

Samenvatting

De cryptocontroverse. Een sleutelconflict in de informatiemaatschappij

Noordwijkerhout, augustus 1998 – In de informatiemaatschappij wordt informatie, en daarmee informatiebeveiliging, steeds belangrijker. Er is dan ook een toenemende behoefte aan cryptografie: programma's die gegevens beveiligen tegen onrechtmatige toegang. Aan de andere kant bestaat er een toenemende bezorgdheid dat misdadigers diezelfde cryptografie kunnen gebruiken om te ontsnappen aan de aandacht van de politie. Cryptografie levert dus een belangenconflict op: privacy en informatiebeveiliging tegenover opsporing. De discussie hierover is sterk gepolariseerd: privacy-groepen en justitie staan lijnrecht tegenover elkaar. Ziedaar de *cryptocontroverse*: één van de sleutelconflicten in de informatiemaatschappij.

Ik organiseer daarom een driedaagse conferentie over het Nederlandse cryptobeleid, die de vraag moet beantwoorden: "Hoe kan en moet de Nederlandse overheid het probleem aanpakken dat het gebruik van sterke cryptografie door misdadigers oplevert voor de opsporing, rekening houdend met de rechtmatige belangen om cryptografie in de informatiemaatschappij te gebruiken?" De conferentie wordt bijgewoond door representanten van relevante groeperingen uit de Nederlandse maatschappij die een belang hebben bij een rechtvaardig cryptobeleid: Annie, een doorsnee cryptogebruiker, Bob, een bedrijfsmatige cryptogebruiker, Paula, een politie-agente, en Vera, een verdachte (die vreest dat haar rechten als verdachte worden aangetast door een draconisch cryptobeleid). Zij moeten een cryptobeleid vaststellen dat de belangen van privacy en informatiebeveiliging verenigt met het belang van de opsporing.

Achtergrond

Om de congressgangers een rechtvaardige keuze te kunnen laten maken, heeft de organisatie (de Brabantse Universiteiten) een uitgebreid achtergrondstuk geschreven over het probleem en de context waarin dat moet worden gezien. De studie begint met een beschrijving van de informatiemaatschappij, die volgens Eurocommissaris Bangemann "de manier waarop wij leven en werken ingrijpend zal veranderen". Nu informatie in ons leven en werk steeds belangrijker wordt, ontstaat er een informatiemaatschappij waarin traditionele grenzen vervagen. De media en de marktsectoren convergeren, staatsmonopolies op telecommunicatie zijn afgeschaft, en elektronische handel stelt consumenten en bedrijven in staat om handel te drijven via andere tussenpersonen dan de detailhandel. Deze maatschappij is van nature wereldwijd, en de grenzen van staat en jurisdictie worden snel minder relevant naarmate het Internet een hogere vlucht neemt. Het is een maatschappij die voor een groot deel afhankelijk is van informatie, en daarom is er een cruciale behoefte aan informatiebeveiliging. De beschikbaarheid, vertrouwelijkheid en deugdelijkheid van informatie (de BVD van informatiebeveiliging) moeten worden gewaarborgd door een combinatie van fysieke, organisatorische, technische en juridische maatregelen.

Een van de voornaamste technieken voor informatiebeveiliging is cryptografie: systemen die met een wiskundig algoritme en een digitale sleutel gegevens vercijferen zodat alleen rechthebbenden deze kunnen ontsleutelen en lezen. Vooral de in de jaren '70 ontwikkelde asymmetrische of publieke-sleutelcryptografie heeft een uitgebreid scala aan grootschalige toepassingen van encryptie mogelijk gemaakt. (In publieke-sleutelcryptografie gebruikt men een sleutelpaar dat bestaat uit een openbare en een privésleutel. Door de openbare sleutel

wijd te verspreiden – waarvoor geen beveiligd kanaal nodig is – kan men met een willekeurig groot aantal mensen veilig communiceren.) Cryptografie wordt gebruikt voor de beveiliging van bijvoorbeeld telecommunicatie, persoonsgegevens, elektronische betaalsystemen, intellectuele-eigendomsrechten, gevoelige overheids- en bedrijfsinformatie en mensenrechten. Cryptografie kan ook misdaad voorkómen, zoals computercriminaliteit en bedrijfsspionage.

