechtketen: Nieuwe uitdagingen vragen om optimalisatie van samenwerking.* Verkregen via: https://www.rijksoverheid.nl/documenten/rapporten/2020/06/26/tk-bijlage-ii-pwc-doorlichting-strafrechtketen

Raad van de Europese Unie (2016). *Encryption: Challenges for criminal justice in relation to the use of encryption – future steps*. Verkregen via: https://data.consilium.europa.eu/doc/document/ST-14711-2016-INIT/en/pdf

Sharma, D.K., Singh, N.C., Noola, D.A., Doss, A.N., & Sivakumar, J. (2022). A review on various cryptographic techniques & algorithms. *Materials Today: Proceedings*, *51*, 104-109.

Stol, W.Ph. (1996). *Politieoptreden en informatietechnologie.* Lelystad: Koninklijke Vermande.

Stol, W.Ph. (2014). Informatie voor politiewerk: Basisprincipes. In E.R. Muller, E.J. van der Torre, A.B. Hoogenboom en N. Kop (red.), *Politie: Studies over haar werking en organisatie.* Deventer: Kluwer, pp. 231-246.

Stol, W.Ph., & Jansen, J. (te verwachten). *Politie in een digitaliserende samenleving*. Politiehandboek.

Stol, W.Ph., Kop, N., & Koppenol, P.A. (2005). *Eén spoor is geen spoor. Naar een landelijke databank voor informatiegestuurde opsporing.* Den Haag: Elsevier Overheid.

Stol, W.Ph., & Strikwerda, L. (2017). *Strafrechtspleging in een digitale samenleving*. Den Haag: Boom Juridische Uitgevers.

The United States Department of Justice (2020). *International statement: End-to-end encryption and public safety.* Verkregen via: https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety

Uden, A. van, & Eeden, C.A.J. van den (2022). *De hackbevoegdheid in de praktijk: Een empirisch onderzoek naar de uitvoering van de hackbevoegdheid (artikelen 126nba, 126uba, 126zpa Sv).* Den Haag: WODC.

United States Courts (2020). *Wiretap reports*. Verkregen via: https://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports

Yar, M. (2006). *Cybercrime and society*. Londen: Sage Publication.

Veenstra, S., Zuurveen, R., Kerstens, J., & Stol, W.Ph. (2016). *Opsporing in een gedigitaliseerde samenleving: Een handreiking voor het herkennen, vinden en benutten van digitale sporen*. Leeuwarden: Onderzoeksgroep Cybersafety (NHL Stenden Hogeschool).

Vermeulen, I., Soudijn, M., & Leest, W. van der (2021). Open heimelijke netwerken in de Nederlandstalige georganiseerde synthetische drugscriminaliteit. *Tijdschrift voor Criminologie*, *63*(2).

Zuurveen, R., & Stol, W.Ph. (2020). *Benutten van digitale sporen*. Den Haag: Sdu (reeks Politiekunde).

Bijlage I: Begrippen- en afkortingenlijst

Tabel I.1: Begrippenlijst

Begrip	**Uitleg**	**Opmerking (i.v.m. encryptie en opsporing)**
Advanced Encryption Standard (AES)	Momenteel de belangrijkste encryptiestandaard met symmetrische sleutels. Het wordt gebruikt in alle belangrijke software. Afhankelijk van de gebruikssituatie kan AES worden gebruikt met 128-, 192- en 256-bits lange encryptiesleutels.	AES kan in de praktijk niet gekraakt worden. De encryptie kan mogelijk worden omzeild.
Asymmetrische codering	Het gebruik van een openbare sleutel voor codering en een openbare sleutel gecombineerd met een privésleutel voor decodering.	
Bruteforcen	Het systematisch uitproberen van wachtwoorden en encryptiesleutels.	
Carrier-Grade Network Address Translation (CGN)	Net als Tor, stelt CGN gebruikers in staat om hun IP-adressen te verbergen. In tegenstelling tot Tor kan met CGN een enkel IP-adres worden gedeeld door duizenden gebruikers tegelijk.	Het is niet meer mogelijk om een IP-adres van een gebruiker vanuit het internet vast te stellen.
Chatbot	Software die een natuurlijk gesprek simuleert.	
Cryptografische hashfuncties	Het toepassen van een algoritme op data om een hashcode te construeren.	
Dark web	Ook wel darknet genoemd. Een besloten deel van het internet dat men niet vindt met normale browsers en zoekmachines.	
Decryptie	Het proces van het omzetten van versleutelde data naar de originele staat met gebruik van een cryptografische sleutel. Een ander woord voor decryptie is ontsleutelen of ontcijferen.	
Domain Name System (DNS)	DNS is een wereldwijd naamgevingssysteem dat gebruiksvriendelijke namen aan computervriendelijke IP-adressen koppelt. Naast dit systeem wordt DNS ook gebruikt voor het protocol dat de DNS-berichten tussen de cliënt en het DNS-systeem specificeert. Bij het verzoeken van het DNS-systeem worden DNS-resolvers gebruikt die de cliënt ondersteunen. Een resolver is verantwoordelijk voor het initiëren en rangschikken van de DNS-verzoeken die uiteindelijk leiden tot een volledige resolutie (vertaling) van de gezochte bron, bijvoorbeeld de vertaling van een domeinnaam naar een IP-adres.	DNS-verkeer wordt niet standaard geauthentiseerd wat het mogelijk maakt om valse servers te gebruiken om gebruikers te misleiden naar criminele webservers. Tevens is DNS-verkeer niet versleuteld waardoor men de data kan lezen.

Tabel I.1 (vervolg): Begrippenlijst

Begrip	Uitleg	Opmerking (i.v.m. encryptie en opsporing)
DNS of HTTPS (DoH)	DNS over HTTPS (DoH) is een relatief nieuw protocol dat het systeemverkeer van domeinnamen versleutelt door DNS-verzoeken door te geven via een HTTPS-geëncrypte sessie.	Door DoH wordt meer privacy en beveiliging bereikt: de bezochte webadressen en IP-adressen worden verborgen en DNS-berichten kunnen niet worden aangepast.
Elliptic Curve Cryptography (ECC)	Een benadering van cryptografie met publieke sleutels die kleinere encryptiesleutels mogelijk maakt in vergelijking met niet-EC-cryptografie om gelijkwaardige beveiliging te bieden.	Een manier om de beveiligingsniveaus van cryptografische systemen te vergelijken is m.g.v. sleutellengtes. Een AES-systeem met 128-bits sleutels komt qua beveiliging ruwweg overeen met een 3072-bits RSA- of een 256-bits ECC-sleutel.
Encryptie	Het proces van het omzetten van data, zoals berichten of delen van informatie, ter preventie ongeautoriseerde toegang. Kortom, de techniek om geheimhouding te bewerkstelligen. Een ander woord voor encryptie is versleutelen of vercijferen.	
End-to-end encryptie (E2EE)	Een geavanceerd communicatiesysteem waarbij alleen de afzender en ontvanger(s) de berichten kunnen lezen door te voorkomen dat potentiële afluisteraars toegang krijgen tot de cryptografische sleutels	Deze afluisteraars zijn onder meer telecom- en internetproviders, kwaadwillende actoren, overheden en zelfs de aanbieder van de communicatiedienst.
HTTPS	HTTP-verkeer over TLS.	HTTPS creëert E2EE tussen een browser en een webserver.
International Mobile Subscriber Identity (IMSI)	Een nummer gekoppeld aan het 06-nummer van de telefoon. Met een IMSI-nummer kan de locatie van een telefoon exacter worden vastgesteld dan met een 06-nummer.	
Internet Service Provider (ISP)	Een organisatie die diensten levert voor toegang tot, gebruik van of deelname aan internet.	ISP's kunnen vaak IP-adressen en verkeersinhoud zien. Vandaag de dag is dit aan het veranderen dankzij E2EE en andere privacy- en beveiligingsmechanismen.
Klare tekst	De oorspronkelijke tekst i.v.m. encryptie. Ook wel leesbare tekst genoemd (plaintext in het Engels).	
Open source	Het publiek beschikbaar zijn van de broncode.	
Pretty Good Privacy (PGP)	Een versleutelingsprogramma dat voornamelijk wordt gebruikt voor het ondertekenen, encrypten en ontsleutelen van e-mails.	OpenPGP is een open internetstandaard van PGP.

