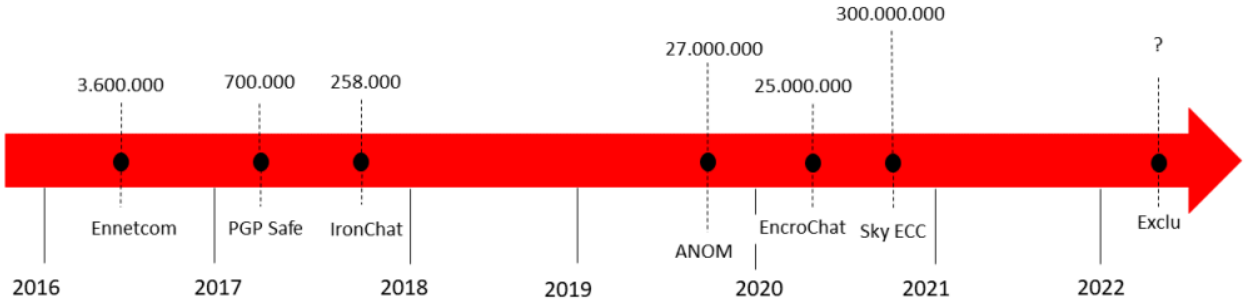
Overzicht cryptophone-operaties

8-11 minutes ⋮ 11/14/2022

Ongeveer vier jaar geleden, in november 2018, verscheen het eerste persbericht op OM.nl over het veiligstellen van berichten die zijn verstuurd met ‘cryptotelefoons’ (ook wel ‘PGP-telefoons’ genoemd).

De beschikbare informatie over cryptotelefoons heb ik in de volgende tijdlijn en blogberichten hieronder op een rijtje gezet:



1. Ennetcom (2016)
2. PGP Safe (2017)
3. Ironchat (2017)
4. EncroChat (2020)
5. Sky ECC (2020)
6. ANOM (2021)
7. Exclu (2022)

(*Dit overzicht van 30 december 2021 is geüpdatet op 19 november 2023).*

Waarom een overzicht?

De operaties zijn blijkbaar bijzonder belangrijk voor de strafrechtpraktijk en toch is er relatief weinig bekend over de operaties. Op 15 september 2022 zijn er al meer dan 400 uitspraken beschikbaar op rechtspraak.nl, waarin bewijs uit de cryptotelefoons een belangrijke rol speelt. In de media worden de cryptophone-berichten ook wel een ‘goudmijn aan bewijs’ genoemd en de gegevens vormen een *game changer* voor de politie. Strafrechtadvocaten trekken vaak de rechtmatigheid van de operaties in twijfel, maar vooralsnog lijkt de verdediging bot te vangen. Op 13 april 2023 maakte de Landelijke Eenheid ook bekend dat de politie inmiddels *1 miljard* “criminele chats” in handen heeft. De initiële cijfers

uit de persberichten die in de tijdlijn hierboven staan kloppen dus opgeteld niet met dit “eindcijfers”.

Duidelijk is wel dat dit om “bulkdata” gaat en dit de brandstof levert voor de nieuwe strategie van “datagedreven opsporing” van de politie en het Openbaar Ministerie.

De grote hoeveelheid jurisprudentie en onduidelijkheid over de ‘wat’, ‘wanneer’ en ‘hoe’-vragen vormde voor mij aanleiding een overzicht te maken (ook voor mijzelf voor toekomstige publicaties). Daarbij heb ik mij gebaseerd op persberichten van het OM, de politie en rechtspraak.

Wat en wanneer

1. Ennetcom (2016)

Leverancier van cryptotelefoons met apps op een Blackberry telefoon. Oprichters van het bedrijf zijn uiteindelijk veroordeeld voor deelname aan een criminele organisatie, gewoontewitwassen en medeplegen van valsheid in geschrifte. Tijdens de operatie zijn 3,6 miljoen berichten veiliggesteld. De operatie werd bekend gemaakt op 9 maart 2017.

- PGP Safe (2017)

Leverancier van cryptotelefoons met apps op Android en Blackberry toestellen. Tijdens de operatie zijn 700.000 berichten veiliggesteld. De verdenking was aanvankelijk dat de verdachte zich tezamen met anderen als professionele *facilitator* van versleutelde communicatie schuldig zou hebben gemaakt aan overtreding van witwassen (art. 420bis Sr) en deelneming aan een criminele organisatie (art. 140 Sr). De verdachte wordt uiteindelijk alleen veroordeeld (ECLI:NL:RBROT:2022:363) voor valsheid in geschrifte en ‘begunstiging’. De operatie werd bekend gemaakt op 9 mei 2017.

- Ironchat (2017)

Leverancier van Wileyfox-telefoons met Ironchat-app er op. Onderzoek gericht op de oprichters van het bedrijf (verdenkingen nog onduidelijk). Tijdens de operatie zijn 258.000 berichten veiliggesteld. De operatie werd bekend op 6 november 2018.

- EncroChat (2020)

Leverancier van cryptotelefoons met EncroChat (en andere Encro) apps. Vermoeden dat Encro en de gebruikers zich in georganiseerd verband schuldig maakten aan o.a. witwassen en deelname aan criminele organisaties. Tijdens de operatie zijn 25 miljoen berichten veiliggesteld. De operatie werd bekend gemaakt op 2 juli 2020.

- Sky ECC (2020)

Leverancier van cryptotelefoons met Sky ECC app. Sky ECC en de daaraan gelieerde (natuurlijke) personen verdacht van deelname aan een criminele organisatie en (gewoonte)witwassen. Tijdens de operatie zijn honderden miljoenen berichten veiliggesteld. De operatie werd bekend gemaakt op 9 maart 2021.