Een nadeel van cryptografie is echter dat misdadigers het kunnen gebruiken om aan de aandacht van telefoontappende en computerspeurende politie-agenten te ontsnappen. Onkraakbare crypto-systemen zijn makkelijk verkrijgbaar, en als misdadigers deze op de juiste manier gebruiken (dat wil zeggen, als ze zorgvuldig omgaan met hun wachtwoorden), dan kunnen zij veilig communiceren en belastende informatie veilig opslaan zonder dat de politie ook maar iets wijzer wordt. Cryptografie zal daarom de opsporing van misdaad bemoeilijken, in het bijzonder de opsporing van georganiseerde criminaliteit, bedrijfs-criminaliteit en computercriminaliteit. Momenteel is het probleem niet groot: in de weinige gevallen waarin de politie encryptie is tegengekomen, waren ze meestal in staat het te kraken of was er voldoende ander bewijsmateriaal om de zaak rond te krijgen. De algemene verwachting is evenwel dat cryptocrimineel gebruik sterk zal toenemen naarmate cryptografie wijdverspreid raakt en gebruikersvriendelijker wordt, vooral als het zal worden ingebouwd in computers en in de telecommunicatie-infrastructuur. Aangezien aftappen en computeronderzoek belangrijke opsporingsmethoden zijn (opsporingsambtenaren noemen aftappen een cruciaal opsporingsmiddel, ook al wordt wel eens getwijfeld aan de effectiviteit ervan), gaat er een wezenlijke bedreiging uit van cryptomisdadigers voor de rechtsorde. Er is derhalve een legitiem publiek belang om het (toekomstig) negatief effect van cryptografie voor de opsporing tegen te gaan. In Nederland kan dit probleem het best worden gezien in de context van de algehele herziening van opsporingsmethoden, die plaatsvindt als gevolg van de IRT-affaire.

Het probleem van cryptomisdadigers wordt in veel landen bestudeerd. Sommige landen hebben wetgeving uitgevaardigd (Frankrijk en Rusland hebben bijvoorbeeld sterke cryptografie zo goed als verboden, terwijl Nederland een bepaling heeft ingevoerd om mensen te bevelen te ontsleutelen – deze bepaling wordt mogelijk binnenkort uitgebreid om dit bevel ook aan verdachten te kunnen geven), en sommige landen (in het bijzonder het Verenigd Koninkrijk en de VS) hebben de uitdrukkelijk wens geuit om de toepassing van cryptografie te beperken tot systemen die een ingebouwde decryptiemogelijkheid voor de overheid hebben. De meeste landen weten echter niet wat ze moeten doen. De OESO heeft ‘richtlijnen’ voor cryptobeleid uitgevaardigd die in feite helemaal geen richting geven, en landen lijken naar elkaar te kijken om te zien wat de internationale tendens zal zijn. Tot zover het achtergrondstuk, dat eindigt met een nogal wanhopig: “er is een algehele impasse in het debat over de cryptocontroversie”.

Procedure

Om deze impasse te doorbreken zullen Annie, Bob, Paula en Vera moeten beslissen welke optie het beste het probleem kan aanpakken van misdadigers die cryptografie gebruiken. Aangezien dit probleem in wezen een belangenconflict is, volgt de agenda van de conferentie een procedure die is geïnspireerd door John Rawls’ *A Theory of Justice*; deze procedure zou moeten leiden tot een uitkomst die iedereen kan accepteren. Een bijzonder aspect van deze conferentie is dat de conferentiekamer is gehuld in een ‘sluier van onwetendheid’, die ervoor

zorgt dat de deelnemers niet weten welke positie ze zelf in werkelijkheid innemen in de maatschappij. Zodoende hebben zij wel alle relevante informatie tot hun beschikking, maar kunnen Paula, Annie, Vera en Bob zich niet laten leiden door hun persoonlijke voorkeuren of door de specifieke belangen van de groepering die zij vertegenwoordigen. Dit zorgt ervoor dat hun besluit onpartijdig is en daadwerkelijk de belangen met elkaar verzoent.