Tabel I.1 (vervolg): Begrippenlijst

Begrip	**Uitleg**	**Opmerking (i.v.m. encryptie en opsporing)**
RSA	RSA (vernoemd naar de uitvinders Rivest, Shamir en Adleman) is een beroemd en veelgebruikt cryptografisch systeem voor encryptie en digitale handtekeningen met gebruik van publieke sleutels.	
Side-channel-aanval	Een aanval op basis van extra informatie die kan worden verzameld vanwege de fundamentele manier waarop een encryptiealgoritme wordt geïmplementeerd, in plaats van gebreken in het ontwerp van het algoritme zelf.	Timinginformatie, stroomverbruik, elektromagnetische lekken en geluid zijn voorbeelden van die extra informatie. Meestal is fysieke toegang nodig tot het apparaat dat de encryptie/decryptie uitvoert.
Sleutel (cryptografisch)	Een set van gegevens (bijv. bits) dat wordt gebruikt bij het cijfer om een leesbare tekst te versleutelen.	
Steganografie	Een verscholen boodschap aangebracht in een drager.	
Symmetrische codering	Het gebruik van één sleutel voor zowel de codering als decodering.	
The Onion Router (Tor)	Een methode om anoniemer op het internet te surfen die ook toegang tot het dark web.	
Tor browser	Een browser die directe toegang geeft aan het Tor-netwerk, waardoor gebruikers de IP-adressen van hun computers kunnen verbergen.	
Transport Layer Security (TLS)	Een netwerkprotocol om de applicatiedata te beschermen met encryptie. Technisch ligt TLS tussen het TCP-protocol en de socket van een applicatieproces. TLS is de opvolger van SSL en zijn nieuwste versie is sinds 2017 versie TLS 1.3.	Op het web wordt de meeste data in communicatie door TLS versleuteld. Verkeer dat wordt beveiligd door TLS 1.2 kan grote zwakke punten hebben die kunnen worden misbruikt om de leesbare tekst te vinden.
User-enrolled encryptie	De serviceprovider heeft geen sleutel voor gebruikersdata, waardoor gebruikers ultieme controle hebben over de encryptie en decryptie van de data.	
Virtual Private Network (VPN)	Een uitbreiding van een computernetwerk over een openbaar netwerk.	VPN stelt een gebruiker in staat om i.p.v. het eigen IP-adres het IP-adres van de VPN-server te laten zien.
Whitebox-analyse	Het onderzoeken van de broncodes van softwaresystemen.	

Tabel I.2: Afkortingenlijst

Afkorting	Uitleg
ACN	Anonymous Communications Network
AES	Advanced Encryption Standard
AI	Artificiële intelligentie (kunstmatige intelligentie)
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
BOB	Bijzondere Opsporingsbevoegdheden
CEO	Chief Executive Officer
CGN	Carrier-Grade Network
CSAM	Child Sexual Abuse Material
DES	Data Encryption Standard
DIGIT	Digital Intrusion Team
DOJ	Department of Justice
DRD	Data Retention Directive
DSI	Dienst Speciale Interventies
E2EE	End-to-End Encryptie
EC3	European Cybercrime Centre
ECC	Elliptic Curve Cryptography
EIO	European Investigation Order
EMCDDA	European Monitoring Centre for Drugs and Drug Addiction
ENISA	Europees Agentschap voor Netwerk- en Informatiebeveiliging
EU	Europese Unie
EVRM	Europees Verdrag voor de Rechten van de Mens
FIOD	Fiscale Inlichtingen- en Opsporingsdienst
FBI	Federal Bureau of Investigation
GDDP	Government Disclosure Decision Process
GPS	Global Positioning System
GSM	Global System for Mobile communication
HIC	High Impact Crime
I2P	Invisible Internet Project
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IP	Internet Protocol
ISP	Internet Service Provider
JIT	Joint Investigation Team
KMAR	Koninklijke Marechaussee
LOVS	Landelijk Overleg Vakinhoud Strafrecht
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
MLA	Mutual Legal Assistance
NC3	National Cybercrime Coordination Centre
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NFI	Nederlands Forensisch Instituut
NIST	National Institute of Standards and Technology
NIT	Network Investigation Technique
NSA	National Security Agency
OM	Openbaar Ministerie
OOG	Onderzoeksopdrachtgerichte interceptie

Tabel I.2 (vervolg): Afkortingenlijst

Afkorting	Uitleg
OS	Operationeel Specialist
OSINT	Open Source INTelligence
OTT	Over-The-Top
OvJ	Officier van Justitie
PGP	Pretty Good Privacy
RC	Rechter-commissaris
RM	Rechterlijke Macht
Rvdr	Raad voor de rechtspraak
Sr	Wetboek van Strafrecht
Sv	Wetboek van Strafvordering
TBKK	Team Bestrijding Kinderporno en Kindersekstoerisme
TDO	Team Digitale Opsporing
THTC	Team High Tech Crime
TIB	Toezichtscommissie Inzet Bevoegdheden
TLS	Transport Layer Security
Tor	The Onion Router
TPM	Trusted Platform Module
USB	Universal Serial Bus
VCAT	Voorziening Crypto Analyse Team
VPN	Virtual Private Network
VS	Verenigde Staten
VVC	Veelvoorkomende criminaliteit

Bijlage II: Interviewprotocol oriënterende fase

Inleiding. Op verzoek van het wetenschappelijk onderzoek- en documentatiecentrum (WODC) onderzoekt de onderzoeksgroep Cybersafety van NHL Stenden Hogeschool, i.s.m. de Politieacademie en de Open Universiteit, de rol van encryptie in opsporingsonderzoeken van de politie. Vooralsnog is onduidelijk wat de precieze rol is van encryptie hierin.

Reden oriënterende interviews. Encryptie binnen de strafrechtketen is een veelomvattend onderwerp. Om het onderzoek te focussen willen we om te beginnen vaststellen of encryptie een rol speelt in de behandeling van zaken in de strafrechtketen, en zo ja hoe die rol eruit ziet. Daarnaast willen we verkennen welke toepassingen van encryptie zoal voorkomen, op welke wijze deze voorkomen, en zijn we benieuwd naar ontwikkelingen op dit gebied in de afgelopen vijf jaar. Antwoorden op die vragen helpt ons om het onderzoek nader af te bakenen.

Belangrijke informatie vooraf.

- Alle input wordt in principe anoniem verwerkt in het onderzoeksrapport. Toestemming vragen voor het in een bijlage (lijst van respondenten) noemen van naam, functie en/of organisatie(onderdeel) in het eindrapport.
- Het verslag van dit interview wordt ter verificatie voorgelegd. De geïnterviewde heeft, indien relevant, de mogelijkheid om de eerder gegeven toestemming in te trekken. Ook mag de geïnterviewde deelname aan het onderzoek op elk moment stoppen, zonder opgave reden.
- Toestemming tot opname? Wordt alleen gebruikt voor uitwerkingsdoeleinden en vernietigd na verificatie van het verslag door de geïnterviewde én het vaststellen van het definitieve verslag. Het geanonimiseerde verslag wordt op veilige wijze voor tien jaar bewaard en kan, op verzoek van de opdrachtgever, worden opgevraagd door het WODC.
- Geïnterviewde gelegenheid bieden tot het stellen van vragen over het onderzoek.
- 'Informed consent'-formulier digitaal laten tekenen.

Introductie.