- ANOM (2021)

ANOM was een zogenoemde 'store front', oftewel een zelf opgezette communicatiedienst. De operatie stond onder leiding van de FBI en de Australische Federal Police met het doel om verdachten van criminele organisaties te identificeren. Tijdens de operatie zijn 27 miljoen berichten onderschept. De operatie werd bekend gemaakt op 8 juni 2021.

- Exclu (2022)

Leverancier van cryptotelefoons met Exclu app(s) erop. Een onderzoek richt zich op de eigenaren en beheerders van de cryptocommunicatiedienst en een ander onderzoek richt zich zich op de gebruikers van Exclu van wie wordt vermoed dat zij in georganiseerd verband misdrijven plegen. De operatie werd op vrijdag 3 februari 2023 bekend gemaakt.

Hoe

1. Ennetcom (2016)

Via een rechtshulpverzoek aan Canada, met machtiging van een Canadese rechter. NL grondslag: 125i Sv. Canadese rechter verbond voorwaarden aan verstrekking en gebruik van gegevens aan Nederlandse opsporingsinstanties.

Zie ook: B.W. Schermer & J.J. Oerlemans, 'AI, strafrecht en het recht op een eerlijk proces', *Computerrecht* 2020/3 en Rb. Rotterdam 21 september 2021, ECLI:NL:RBROT:2021:9085, *TBS&H* 2022/2.8, m.nt. J.J. Oerlemans (*veroordeling oprichter Ennetcom*). (HR uitspraak: HR 28 juni 2022, ECLI:NL:HR:2022:900 en blog).

2. PGP Safe (2017)

Via een rechtshulpverzoek aan Costa Rica, met assistentie van Nederlandse politie. Machtiging voor bevel tot binnentreden, de doorzoeking en de beslaglegging afgegeven door het Gerecht in Strafzaken van het Eerste District San Jose. Aan de verstrekking van de veilig gestelde gegevens zijn geen beperkingen aan Nederland opgelegd.

3. Ironchat (2017)

Gegevensvergaring via een Europees Opsporingsbevel aan het Verenigd

Koninkrijk. Na eigen onderzoek vond verstrekking van een kopie van de server (een *image*) plaats. Grondslag strafvordering voor operatie vooralsnog onduidelijk.

4. EncroChat (2020)

Via JIT en EOB's. Franse autoriteiten verzamelden gegevens met inzet "interceptietool". Extra machtiging voor inzet hackbevoegdheid (126uba Sv) op verdachten met verdenking van betrokkenheid/beramen van het plegen van misdrijven in georganiseerd verband. Beperkingen en vereisten aan onderzoek opgelegd door Nederlandse rechter-commissaris in een machtiging voor het onderzoeken van gegevens van Nederlandse ingezetenen.

Zie ook: B.W. Schermer & J.J. Oerlemans, 'De EncroChat-jurisprudentie: teleurstelling voor advocaten, overwinning voor justitie?', *TBS&H* 2022/2.2.

5. Sky ECC (2020)

Via JIT. Franse autoriteiten vergaren gegevens met inzet "interceptietool". Door Nederlandse opsporingsambtenaren is technische expertise en/of bijstand geleverd met betrekking tot de ontwikkeling en plaatsing van de tool.

De in Frankrijk vergaarde informatie is aanvankelijk vrijwillig op basis van artikel 26 van het Cybercrimeverdrag gedeeld met het Nederlandse Openbaar Ministerie. Later zijn ook machtigingen Nederlandse rechter-commissaris verleend. De vorderingen en machtigingen zagen op de toepassing van de artikelen 126t lid 1 en 126t lid 6 Sv (onderzoek communicatie door middel van een geautomatiseerd werk bij georganiseerde criminaliteit) en later ook op aanvullende, ondersteunende vorderingen op de voet van artikel 126uba Sv (hackbevoegdheid bij verdenking betrokkenheid beramen/plegen misdrijven in georganiseerd verband).

De Hoge Raad beantwoordde op 13 juni 2023 in een arrest (ECLI:NL:HR:2023:913) prejudiciële vragen over EncroChat en SkyECC. Kortgezegd maakt de Hoge Raad (wederom) duidelijk dat het niet behoort tot de taak van de Nederlandse strafrechter om de rechtmatigheid van de uitvoer van het buitenlandse onderzoek te toetsen. Zie ook J.J. Oerlemans & B.W. Schermer, 'Antwoorden op prejudiciële vragen in de EncroChat- en SkyECC-zaken', NJB 2023/2244, afl. 31, p. 2610-2618.

6. ANOM (2021)

Door een 'spontane eenzijdige verstrekking van informatie zonder een voorafgaand verzoek van de Nederlandse opsporingsdiensten'.

De Nederlandse opsporingsdiensten zouden niet betrokken zijn geweest bij de *verkrijging* van de gegevens. Wel heeft de Nederlandse software ontwikkeld waarmee de berichten konden worden geanalyseerd en geduid. Deze software is

ook beschikbaar gesteld aan Europol, zodat deze dienst de gegevens kon analyseren en beschikbaar stellen aan andere landen.

7. Exclu (2022)

In Duitsland stond een server en die is veilig gesteld. Tijdens de operatie is ook de hackbevoegdheid in een opsporingsonderzoek naar de betrokkenheid naar misdrijven die worden gepleegd in georganiseerd verband. De rest van de feiten over de operatie zijn vooralsnog onduidelijk.

Previous Chapter Next Chapter