Het eerste agendapunt betreft het kiezen van een minst-bevoordeelde groep, dat wil zeggen de groep die het meest te verliezen heeft in het cryptodebat, waarbij alleen verliezen in fundamentele vrijheden meetellen, niet in materieel bezit. Het centrale uitgangspunt van het recht is immers om de zwakken tegen de sterken te beschermen: “het recht [kan] in zijn functie van normering van orde niet onpartijdig zijn: het zal aan de kant moeten staan van de machtelozen, van de onder gezag gestelden, van hen die het meest dreigen in verdrukking te komen.” [Peters] Als er geen optie is die op alle punten te prefereren valt boven de andere, is het perspectief van de minst bevoordeelde groep een goede methode om een beslissing te nemen die recht doet aan dit centrale uitgangspunt. De deelnemers zijn het erover eens dat in de Nederlandse context Annie de minst-bevoordeelde groep vertegenwoordigt: haar privacy, inclusief haar recht op vertrouwelijke communicatie, staat op het spel. Zij heeft meer te verliezen dan Paula, die – zelfs als telefoontaps zinloos worden – nog steeds diverse opsporingsmiddelen heeft om boeven te vangen, terwijl Vera’s rechten voldoende worden beschermd door het recht op een eerlijk proces, zoals dat is geïnterpreteerd door het Europese Hof (aangezien dit een Nederlandse conferentie is, moet zij het Europees verdrag tot bescherming van de rechten van de mens respecteren). En zakenman Bob heeft geen fundamentele vrijheden te verliezen. De zaak zal daarom worden beslist vanuit het perspectief van Annie, en de conferentie moet dus die uitkomst opleveren die het best te aanvaarden is voor de gezagsgetrouwe cryptogebruiker.

Vervolgens kiezen de conferentiedeelnemers een verzameling principes, aan de hand waarvan zij de opties om het cryptoprobleem aan te pakken kunnen beoordelen. Ze beschouwen vier fundamentele rechten als essentieel voor het cryptoprobleem:

- het recht op privacy (inclusief vertrouwelijke communicatie),
- het recht op een eerlijk proces,
- de rechtsorde (inclusief het recht om van misdaad gevrijwaard te blijven) en
- het recht op economische ontwikkeling.

Ook zullen de deelnemers rekening houden met de minder fundamentele maar niettemin wenselijke principes van uitvoerbaarheid, internationale verenigbaarheid en technologische duurzaamheid. Aangezien deze principes zullen botsen, definiëren de deelnemers ook een beslisregel: men kan alleen een inbreuk op een fundamenteel recht toestaan op grond van een ander fundamenteel recht, niet op grond van een wenselijk principe. En om te bepalen welk fundamenteel recht het meeste gewicht draagt, komen de deelnemers overeen dat zij bij gelijke omstandigheden een principe dat hoger op de lijst staat meer gewicht zullen toekennen.

Oplossingsrichtingen

Om de eerste dag te besluiten, discussiëren Bob, Paula, Vera en Annie welke opties geschikt zijn kunnen om het cryptoconflict aan te pakken. Ze verwerpen direct de non-optie van een cryptoverbod, aangezien dat het rechtmatig belang van cryptogebruik aantast en daarmee privacy en informatiebeveiliging sterk aantast, terwijl het in het geheel niet effectief is om

misdadigers van cryptografie af te houden. Met enkele breinstormen komen de volgende oplossingsrichtingen tevoorschijn.

- Stimuleer het gebruik van crypto-systemen die de opsporing niet hinderen, hetzij omdat ze alleen digitale handtekeningen en niet vertrouwelijkheid faciliteren, hetzij omdat ze BEDOTten (dat wil zeggen: Bevat Een Decryptiemogelijkheid voor Opsporings-Toegang).
- Beveel verdachten om te ontsleutelen en straf hen als ze dat weigeren, hetzij door hen te veroordelen voor de weigering medewerking te verlenen aan een decryptiegebod (dat zou een nieuwe strafbepaling zijn), hetzij door de decryptieweigering als bewijs te gebruiken in de hoofdzaak (wat zou neerkomen op een omkering van de bewijslast).