1. Kunt u iets vertellen over uw functie en welke rol u hebt (in het opsporingsproces)?

Aard en omvang.
**Instructie: Afhankelijk van achtergrond/organisatie geïnterviewde vragen 2 en 3 omdraaien. Ook rekening houden met expertise geïnterviewde aangaande vervolgvragen.*

2. Speelt encryptie een rol in de opsporing? Zo ja, wat is die rol?
   **Instructie: Doorvragen naar positieve en negatieve aspecten van die rol.*

3. Speelt encryptie een rol in de doorstroom van zaken in de strafrechtketen? Zo ja, wat is die rol?
   **Instructie: Doorvragen naar positieve en negatieve aspecten van die rol.*

4. Bent u in het afgelopen jaar in aanraking gekomen met encryptie in de opsporing / uw werk?
   a. Zo ja, wat deed zich toen voor? Welke rol speelde encryptie toen?

**Instructie: Indien niet spontaan benoemd, ingaan op toepassing(en) van encryptie:*

i. t.b.v. het versleutelen van communicatie (end-to-end encryptie van diensten zoals cryptotelefoons, WhatsApp, Signal, Telegram en ProtonMail)
ii. t.b.v. het versleutelen van apparaten/hardware (zoals smartphones en harde schijven, denk aan VeraCrypt, BitLocker en FileVault)
iii. t.b.v. van onlinediensten (zoals cloudopslag, bulletproof hosting en betalingsverkeer [crypto currency])
iv. Specifieke tools voor het verhullen van digitale locaties (IP-adres) anders dan encryptie (zoals VPN en Tor)

b. Maakte encryptie het de opsporing daarmee moeilijk of juist makkelijk?

5. In welke situaties komt [de genoemde toepassing(en) van] encryptie voor?
   **Instructie: Indien niet spontaan benoemd, ingaan op:*
   i. Bij wat voor opsporingsonderzoeken speelt encryptie een rol?
   ii. Bij welk type delicten speelt encryptie een rol?
   iii. Wie maken gebruik van encryptie?

6. Hoe vaak bent u (en/of uw collega's) in het afgelopen jaar in aanraking gekomen met [de genoemde toepassing(en) van] encryptie?
   a. In welke situatie/omstandigheden komt encryptie voor? Hoe vaak komt dát voor (aantal keer per jaar en percentage)?

7. Is de aard en omvang van encryptie in de opsporing in de afgelopen vijf jaar (tussen 2016-2020) veranderd, en zo ja in welk opzicht?

Rol encryptie.

We willen nu met u meer gedetailleerd in gesprek over uw ervaringen omtrent de rol van encryptie in de opsporing waar u en/of u collega's bij zijn betrokken en/of waar u veel vanaf weet. Wij zijn daarbij vooral benieuwd naar algemene principes, en niet zozeer naar specifieke zaken.

**Instructie: Houdt rekening met positieve en negatieve aspecten van die rol in onderstaande vragen.*

8. Speelt encryptie een rol in het *verloop* van opsporingsonderzoeken? Zo ja, wat voor rol?

Toelichting 'verloop'. Hiermee bedoelen we bijvoorbeeld de slagingskans om encryptie te kraken, te omzeilen of alternatieve opsporingsmiddelen in te zetten en wat dit betekent in termen van inzet van mensen en middelen (o.a. doorlooptijd, menskracht, expertise, aanschaf soft-/hardware).

   a. Speelt encryptie een rol in de voortzetting van opsporingsonderzoeken? Zo ja, wat voor rol?
      i. Hoe vaak komt dit voor (aantal keer per jaar en percentage)?
   b. Speelt encryptie een rol in de doorlooptijd van opsporingsonderzoeken? Zo ja, wat voor rol?
      i. Hoe vaak komt dit voor (aantal keer per jaar en percentage)?

c. Hoe vaak lukt het om toegang te krijgen tot voor de opsporing relevante digitale informatie in zaken waarin encryptie voorkomt?
    i. Wat is over het geheel genomen de slagingskans (aantal en percentage)?
    ii. Op welke wijze?
        **Instructie: Indien niet spontaan benoemd, de volgende suggesties noemen:*
        - Encryptie kraken
        - Encryptie omzeilen *(1. Vind de sleutel, 2. Raad de sleutel, 3. Dwing de sleutel af, 4. Misbruik fouten in encryptieschema, 5. Toegang tot klare tekst [i.e., de oorspronkelijke, leesbare tekst] wanneer apparaat in gebruik is, 6. Zoek kopie van klare tekst).*
        - Alternatieve opsporingsmiddelen inzetten. Zo ja, hoe effectief zijn deze? *(Bijv. tijdsinvestering en bruikbaarheid)*
    iii. Onder welke omstandigheden?
    iv. Welke mensen en/of middelen zijn nodig?
    v. Wat betekent dit voor het opsporingsproces? *(Bijv. zicht op hoeveelheid en bruikbaarheid van data)*

d. [**geschikt voor IT-experts*]
    i. Wat zijn relevante technische aspecten van encryptie met betrekking tot opsporing?
    **Instructie: Indien nodig encryptiealgoritmen en sleutellengten als voorbeelden noemen.*
    ii. Hoe beïnvloeden externe technische factoren de efficiëntie van het kraken van de encryptie?
    **Instructie: Indien nodig open source broncode en slordig sleutelbeheer als voorbeelden noemen.*

9. Speelt encryptie een rol in de *opbrengst* van opsporingsonderzoeken? Zo ja, wat voor rol?

Toelichting 'opbrengst'. Hiermee bedoelen we in hoeverre encryptie van invloed is op bijvoorbeeld het identificeren en/of lokaliseren van relevante personen en het succesvol achterhalen van bewijsmateriaal. Meer concreet: in hoeverre encryptie van invloed is op de mogelijkheden om verdachten succesvol of kansrijk te kunnen vervolgen.

**Instructie: Indien niet spontaan benoemd, ingaan op rol aangaande:*
a. het identificeren en/of lokaliseren van relevante personen / goederen?
b. het signaleren criminele activiteiten?
c. het vergaren van bewijsmateriaal?
d. Andersoortige rol/invloed/bijvangst? (bijv. grote hoeveelheden data)
    i. Hoe vaak komt het door respondent benoemde (eigen input en 9a-d) voor (aantal keer per jaar en percentage)?

10. Alles overziend, in welke situatie(s) speelt encryptie de grootste rol, positief danwel negatief, ten aanzien van de opsporing? (*noem maximaal twee)

Strafrechtelijke vervolging.
We willen nu met u meer gedetailleerd in gesprek over uw ervaringen omtrent de rol van encryptie in de strafrechtelijke vervolging.
**Instructie: Houdt rekening met positieve en negatieve aspecten van die rol in onderstaande vragen.*
***Instructie: Wees alert op antwoorden op gebied van opsporing versus verstoren.*

11. Speelt encryptie een rol in de strafrechtelijke vervolging van zaken? Zo ja, hoe?
    a. Speelt encryptie een rol in de beslissing van het OM omtrent het inzetten van opsporingsbevoegdheden? Zo ja, hoe?
        i. Hoe vaak komt dit voor (aantal keer per jaar en percentage)?
    b. Speelt encryptie een rol in de mogelijkheid om verdachten succesvol of kansrijk te kunnen vervolgen? Zo ja, hoe?
        i. Hoe vaak komt dit voor (aantal keer per jaar en percentage)?

12. Speelt encryptie een rol in de rechterlijke afdoening van zaken? Zo ja, hoe?

13. [**geschikt voor juridisch/ethisch*]
    a. Zijn er juridische aspecten die een rol spelen bij zaken in de opsporing waarin encryptie voorkomt? Zo ja, welke?
        i. Hoe vaak komt dit voor (aantal keer per jaar en percentage)?
    b. Zijn er ethische aspecten die een rol spelen bij zaken in de opsporing waarin encryptie voorkomt? Zo ja, welke?
        i. Hoe vaak komt dit voor (aantal keer per jaar en percentage)?

