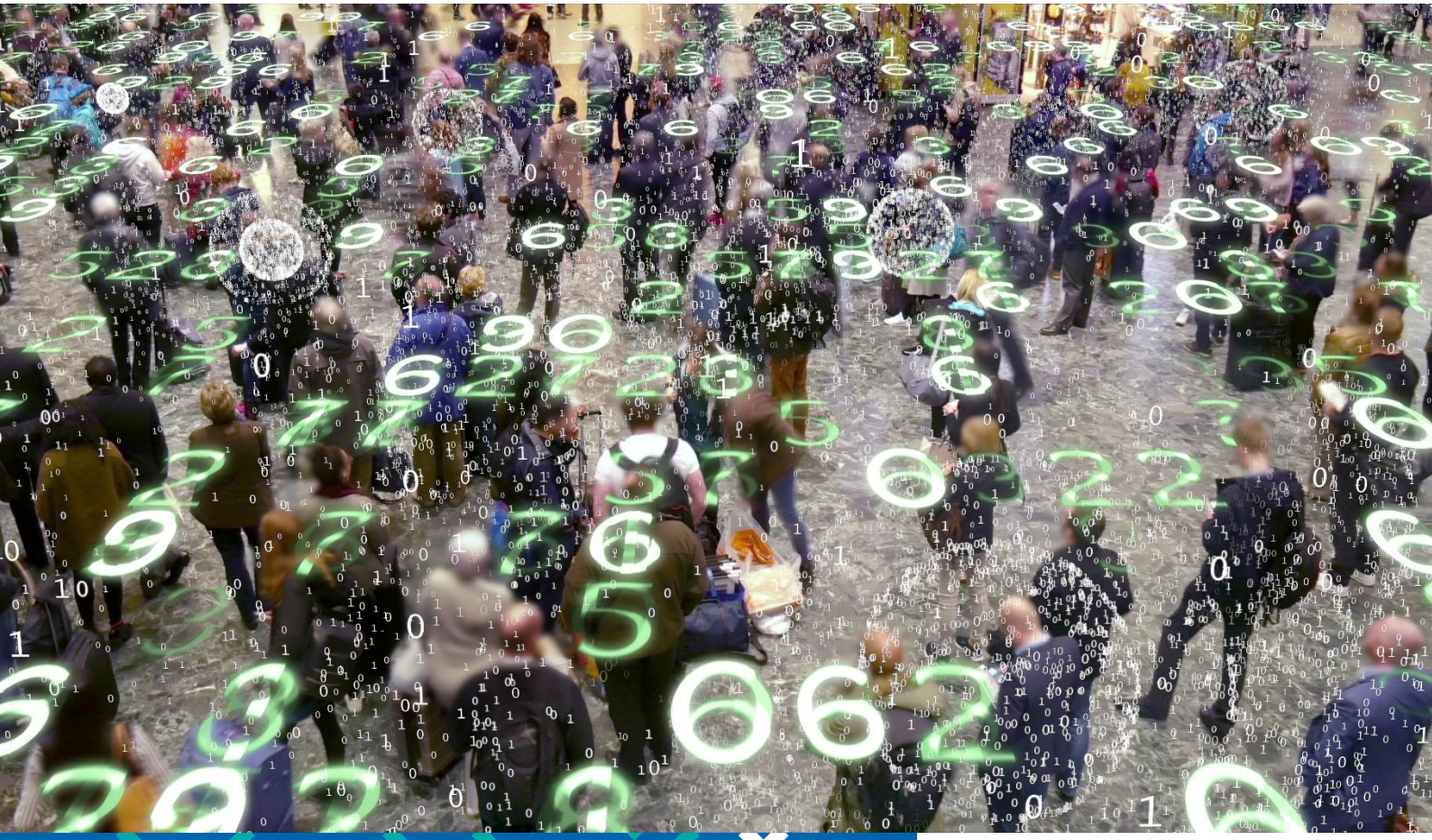
De rol van encryptie in de opsporing

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.