Deze eerste twee opties zijn in feite de enige die zeker stellen dat de politie toegang kan krijgen tot cryptosleutels om versleutelde informatie te ontcijferen. Als zou blijken dat deze opties beide onuitvoerbaar of onwenselijk zijn, zal de politie iets anders moeten verzinnen.

- Zoek elders. Men kan denken aan 'direct af luisteren' (met richtmicrofoons en af luisterapparaatjes), elektromagnetische straling van computerschermen onderscheppen (via TEMPEST), meer infiltreren, of kroongetuigen ten tonele voeren. Dit zijn alternatieve opsporingsmethoden om, ongehinderd door cryptografie, belastende informatie te verzamelen.
- Besluit om niets te doen (de nuloptie).

De tweede dag discussiëren Paula, Vera, Bob en Annie over de voor- en nadelen van de opties. Het stimuleren van de ontwikkeling van niet-vertrouwelijkheidscrypto maakt het probleem niet erger voor de politie, maar het doet ook niets aan het probleem van cryptocriminelen als zodanig. Daarom vinden ze dat uiteindelijk geen echte optie. Vervolgens bekijken ze BEDOT-cryptografie: systemen met een ingebouwd sleuteldepot- of sleutelherwinningsmechanisme, dat ervoor zorgt dat de politie automatisch toegang heeft tot de benodigde decryptiesleutels. De conferentiedeelnemers merken op dat deze technologie nog in de kinderschoenen staat en intrinsieke beveiligingsrisico's met zich meebrengt. Belangrijker nog is dat het niet effectief is om cryptocriminelen te vangen, omdat (slimmere) boeven geen systeem zullen gebruiken waarvan ze weten dat het hun BEDOT. De politie kan weliswaar profiteren van vrijwillig gebruik van gegevensherwinnings-technieken (*data recovery*) door het bedrijfsleven, maar de ontwikkeling van deze technologie moet aan de markt worden overgelaten.

Nu bekijken de conferentiegangers onder welke voorwaarden een decryptiegebod aan verdachten kan worden gegeven, met inachtneming van het *nemo tenetur*-beginsel (verdachten hoeven niet aan hun eigen veroordeling mee te werken) zoals het Europees Hof dat in de *Funke*- en *Saunders*-arresten heeft geïnterpreteerd. (Bob merkt terzijde op dat het gebod gemakkelijk aan niet-verdachten kan worden gegeven, en veelal ook aan bedrijfsmatige cryptogebruikers, zodat een decryptiegebod zonder meer in diverse gevallen kan worden gegeven.) Het beginsel is niet absoluut en de politie kan bevelen diskettes met privé sleutels uit te leveren, gegeven de *Saunders*-uitspraak dat afgifte kan worden bevolen van materiaal dat onafhankelijk van de wil van de verdachte bestaat. Of de politie ook een verdachte kan dwingen het wachtwoord te geven dat normaliter de sleutel beveiligd, is controversiëler. Als de politie er zo goed als zeker van is dat de verdachte in staat is te ontsleutelen (in VS-terminologie: als het een uitgemaakte zaak is dat de verdachte kan ontsleutelen), is een decryptiebevel juridisch aanvaardbaar. De kritieke vraag is evenwel hoe

men de naleving van een decryptiebevel kan afdwingen: de algemene straf voor een weigering mee te werken aan een ambtelijk bevel is drie maanden, en dat kan niet genoeg zijn om ernstige misdadigers ertoe aan te zetten te ontsleutelen (waarmee ze immers vele jaren gevangenisstraf zouden riskeren). Het strafbaarstellen van cryptogebruik ‘ter bevordering van een misdrijf’ is geen optie, omdat het niet de bewijsproblemen verlicht die het juist zou moeten oplossen. De twee belangrijkste handhavingsopties zijn daarom het strafbaarstellen van een decryptieweigering met een substantiële straf (zeg een paar jaar), en de bewijslast omkeren om de decryptieweigering te gebruiken als bewijs in de hoofdzaak (“als je dit niet wil ontsleutelen, nemen we aan dat het belastende informatie bevat”). Aangezien de eerste optie misdadigers om de verkeerde reden aanpakt (men wil wetsovertreders straffen voor de misdaad die ze hebben begaan, niet voor ‘misbruik van cryptografie’), en omdat de tweede optie beter is toegespitst op ernstige misdadigers, zou de omkering van de bewijslast beter zijn om een decryptiegebod af te dwingen. Daarbij moeten echter strenge voorwaarden in acht worden genomen, in overeenstemming met de voorwaarden die het Europees Hof in *Murray* heeft geformuleerd, om het fundamentele beginsel van de onschulds-presumptie (men wordt voor onschuldig gehouden tot het tegendeel is bewezen) te respecteren. Het bevel zou daarom in slechts weinige gevallen effectief kunnen zijn.