Afsluiting.
Wij zijn hiermee aan het einde gekomen van het interview. Tot slot willen we u graag nog enkele praktische vragen stellen omtrent het onderwerp.

14. Hebt u interessante bronnen omtrent dit onderwerp die u met ons kunt delen en/of kent u geschikte databronnen om informatie over dit onderwerp op te halen?

15. Kent u interessante mensen/experts in uw netwerk om ook een interview mee te houden? Zo ja, kunt u ons met hen in contact brengen?

16. Begin 2022 start een tweede interviewronde waarin we meer de diepte in willen gaan op dit onderwerp. Hebt u interesse in deelname aan een verdiepend interview?
    **Instructie: T.o.v. het huidige interview wordt dieper ingegaan op de hoofdlijnen die we tijdens dit interview bespraken. Dus meer op details, oplossingen, alternatieven, etc.*

17. Hebt u nog suggesties of anderszins opmerkingen omtrent dit onderwerp die we niet hebben besproken in het interview, maar die u wel graag wilt delen?

**Instructie: Procedure uitwerking (zie p.1) kort herhalen en respondent bedanken voor deelname.*

Bijlage III: Informed consent formulier interviews

1. Ik ben over het onderzoek geïnformeerd en heb het doel van het interview begrepen.

2. Ik ben in de gelegenheid gesteld om vragen over het onderzoek te stellen.

3. Ik heb de tijd gehad over mijn deelname aan het interview kunnen nadenken.

4. Ik geef toestemming voor het gebruik van de gegevens, waaronder (bijzondere) persoonsgegevens, die tijdens dit interview worden verzameld en verwerkt voor dit onderzoek.

5. Ik geef toestemming voor het gebruik van de gegevens door derden (WODC), zoals mondeling toegelicht.

6. Ik heb mijn toestemming(en) in volledige vrijheid gegeven. Niemand dwingt mij (zowel niet direct als indirect) om aan dit interview mee te doen.

7. Ik ben ervan verzekerd dat ik niet te identificeren ben in door dit onderzoek naar buiten gebrachte gegevens, rapporten, presentaties of artikelen. Mijn privacy en mijn persoonsgegevens zijn gewaarborgd als deelnemer van dit interview.

8. Ik begrijp dat ik op elk moment mijn deelname aan het onderzoek kan beëindigen en mijn toestemming kan intrekken op de wijze zoals mondeling toegelicht en ik hoef daar geen reden voor op te geven. De gegevens die tot dat moment zijn verzameld, mogen geanonimiseerd worden gebruikt voor het onderzoek.

9. Ik begrijp dat de verzamelde gegevens minimaal 10 jaar, op een veilige manier, door NHL Stenden Hogeschool worden bewaard.

Vragen

1. Bij deze geef ik akkoord op bovengenoemde 9 stellingen.
    - Akkoord
    - Niet akkoord
2. Wat is uw naam? [open veld]
3. Wat is uw functie? [open veld]
4. Welke gegevens mogen we gebruiken in het rapport?
    - Uw naam en uw functie
    - Alleen uw functie
    - Beide niet, ik wens anoniem te blijven
5. Wilt u nog iets toevoegen? [open veld]

Bijlage IV: Uitnodiging vragenlijst

Onderwerp Uitnodiging voor onderzoek naar de rol van encryptie in de opsporing

Beste heer/mevrouw,

Mijn naam is Jurjen Jansen, lector digitale weerbaarheid bij NHL Stenden Hogeschool en senior onderzoeker bij de Politieacademie. Ik wil u vragen om mee te werken aan een onderzoek naar de rol van encryptie in de opsporing. Hieronder leg ik uit wat het onderzoek inhoudt en hoe u mee kunt doen.

Doel en achtergrond van het onderzoek
Op verzoek van het wetenschappelijk onderzoek- en documentatiecentrum (WODC) onderzoekt de onderzoeksgroep Cybersafety van NHL Stenden Hogeschool, i.s.m. de Politieacademie en de Open Universiteit, de rol van encryptie in de opsporing. Vooralsnog is onduidelijk wat de precieze rol is van encryptie hierin. De uitkomsten van dat onderzoek kunnen helpen om verbeteringen door te voeren in politiewerk en landelijk beleid hieromtrent. Uw deelname is daarom zeer waardevol. Meer informatie over het onderzoek vindt u op [projectwebsite].

Waarom ontvangt u deze uitnodiging?
De afdeling Onderzoekscoördinatie van de Nationale Politie heeft een steekproef getrokken van politiecollega's uit de opsporing. U bent in die selectie naar voren gekomen.

Hoe kunt u meewerken?
Ik nodig u uit om eenmalig een online vragenlijst in te vullen. Dat duurt ongeveer vijftien minuten. De vragenlijst bestaat uit een aantal meerkeuzevragen en enkele open vragen die gaan over uw ervaringen met encryptie in de opsporing.

Zo komt u bij de vragenlijst:
1. [URL vragenlijst]
2. U komt vervolgens op het beginscherm waar om uw toestemming wordt gevraagd.
3. Na het geven van toestemming kunt u beginnen met het invullen van de vragenlijst.

Vertrouwelijkheid van uw gegevens
Uw anonieme e-mailadres is alleen gebruikt voor deze uitnodiging. Het invullen van de vragenlijst is volledig anoniem en u hoeft geen gegevens in te vullen die naar u te herleiden zijn.

Deelname
U beslist zelf of u meedoet aan het onderzoek; deelname is vrijwillig. Ik waardeer het enorm als u meedoet. Hoe meer deelnemers, hoe beter wij een beeld krijgen rondom de geschetste problematiek en hoe beter de politie haar werk kan doen.

Ten slotte
Heeft u vragen over het onderzoek, uw privacy of zijn er problemen bij het bereiken of invullen van de vragenlijst? Neem dan contact op met het onderzoeksteam van NHL Stenden Hogeschool via [e-mailadres onderzoeksteam]. Het team is op werkdagen tussen 9.00 en 17.00 uur bereikbaar.

Alvast hartelijk dank voor uw deelname.

Met vriendelijke groet, namens het onderzoeksteam,

Jurjen Jansen
Lector digitale weerbaarheid

Bijlage V: Vragenlijst

Consent

Bedankt voor uw interesse in dit onderzoek. Dit onderzoek is bedoeld voor operationeel specialisten A, B en C. Nadat u het onderstaande toestemmingsformulier heeft gelezen, klikt u op 'Ik ga akkoord' als u wilt deelnemen.

Doel van het onderzoek

Dit onderzoek wordt uitgevoerd in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) door de onderzoeksgroep Cybersafety van NHL Stenden Hogeschool, in samenwerking met de Politieacademie en de Open Universiteit. Het doel van dit onderzoek is om beter te begrijpen wat de rol is van encryptie in de opsporing. Uw antwoorden zijn daarbij van groot belang.

Invullen vragenlijst

Het invullen van deze vragenlijst duurt ongeveer 15 minuten. De vragenlijst bestaat uit meerkeuzevragen en enkele open vragen.

Uw rechten

U mag op elk moment stoppen met het invullen van de vragenlijst. Uw beslissing over deelname heeft geen nadelige gevolgen.

Risico's en voordelen van deelname

In dit onderzoek wordt uw mening gevraagd over de rol van encryptie in de opsporing. Voor zover ingeschat kan worden door de onderzoekers brengt het invullen van de vragenlijst geen fysiek of emotioneel risico met zich mee. Uw deelname aan dit onderzoek draagt bij aan een beter begrip van hoe politiemensen denken over de rol van encryptie in de opsporing en wat de (praktische) gevolgen – positief dan wel negatief – zijn van encryptie op opsporingsonderzoeken. Met deze inzichten kunnen verbeteringen worden doorgevoerd in politiewerk en landelijk beleid.