Er daalt een algehele moedeloosheid neer over de conferentie: misschien is er geen haalbare manier om ervoor te zorgen dat de politie cryptosleutels kan verkrijgen en versleutelde, mogelijk belastende gegevens kan ontcijferen. Aan de andere kant realiseren Vera, Bob, Annie en Paula zich met enige opluchting dat de politie nog andere opsporingsbevoegdheden heeft om gegevens te verzamelen, te meer nu in het post-IRT-tijdperk nieuwe opsporingsmethoden worden overwogen. Het Nederlandse wetsvoorstel *Bijzondere opsporingsmethoden* stelt ‘direct afluisteren’ voor: richtmicrofoons en af luisterapparaten die gesprekken (en wie weet toetsenbordaanslagen) kunnen opvangen op het moment dat ze worden uitgesproken (of getikt) nog voordat ze kunnen worden versleuteld. Deze bevoegdheid zou vergaand kunnen worden uitgebreid om het cryptoprobleem aan te pakken, vooral door de politie toe te staan om in woningen af te luisteren. Een andere alternatieve opsporingsmethode is het onderscheppen van elektromagnetische straling (TEMPEST-afluisteren), waarmee men de inhoud van computerschermen kan reproduceren vanuit een naburig gebouw of vervoermiddel. Verder zijn er andere manieren om informatie te verzamelen over de georganiseerde misdaad in het bijzonder: men kan in een misdaadorganisatie infiltreren of men kan een medeplichtige ter terechtzitting laten optreden als kroongetuige in ruil voor strafvermindering. De conferentiedeelnemers realiseren zich dat deze juridische methoden, in tegenstelling tot de technische methoden van direct en TEMPEST-afluisteren, ver verwijderd zijn van telefoontaps en computeronderzoek, omdat ze andersoortige informatie opleveren. Daar komt nog bij dat al deze methoden een ernstige inbreuk maken op fundamentele rechten: de eerste twee vormen een grote bedreiging voor de privacy, en de laatste twee bedreigen de heerschappij van het recht. Geen van deze maatregelen is daarom een evidente oplossing om de lacune op te vullen die cryptocriminelen veroorzaken in de mogelijkheden van informatievergaring van de politie. Het enige dat de conferentiegangers op dit moment kunnen zeggen is dat direct afluisteren werkbaarder is dan TEMPEST-afluisteren en dat infiltratie te prefereren valt boven kroongetuigen (die een grotere inbreuk maken op de heerschappij van het recht).

Misschien, verzucht Vera, moeten we dan maar helemaal niets doen. Als de negatieve gevolgen van elke optie groter zijn dan de positieve, dan is dat wellicht de beste optie. Het enige nadeel daarvan is natuurlijk dat het cryptocriminelen ruim baan geeft. De conferentiedeelnemers sluiten de tweede dag dan ook enigszins verward af. Zij hebben vastgesteld welke opties haalbaar zijn om het cryptoprobleem aan te pakken: verdachten bevelen te ontsleutelen en de bewijslast omkeren als zij dat weigeren, meer 'direct af luisteren' en infiltreren, of besluiten om niets te doen – maar ze realiseren zich dat geen enkele optie echt bevredigend is.