Vertrouwelijkheid en privacy van uw gegevens

Deelname is anoniem. In de vragenlijst worden geen tot de persoon herleidbare gegevens gevraagd. Mocht persoonlijk identificeerbare informatie worden verstrekt in uw antwoorden, dan verwijderen de onderzoekers deze gegevens, zodat uw antwoorden op geen enkele manier aan uw naam of identiteit kunnen worden gekoppeld.

De vragenlijstresultaten worden uitsluitend gebruikt voor wetenschappelijke publicaties. De uitkomsten worden gepresenteerd in een eindrapport dat door het WODC wordt gepubliceerd. De geanonimiseerde vragenlijstdata kunnen na oplevering van het eindrapport worden gedeeld met andere onderzoekers voor secundaire analyse of worden gebruikt in ander onderzoek zonder aanvullende geïnformeerde toestemming van u. De onderzoeksgegevens worden minimaal tien jaar bewaard door de onderzoeksgroep Cybersafety en het WODC nadat alle analyses en publicaties met betrekking tot dit onderzoek zijn voltooid. De gegevens worden opgeslagen in een beveiligde online omgeving.

Contactgegevens voor vragen

Als u vragen of opmerkingen heeft over uw rol en rechten als deelnemer, informatie wilt verkrijgen over het onderzoek, input wilt leveren, of een klacht over dit onderzoek wilt indienen, dan kunt u contact opnemen met dr. Jurjen Jansen. Hij is verantwoordelijk voor dit onderzoek. Dit kan via e-mail: [e-mailadres].

Toestemming om deel te nemen

Uw deelname aan dit onderzoek is geheel vrijwillig. Door hieronder op 'Ik ga akkoord' te klikken, gaat u akkoord met deelname.

0. Ik heb bovenstaande informatie gelezen. Ik begrijp dat mijn deelname volledig vrijwillig is en dat ik mijn deelname op elk moment kan beëindigen. Door hieronder op 'Ik ga akkoord' te klikken, ga ik akkoord met deelname aan dit onderzoek.
   □ Ik ga akkoord (naar vragenlijst)
   □ Ik ga niet akkoord (naar exit pagina)

Vragenlijst

Achtergrondkenmerken

1. Op welk niveau bent u werkzaam bij de politie?

O	Landelijk
O	Regionaal (eenheidsbreed)
O	Districtelijk
O	Anders, namelijk:

2. Wat is uw functie?

O	Operationeel Specialist A
O	Operationeel Specialist B
O	Operationeel Specialist C
O	Anders, namelijk:

3. Wat typeert uw huidige werkzaamheden het best?

O	Forensisch onderzoek
O	Tactisch onderzoek
O	Digitaal onderzoek
O	Technisch onderzoek
O	Financieel onderzoek
O	Anders, namelijk:

4. Hoe lang bent u werkzaam in de opsporing?

O	0 tot 2 jaar
O	2 tot 5 jaar
O	5 tot 10 jaar
O	10 tot 25 jaar
O	25 jaar of meer

5. Hoeveel affiniteit heeft u met digitalisering in politiewerk (denk aan cybercrime, gedigitaliseerde criminaliteit, digitaal sporenonderzoek)?

O	Heel weinig
O	Weinig
O	Niet weinig, maar ook niet veel

O	Veel
O	Heel veel

6. Heeft u een opleiding of cursus gevolgd op het gebied van cybercrime en/of digitale criminaliteit? (meerdere antwoorden mogelijk)

O	Ja, op het gebied van cybercrime
O	Ja, op het gebied van gedigitaliseerde criminaliteit
O	Ja, op het gebied van IT
O	Anders, namelijk
O	Nee

Rol encryptie in opsporingsonderzoeken

De volgende vragen gaan over encryptie oftewel de versleuteling van gegevens, en de rol die dat speelt in de opsporing. Encryptie is een middel om bijvoorbeeld opgeslagen informatie of internetverkeer te beveiligen. Encryptie-tools stellen gebruikers van digitale apparaten in staat om hun informatie en communicatie af te schermen voor derden.

7. In hoeverre heeft uw team in de afgelopen vijf jaar te maken gehad met opsporingsonderzoeken waarin encryptie een rol speelde? (Bijv. pincode op de telefoon, versleutelde WhatsApp communicatie, gebruik van cryptotelefoon, of versleutelde harde schijf)

O	Uitsluitend met dergelijke zaken te maken gehad
O	Veel mee te maken gehad
O	Niet veel, maar ook niet weinig mee te maken gehad
O	Weinig mee te maken gehad
O	Nooit mee te maken gehad (einde vragenlijst)

**Einde vragenlijst: Dit is het einde van de vragenlijst. We onderzoeken de rol van encryptie in opsporingsonderzoeken en u geeft aan hier niet mee te maken hebben gehad. Hartelijk bedankt voor uw interesse en deelname aan het onderzoek.*

U heeft aangeven dat uw team in opsporingsonderzoeken te maken heeft gehad met encryptie. De volgende vragen gaan hierover.

8. Met welke soorten opsporingsonderzoeken heeft uw team in het dagelijks werk te maken? (Let op: encryptie hoeft geen rol te spelen) (meerdere antwoorden mogelijk)

	Delict
□	Levensdelicten (zoals doodslag en (poging tot) moord)
□	Geweldsdelicten (zoals mishandeling, bedreiging en stalking)
□	Kinderporno
□	Seksuele misdrijven / zeden
□	Vermogensdelicten (zoals diefstal, inbraak en fraude/bedrog)
□	Vandalisme / vernieling
□	Cybercrime (IT zowel doel als middel, zoals hacken en DDoS-aanval)
□	Gedigitaliseerde criminaliteit (IT slechts als middel, zoals online oplichting)
□	Wapendelicten (zoals wapenbezit en -handel)
□	Verkeersdelicten (zoals verlaten plaats ongeval en rijden onder invloed)
□	Drugsmisdrijven

□	Milieucriminaliteit
□	Georganiseerde criminaliteit

9. Hoe vaak speelt encryptie een rol in onderstaande opsporingsonderzoeken waarmee uw team te maken heeft?

Delict	Niet	Weinig	Niet weinig / niet veel	Veel	Altijd
*Alle delicten uit vraag 8 die met ja zijn beantwoord	O	O	O	O	O

10. In hoeveel procent van de onderstaande typen opsporingsonderzoeken die door uw team worden uitgevoerd speelt encryptie volgens u een rol?

Type	0 tot 25% van de gevallen	25 tot 50% van de gevallen	50 tot 75% van de gevallen	75 tot 100% van de gevallen	Weet niet	Ons team houdt zich hier niet mee bezig
Veelvoorkomende criminaliteit (VVC, zoals inbraak, diefstal, vandalisme en bedreiging)	O	O	O	O	O	O
High impact crime (HIC)	O	O	O	O	O	O
Ondermijning	O	O	O	O	O	O

11. Hoe vaak schat u in dat het gemiddeld genomen binnen een opsporingsonderzoek lukt om toegang te krijgen tot **versleutelde communicatie**? (bijv. door het kraken of omzeilen van encryptie)

O	0 tot 24% van de gevallen
O	25 tot 49% van de gevallen
O	50 tot 74% van de gevallen
O	75 tot 100% van de gevallen
O	Weet niet / niet van toepassing

12. Hoe vaak schat u in dat het gemiddeld genomen binnen een opsporingsonderzoek lukt om toegang te krijgen tot **versleutelde data** (bijv. bestanden), anders dan communicatie? (bijv. door het kraken of omzeilen van encryptie)

O	0 tot 24% van de gevallen
O	25 tot 49% van de gevallen
O	50 tot 74% van de gevallen
O	75 tot 100% van de gevallen
O	Weet niet / niet van toepassing

13. Op welke wijze wordt geprobeerd toegang te krijgen tot versleutelde data/communicatie die in opsporingsonderzoeken een rol spelen?

	Niet	Weinig	Niet weinig / niet veel	Veel	Altijd	Weet niet
Via uitbesteding aan een andere politieafdeling of partij (bijv. NFI)	O	O	O	O	O	O
Door encryptie technisch te kraken (bruteforce)	O	O	O	O	O	O
Door encryptie te omzeilen (bijv. de sleutel vinden of raden)	O	O	O	O	O	O
Door alternatieve opsporingsmiddelen in te zetten (bijv. verhoren, observeren, huiszoekingen)	O	O	O	O	O	O
Door een aanhouding met open devices (zodat encryptie geen rol meer speelt)	O	O	O	O	O	O
Door een meewerkende verdachte (die bijv. de sleutel vrijwillig afgeeft)	O	O	O	O	O	O
Middels het decryptiebevel (art. 126nh lid 1 Sv)	O	O	O	O	O	O
Middels de 'terughackwet' (art. 126nba)	O	O	O	O	O	O
Anders, namelijk:	O	O	O	O	O	O

14. Met welke toepassingen van encryptie heeft uw team te maken in opsporingsonderzoeken?

Toepassing encryptie	Niet	Weinig	Niet weinig / niet veel	Veel	Altijd	Weet niet / ken ik niet
Versleutelde communicatie (end-to-end-encryptie)						
Crypto-telefoons (bijv. Ennetcom, EncroChat)	O	O	O	O	O	O
Versleutelde berichtendiensten (bijv. Sky ECC, PGP)	O	O	O	O	O	O
Versleutelde maildiensten (bijv. ProtonMail)	O	O	O	O	O	O
Versleutelde chatdiensten (bijv. Telegram, Signal, WhatsApp)	O	O	O	O	O	O
Versleutelde hardware en data						
Gelockte mobiele telefoons (bijv. met pincode, gezichtsherkenning)	O	O	O	O	O	O
Gelockte devices, anders dan mobiele telefoons (bijv. laptop en desktop computers)	O	O	O	O	O	O
Versleutelde gegevensdragers (bijv. usb-sticks, harde schijf)	O	O	O	O	O	O
Cryptocontainers (versleutelde data, bijv. met VeraCrypt, BitLocker)	O	O	O	O	O	O
Versleutelde onlinediensten						
Versleutelde cloudopslag	O	O	O	O	O	O
Bulletproof hosting	O	O	O	O	O	O
Sociale media (bijv. wachtwoordbeveiliging)	O	O	O	O	O	O
Tools voor verhullen digitale locaties (IP-adres)						
VPN	O	O	O	O	O	O
Tor	O	O	O	O	O	O

15. Welke toepassingen van encryptie die in de vorige vraag niet zijn benoemd komt u nog meer tegen in opsporingsonderzoeken?
[open invoerveld] (*niet verplicht)

16. In hoeverre is de frequentie van encryptie in opsporingsonderzoeken veranderd in uw team in de afgelopen vijf jaar?

O	De frequentie van encryptie is afgenomen
O	De frequentie van encryptie is (vrijwel) hetzelfde gebleven
O	De frequentie van encryptie is toegenomen
O	Weet niet / niet van toepassing

17. Welke criteria zijn volgens u het meest van belang in de keuze om een opsporingsonderzoek waarin encryptie een rol speelt voort te zetten? (kies maximaal 3)

□	Prioriteit van de zaak / het misdrijf
□	Beschikbare capaciteit
□	Benodigde expertise
□	Hoeveel tijd het ontsleutelen of omzeilen van de encryptie vermoedelijk kost
□	Kans van slagen om toegang te krijgen tot data achter encryptie
□	(Toekomstige) schade voorkomen
□	Geen andere optie om tot bewijs te komen
□	Anders, namelijk:

18. Hoe vaak schat u in dat uw team een opsporingsonderzoek succesvol kan afronden in het geval de encryptie van een potentieel bewijsstuk niet is te kraken of omzeilen (bijv. omdat andere bewijslast voldoende is)?

O	0 tot 24% van de gevallen
O	25 tot 49% van de gevallen
O	50 tot 74% van de gevallen
O	75 tot 100% van de gevallen
O	Weet niet / niet van toepassing

19. In hoeverre speelt encryptie volgens u een belemmerende rol in de voortgang van opsporingsonderzoeken op onderstaande gebieden?

	Niet	Weinig	Niet weinig / niet veel	Veel	Altijd	Weet niet
Het verkrijgen van communicatie/data	O	O	O	O	O	O
Het onderscheppen van communicatie/data (tappen)	O	O	O	O	O	O
Het verkrijgen van toegang tot data, anders dan communicatiedata	O	O	O	O	O	O
De mogelijkheden om criminele activiteiten vast te stellen	O	O	O	O	O	O
De kans om relevante personen te identificeren	O	O	O	O	O	O
De kans op relevante personen te lokaliseren	O	O	O	O	O	O

De mogelijkheden om criminele samenwerkingsverbanden vast te stellen	O	O	O	O	O	O
De kans om relevante goederen te identificeren	O	O	O	O	O	O
De kans op relevante goederen te lokaliseren	O	O	O	O	O	O
De mogelijkheden om relaties tussen personen, goederen en locaties vast te stellen	O	O	O	O	O	O
De mogelijkheden om bewijsmateriaal te vergaren	O	O	O	O	O	O

20. Welke rol speelt encryptie volgens u in opsporingsonderzoeken op de volgende terreinen?

	Negatief	Voor-namelijk negatief	Niet positief, maar ook niet negatief	Voor-namelijk positief	Positief	Weet niet
De kans om een opsporingsonderzoek voort te zetten	O	O	O	O	O	O
De doorlooptijd van een opsporingsonderzoek	O	O	O	O	O	O
De inzet van mensen (capaciteit)	O	O	O	O	O	O
De inzet van middelen	O	O	O	O	O	O
De betrouwbaarheid van gevonden data na ontsleuteling	O	O	O	O	O	O
De kans om een zaak succesvol af te ronden	O	O	O	O	O	O
De kans op het vinden van aanknopingspunten voor nieuwe zaken (restinformatie) na ontsleuteling	O	O	O	O	O	O
De mogelijkheden om verdachten aan te dragen bij het OM	O	O	O	O	O	O

21. Als u kijkt naar de rol van encryptie in opsporingsonderzoeken in zijn algemeenheid, hoe zou u die rol dan willen duiden?

O	Positief
O	Voornamelijk positief
O	Niet positief, maar ook niet negatief
O	Voornamelijk negatief
O	Negatief

22. Wilt u uw bovenstaande antwoord kort toelichten?
    [open invoerveld] (*niet verplicht)

23. Tot slot, zijn er nog onderwerpen of gedachten die u met de onderzoekers wilt delen aangaande de rol van encryptie in het opsporingsproces? Zo ja, dan kunt u die hier kwijt.
    [open invoerveld] (*niet verplicht)

Afsluiting

Dit is het einde van de vragenlijst. Hartelijk dank voor uw deelname!

Bijlage VI: Pearson correlatietabellen

In deze bijlage zijn de correlatietabellen gepresenteerd die horen bij hoofdstuk 4.