Conclusie

Een nachtje rust verheldert evenwel de geest en de conferentiegangers beginnen de derde dag de opties met hernieuwde moed nog eens te bekijken. Ze herinneren zich het perspectief van Annie, de gezagsgetrouwe cryptogebruiker, als het perspectief vanwaaruit zij naar het probleem moeten kijken, en met die blik bekijken ze de opties opnieuw. Ze merken eerst op dat alle haalbare opties maar beperkt effectief zijn, omdat ze alleen met moeite of in een beperkt aantal gevallen kunnen worden geïmplementeerd. Ze herinneren zich ook uit het achtergrondstuk dat momenteel de bedreiging van cryptocriminelen klein is – nauwelijks voldoende om ernstige inbreuken op fundamentele rechten te rechtvaardigen. Ook heeft de politie veel opsporingsbevoegdheden die kunnen helpen om ten dele het informatieverlies te compenseren dat cryptocriminelen veroorzaken. Ze kunnen bijvoorbeeld verkeersanalyse bij telecommunicatie gebruiken (wat niet door cryptografie wordt gehinderd), infiltreren en (binnenkort) 'direct af luisteren'. Daarnaast kunnen ze in sommige gevallen nog (niet-verdachte of bedrijfsmatige) mensen vragen te ontsleutelen, met een redelijke kans van slagen. Aangezien Annies recht op privacy meer gewicht draagt dan haar recht op vrijwaring van misdaad (de ondergrens van dit laatste recht staat immers niet op het spel in welke optie dan ook), moeten de conferentiegangers voorzichtig zijn met opties die de privacy bedreigen maar die een beperkte effectiviteit en een povere rechtvaardiging in de opsporingspraktijk hebben.

Dit alles in aanmerking genomen, kiezen de conferentiedeelnemers de nuloptie. Zij concluderen dus dat vooralsnog de Nederlandse overheid de nuloptie moet aannemen als de optie die het beste de tegenstrijdige cryptobelangen met elkaar verzoent.

Toekomst

Aangezien alles in beweging is, realiseren Vera, Annie, Paula en Bob zich evenwel dat in de toekomst dit beleid periodiek moet worden herzien. Ze speculeren dat als eenmaal cryptocriminelen daadwerkelijk een belangrijk probleem blijken te zijn voor de opsporing en vervolging van misdaad, mogelijk een andere optie dan de nuloptie zou moeten worden gekozen. De grootste toekomstige cryptocriminele bedreiging zal hoogstwaarschijnlijk door georganiseerde misdadigers worden gevormd, en cryptocriminelen zullen meer het tappen dan het doen van onderzoek in computers belemmeren. Alternatieve opsporingsmethoden hebben meer potentie om misdaadorganisaties op te sporen en te vervolgen dan het omkeren van de bewijslast door controversiële juridische constructies. Vanuit het perspectief van Annie zijn alternatieve opsporingsmethoden waarschijnlijk aanvaardbaarder dan een regeling van een decryptiebevel die het effect kan hebben van een risico-aansprakelijkheid op cryptogebruik. Misschien zou daarom de overheid langzaam moeten wennen aan het idee dat

aftappen geen panacee is voor de informatiebehoefte van de politie, en zouden ze hun middelen moeten richten op andere, minder cryptogevoelige, opsporingsmethoden.

Aan het eind van de conferentie kijken de deelnemers terug om te evalueren wat zij hebben gedaan. Na het definiëren van principes en beslisregels, het overzien van mogelijke opties en het verkleinen van de lijst tot haalbare opties, moesten de deelnemers een beslissing nemen over het kernprobleem. Met gebruikmaking van het perspectief van de gezagsgetrouwe cryptogebruiker als de minst bevoordeelde groep, oordeelden zij dat vooralsnog de nuloptie de voorkeur verdient. Beleidsmakers moeten echter de ontwikkelingen nauwgezet blijven volgen om dit besluit periodiek te toetsen en zonodig bij te stellen. Afhankelijk van de omvang van de misdaad, van het cryptogebruik van misdadigers en van de opsporingsmethoden die de politie ten dienste staan, zou dat kunnen leiden tot het toestaan van meer alternatieve opsporingsmethoden, teneinde de mogelijk verminderde effectiviteit van tappen tegen te gaan.