Tabel VI.1: Correlatietabel (Spearman) van type delict en in hoeverre men met toepassingen te maken heeft in opsporingsonderzoeken (N=177)

Type delict **Toepassing encryptie**	Drugs-misdr.	Georg. crim.	Levens-delicten	Wapen-delicten	Gewelds-delicten	Vermogens-delicten	Gedig. crim.	Cyber-crime	Seks. misdr. / zeden	Kinder-porno	Vanda-lisme / vern.	Milieu-crim.	Verkeers-delicten
Versleutelde communicatie (end-to-end-encryptie)													
Crypto-telefoons (bijv. Ennetcom, EncroChat)	.30**	.40**	.05	.28**	.18	-.03	-.08	-.11	-.29**	-.19*	-.14	-.05	-.09
Versleutelde berichtendiensten (bijv. Sky ECC, PGP)	.25**	.35**	.02	.22**	-.15	-.06	-.07	-.12	-.33**	-.20**	-.18*	-.09	-.14
Versleutelde maildiensten (bijv. ProtonMail)	-.06	.12	.09	.06	.04	.15*	.08	.21	-.11	.06	.04	.01	.02
Versleutelde chatdiensten (bijv. Telegram, Signal, WhatsApp)	.00	.11	.10	.10	.03	.04	.04	-.04	.06	.02	-.06	.08	.10
Versl. hardware en data													
versleutelde mobiele telefoons (bijv. met pincode, gezichtsherk.)	-.09	.08	.08	.03	.05	.04	.00	.02	.10	.03	-.04	.07	.13
Versleutelde devices, anders dan mobiele telefoons (bijv. laptop en desktop computers)	-.02	.03	-.03	-.01	-.05	.10	.05	.12	-.10	.01	-.04	.03	-.01
Versleutelde gegevensdragers (bijv. usb-sticks, harde schijf)	-.09	-.01	-.08	-.07	-.04	.09	.09	.14	.03	.19*	-.05	.09	-.02
Cryptocontainers (versleutelde data, bijv. met VeraCrypt, BitLocker)	-.09	.10	-.05	.00	-.01	.19*	.12	.15*	.05	.21	.05	.23**	.03

*Noot. *p < .05, **p < .01; Type delict (ja/nee); Toepassing encryptie (1=niet, 5=altijd).*

Tabel VI.1 (vervolg): Correlatietabel (Spearman) van type delict en in hoeverre men met toepassingen te maken heeft in opsporingsonderzoeken (N=177)

Type delict **Toepassing encryptie**	Drugs-misdr.	Georg. crim.	Levens-delicten	Wapen-delicten	Gewelds-delicten	Vermogens-delicten	Gedig. crim.	Cyber-crime	Seks. misdr. / zeden	Kinder-porno	Vanda-lisme / vern.	Milieu-crim.	Verkeers-delicten
Versleutelde onlinediensten													
Versleutelde cloudopslag	-.17*	.10	.11	.02	.05	.13	.01	.02	.00	.06	.05	.12	.02
Bulletproof hosting	-.02	.12	.11	.07	.02	.07	-.10	-.09	-.02	-.07	.03	.11	-.05
Sociale media (bijv. wachtwoordbeveiliging)	-.15*	-.07	.01	-.01	.05	.02	-.01	-.03	.07	.03	.04	.13	.02
Tools voor verhullen digitale locaties (IP-adres)													
VPN	-.09	-.01	-.17*	-.05	-.01	.07	.04	.01	.04	.07	-.02	.08	-.01
Tor	-.09	-.04	-.08	-.03	.00	.07	.00	-.03	.09	.10	-.06	.15	-.02

*Noot. *p < .05, **p < .01; Type delict (ja/nee); Toepassing encryptie (1=niet, 5=altijd).*

Tabel VI.2: Correlatietabel (Spearman) tussen type delict en het succesvol verkrijgen van toegang tot data en communicatie (N=169)

Delict	Drugs-misdr.	Georg. crim.	Levens-delicten	Wapen-delicten	Gewelds-delicten	Vermogens-delicten	Gedig. crim.	Cyber-crime	Seks. misdr. / zeden	Kinder-porno	Vanda-lisme / vern.	Milieu-crim.	Verkeers-delicten
Succesvolle toegang tot communicatie en data	.06	.16*	-.01	-.07	.07	.09	.17*	.25**	.08	.10	.14	.10	.11

*Noot. *p < .05, **p < .01; Type criminaliteit (ja/nee); Succesvolle toegang tot communicatie data (1=in 0-25% van de gevallen, 4=in 75-100% gevallen).*

Tabel VI.3: Spearman correlaties tussen het meewerken van de verdachte en het type delict waar men dagelijks mee te maken heeft (N=177)

Type delict	Drugs-misdr.	Georg. crim.	Levens-delicten	Wapen-delicten	Gewelds-delicten	Vermogens-delicten	Gedig. crim.	Cyber-crime	Seks. misdr. / zeden	Kinder-porno	Vanda-lisme / vern.	Milieu-crim.	Verkeers-delicten
Meewerken verdachte	-.03	-.10	.09	.10	.22**	.12	.11	.10	.11	.11	.17*	.15*	-.02

*Noot. *p < .05, **p < .01; Type criminaliteit (ja/nee); Meewerken verdachte (1=niet, 5=altijd).*

Tabel VI.4: Spearman correlaties tussen de duiding van de rol van encryptie en het type delict waar men dagelijks mee te maken heeft (N=177)

Type delict	Drugs-misdr.	Georg. crim.	Levens-delicten	Wapen-delicten	Gewelds-delicten	Vermogens-delicten	Gedig. crim.	Cyber-crime	Seks. misdr. / zeden	Kinder-porno	Vanda-lisme / vern.	Milieu-crim.	Verkeers-delicten
Duiding rol encryptie	-.05	.10	.00	.02	.06	.03	.16*	.12	.11	.13	.02	.11	.06

*Noot. *p < .05, **p < .01; Type delict (ja/nee); Duiding rol encryptie (1=positief, 5=negatief).*

Bijlage VII: Summary (in English)

Encryption is increasingly common in all forms of crime. There are broadly two reasons for this. First, encryption is commonly integrated in software and hardware and is therefore easily accessible to criminals. Second, the ability to hide relevant information and communications greatly facilitates criminal activity. Consequently, law enforcement increasingly encounters encryption in criminal investigations. This raises the question of what role encryption plays in these investigations, which is the focus of the current study.

Encryption poses a dilemma to policy makers and legislator. This dilemma can be seen, for example, in a resolution on encryption adopted by the European Council on 14 December 2020. On the one hand, encryption is considered crucial to protect the fundamental rights and digital safety and security of citizens, governments, businesses and society. On the other hand, encryption hampers law enforcement and judicial authorities in the exercise of their legal powers to protect society and citizens.

The Dutch Minister of Justice and Security supports this resolution and has requested the Dutch Research and Documentation Centre (WODC) to study the impact of encryption in criminal investigations. This study aims to provide insights to support the consideration of the dilemma of encryption. The researchers have chosen to discuss 'the role' of encryption, instead of talking about 'the impact' of encryption. The choice of the term role, which seems more neutral, was taken to prevent the impression that the current study is biased or prejudiced. The main research question that this study aims to answer is: What is the role of encryption in police investigations? This question is elaborated in three sub-questions: (i) What is the nature of encryption that is encountered in criminal investigations?; (ii) Does encryption affect the conduct of criminal investigations, and if so, how?; (iii) Does encryption affect the outcome of criminal investigations, and if so, how?

This is an exploratory study, as there is limited information available on this topic. To answer the main question and sub-questions, desk and field research have been carried out. Desk research consisted of a literature review, media analysis and an analysis of court decisions. In addition, sixteen exploratory interviews were held with nineteen professionals of the Dutch police, the Netherlands Public Prosecution Service and the Netherlands Forensic Institute. Based on their knowledge and experience, they were able to give an expert judgement on the subject. An online questionnaire was also administered to Dutch police employees, which was fully completed by 177 operational specialists (response rate 20%). Lastly, in-depth interviews were conducted with three Netherlands Public Prosecution Service staff and five staff members from the judiciary.

Sub-question 1: What is the nature of encryption in criminal investigations? First, the role of encryption in criminal investigations was examined. This study suggests that encryption is common in all type of crimes, but the extent to which it is common differs according to crime. The most significant factor affecting the significance of encryption to investigation may be the prevalence of seized mobile phones in criminal investigations, as mobile phones are usually protected by some form of encryption. Other significant forms of encryption include encrypted chat services, locked devices other than mobile phones (e.g., laptops), encrypted e-mail services and crypto phones. It is difficult to determine the extent to which encryption affects criminal investigations. However, interviewees perceive that encryption has become increasingly central to criminal investigations in the last few years, even though this cannot be substantiated by statistics. They acknowledge that the prevalence of this depends heavily on the type of crime.

When focusing on different categories of crime, encryption is most common in subversive crimes, and to a fairly large extent, in high-impact crimes. It is less prevalent in common crimes. When focusing on specific types of crime, encryption mostly plays a role in drugs offences, child pornography and cybercrime – both cyber-dependent and cyber-enabled crime. Furthermore, interviewees suggest that encryption plays a significant role in all types of organised crimes.

Some interviewees distinguish two types of encryption: technology-driven encryption, in which messages are automatically end-to-end encrypted (e.g., WhatsApp); and human-driven encryption which is used to deliberately encrypt information (e.g., crypto phones). Interviewees describe human-driven encryption as an indicator of crime. However, this impressionistic perception does not mean that this is always the case. After all, it is not prohibited by law to use crypto phones. Moreover, some individuals use encryption for their own safety, for instance journalists or individuals who want to protect trade secrets.

Sub-question 2: Does encryption play a role in the progress of criminal investigations, and if so, how? Encryption plays a role in the conduct of criminal investigations. One of the key factors is prioritisation. Cases get prioritized when it is in the interest of Dutch society. Another important factor to continue the investigation when encountering encryption is the perceived likelihood to gaining access to the encrypted data. However, how likely it objectively is to succeed and get access to encrypted data cannot be quantified.

To gain access to encrypted information, law enforcement agencies have roughly two options: bypassing encryption and cracking encryption. Both options may require a lot of capacity, but this is not always the case. Bypassing can take place by finding the encryption key, guessing the key, enforcing the key, exploiting a leak in the encryption software, gaining access to readable text when using the device, and by locating a copy of the readable text. Cracking encryption – or gaining access to a computer system using forensic tools – requires specialised software and hardware. Participants in the study mentioned that cracking is often outsourced to another party or department, such as the Netherlands Forensic Institute. In case of international cooperation, Europol may play a role. The success of cracking encryption depends on the cryptographic algorithm used and the key length. A general rule is that the longer the key is, the more difficult it is to crack it. Firmly quantifying the time required is not included in the scope of the current study.

When focusing on the use of investigative powers, the Netherlands Public Prosecution Service determines whether capacity and time of the police or the Netherlands Forensic Institute will be used to crack encrypted data. The investigation department has the decryption order (art. 126nh paragraph 1 of the code of criminal procedure) and hacking powers (art. 126nba, 126uba and 126zpa of the code of criminal procedure). However, little use is made of these powers since they may only be used under strict conditions. Furthermore, regarding mutual legal assistance, law enforcement agencies depend on, among other things, laws and regulations, whether requested data are delivered (on time) and whether they are useful for the investigation.

Encryption can also affect the duration of investigations. One outcome may be that due to encryption an investigation can be terminated, which happens when there is not enough evidence or when the encrypted data (presumably) cannot be decrypted. Nonetheless, even without cracking or circumventing encryption, a case is not immediately lost. Evidence can be gathered in other ways, which may still lead to a successful conviction.

Thus, encryption may create obstacles in criminal investigations. On the other hand, once encryption is circumvented or cracked, an investigation might accelerate. One respondent stated that after decryption, a case that traditionally would take months to a year can now be completed in a few weeks. It was also noted that encryption does not always have an obstructive influence, as suspects sometimes voluntary unlock their device. Finally, the learning capacity of Dutch police organisation and affiliated parties, such as the Netherlands Public Prosecution Service, the Netherlands Forensic Institute and the judiciary is constantly evolving. The increasing knowledge and experience of cracking and bypassing encryption, as well as the deploying alternative investigation strategies to complete the evidence, may reduce the processing time of cases in which encryption is present.

Sub question 3: Does encryption play a role in the outcome of criminal investigations, and if so, how? The role of encryption in the outcome of criminal investigations includes such issues as the extent to which encryption affects the identification and/or localisation of relevant persons and the successful discovery of evidence. In general, encryption hampers the identification and/or localisation of relevant persons and assets of collaborations or (criminally relevant) relations between persons, assets and locations, and the possibility of establishing (detecting) criminal activities. The main barrier is the reduction of direct access to evidence. Also, unencrypted and retrieved data differ in their investigative utility. Lastly, retrieved data regularly arrive late, not at all or are not usable.

Although it is not clear what kind of data – and thus evidence – is missing, respondents mention that not being able to circumvent or crack encryption does not always lead to termination of an investigation. In cases where it is not successful, alternatives can be used to still gather the evidence needed in a case. Think for example about the significance and use of metadata in investigations. Although encryption may have made it more difficult and challenging, law enforcement agencies still often succeed. For example, interviewees and respondents indicate that there is a relatively high success rate in retrieving information from devices and applications with technology-driven encryption (by default). Human-driven encryption (consciously applied), on the other hand, seems to be more difficult to circumvent or crack. However, we cannot substantiate this with statistics.

In addition, decrypted data is highly valued. It is generally seen as more reliable than (witness) statements. According to interviewees, this information is less likely to have been altered by third parties. The open communication of suspects – who feel safe behind encryption – is valuable. Interviewees also indicate that decryption is beneficial to create an idea of criminal collaborations, as this is more complete than the global and fragmentary ideas of the situation before and/or without encryption. Moreover, when access is gained to encrypted data (the decryption phase), there is potentially a wealth of information, which could be beneficial for the investigation.

Main question: What is the role of encryption in criminal investigations? This study shows that encryption plays a prominent role in criminal investigations. This role works both ways. On the one hand, encryption plays an obstructing role for criminal investigations, but on the other hand it also plays a practical role in improving the investigations.

Overall, it can be concluded that it is, however, not easy to quantify the challenge. It cannot be determined how many cases are not solved or how much time is lost because of encryption. By the same token, it is also not possible to determine how many additional cases are solved or how much time is gained. Criminal investigation is too complex by the entirety of facts, coincidences, circumstances and trade-offs for that. This study provides a nuanced image of what the use of

encryption – consciously or unconsciously – means for criminal investigations. There are negative sides to the use of encryption, but positive aspects can also be identified.

When encryption is being examined, the process of encryption is not the only thing that needs to be considered. A holistic view is needed to get to the core of the 'problem' of encryption. This has been done by deliberately including decryption in the study as well. The nuanced effect of encryption on criminal investigations was also reflected in the responses we received through the various methods that we applied. Interviewees accepted that new phenomena have to be dealt with and acted upon in novel ways. The so-called 'cat-and-mouse' game that occurs between police and criminals is thus seen as an opportunity for the police organisation to develop further.

It is therefore important to (continue to) invest in developing knowledge and skills regarding detection and digital aspects of police work, such as encryption. It is also important to keep track of future (technological) developments and what they mean for the role of criminal investigations. These include quantum computing, which was mentioned by participants in this study, as well as developments that are already underway, such as 5G and in the field of AI (artificial intelligence).

To conclude. This study is about the role of encryption in criminal investigations. What we would like to convey here is the practical and often contradictory effects of encryption on criminal investigations, and the follow-up question of whether it should then be treated differently from the way it currently is.

After all, the police have always been dealing with crucial crime information stored in a memory to which they do not have direct access. We call that memory the human brain. Since the police cannot read that (they do not have a key) and the criminal may choose to remain silent, police have to think of all kinds of ways to bypass that security and/or get the key and/or trick someone into revealing the information. Now we have a computer that, like the criminal, says: you will not get in and I will not say anything. Then, as police, you must think of alternatives to deal with that. The police have always done that. So, what is really different now?

The tendency may be to compare the current situation – where encryption is thus a daily occurrence – with the situation where digital information was not yet encrypted. The question behind this is what standard is being followed. We can argue that compared to five, ten or fifteen years ago, the current conditions are more difficult for the police. We can also argue that by contrast, armed with decryption power, the police have gained extra access to information that is potentially much greater than before. Ultimately, digitalisation requires moving with and adapting to what comes our way. Therein lies the constant challenge.