Satelliet notitie: Open Bron Criminaliteit 'de anonieme en flexibele vijand'

Probleemgebied: Symbiose Misdaad Terrorisme

Probleem: **De nieuwe criminele netwerken bestaan uit kleine, diverse en autonome groepen van fanatiekelingen en misdadigers. Met als doorslaggevende kenmerken anonimiteit en een adaptieve vernieuwende structuur, die o.a. resulteert in significant kortere besluitvorming cycli dan die van de overheidsdiensten. De symbiose internationale misdaad en terrorisme creëert een voedingsbodem en een wereldwijd podium voor systeem verstoringen door nieuwe anonieme vijanden. De ultra bureaucratische overheid is niet ingericht om dreigingen te isoleren en uit te schakelen.**

Initiatiefnemer: De 419 Unit van Ultrascan Advanced Global Investigations [1]
Liaison in Nederland is Frank Engelsman
419unit@ultrascan.nl

Doel: **Het aanreiken van een model waarmee georganiseerde Open Bron criminaliteit kan worden geïnventariseerd, voorkomen c.q. kan worden teruggedrongen.**

Middel: **Het inrichten van laagdrempelige (mobiele) helpdesk annex studie centra waar consumenten en marktpartijen vragen kunnen stellen over (de betrouwbaarheid van) of melding kunnen doen van Open Bron gemeenschapsnetwerken.**

De anonieme en flexibele vijand – Voorwoord

Deze notitie is als verkort discussie stuk samengesteld aan de hand van onderzoeksresultaten van de 419 Unit die onderzoek doet naar de werking en trends van met name Nigeriaanse Criminele Netwerken bestaande uit tenminste 23.740 personen. Het onderzoek heeft zich uitgebreid naar criminele cellen met een andere achtergrond, omdat onderzoeksgroep zich gedurende 2006 en 2007 flexibel uitbreidde met ongeveer 3500 hoofdzakelijk Roemeense en Chinese personen die zich merendeels niet gewaar zijn met wie ze nu eigenlijk werken. Het gemak waarmee dit fenomeen zich heeft voorgedaan is onheilspellend, was het voorheen zo dat etnische culturele achtergronden een zekere drempel opwierp om tot samenwerking te komen (vraag een Roemeen of een Chinees eens of hij/zij voor een Nigeriaan wil werken), de groeiende acceptatie van anonimiteit heft die barrière op.

Anonimiteit binnen (internet) criminele netwerken is niet alleen dáár norm, maar ook het preventie advies van de overheid aan de deelnemers van gemeenschapsnetwerken in het algemeen. *"geef nooit persoonlijke gegevens aan iemand die je niet kent"* Dit zijn o.a. de redenen waardoor het als normaal word ervaren dat miljoenen vooral jonge mensen inmiddels een belangrijk deel van hun leven onder een valse of zoals zij het zelf soms zien een fantasie identiteit voeren, een prefab fantasie identiteit is tegenwoordig duurder dan een vals paspoort, de grenzen vervagen hier in een rap tempo. De meerderheid van deelnemers aan gemeenschapsnetwerken weten niet wie en waar hun contact, vriend of vijand, werkelijk is, hoewel daar bijvoorbeeld wel een nieuwe moraliteit gevormd word. Bijvoorbeeld, in publieke discussie fora is dubbel of tripel spel om andere deelnemers te manipuleren inmiddels meer regel dan uitzondering.

Zijn wij in de komende decennia nog wel geïnteresseerd in "lokale criminelen" met een gezicht, de Holleeders, Al Capone's, of de buren die teveel uit een sociaal potje hebben verbruikt? Dit type crimineel is dan waarschijnlijk niet meer relevant en middels nieuwe wetgeving afgeserveerd, alleen nog net goed genoeg als Romeinse brood en spelen voor een lokaal publiek.

Zeg nou zelf, het word toch pas bedreigend als een criminele organisatie zonder gezicht het dagelijks leven beïnvloed en bijvoorbeeld het gebruik van water of pinpassen voor onbepaalde tijd ondermijnt. En het idiote is, als dat U t.z.t. overkomt, het U niet eens meer zal verbazen omdat de beheerders van dat type diensten ons nu al met regelmaat van de klok aan die praktijk laten wennen.

Wij hebben nu de kans om de systemen die ons tot voor kort beschermde te herzien of aan te passen. Een kans die we beter niet missen. – Frank Engelsman

Inleiding
Het volgende decennium belooft veel voor het bedrijfsleven. De globalisatie opent nieuwe markten. De technologie ploegt vooruit en voorziet in - en transformeert - volledige industrieën, en diensten die wij nooit voor mogelijk achtte. En wereldwijd maken mensen op alle mogelijke manieren gebruik hiervan. Maar omdat globalisatie en technologie moreel neutrale machten zijn, kunnen zij ook tot andersoortige verandering leiden. Wij zagen dit duidelijk op 11 september en zien het nu in Irak en in conflicten rond de wereld. In het kort, ondanks het aura van onbeperkte mogelijkheden, kan ons leven zich ontwikkelen op een manier die wij alleen kunnen controleren indien wij het nieuwe landschap herkennen. Het is tijd om een serieuze blik vooruit te werpen.

Wij zijn het tijdperk van de anonieme en beweeglijke vijand (vriend) binnengegaan. Van Londen tot Madrid en Nigeria naar Rusland, staatloze terroristische en criminele groepen zijn opgedoken om slag na slag tegen ons te scoren. Gedreven door culturele versplintering, die middels de laatste technologieën onderricht wordt en gefinancierd met de opbrengsten uit transnationale misdaad, dwingen deze organisaties ons om nieuwe methoden ter verdedigen te ontwikkelen. Deze strijd zal leiden tot een nieuwe, veerkrachtiger benadering van (staats)veiligheid, niet gebouwd rond de staat, maar rond burgers en bedrijven. Dat nieuwe systeem zal veranderen hoe wij leven en werken.

Het eerste inzicht

Open-Bron Criminele Netwerken.

Verschillend aan bekende criminele structuren bestaan de nieuwe criminele netwerken uit 280 [2] tot 1187 [2] kleine, diverse en autonome groepen van fanatiekelingen en misdadigers. Deze groepen gebruiken dezelfde mogelijkheden als ons - van satelliettelefoons tot universitaire opleiding. Maar de meest waardevolle en doorslaggevende eigenschap is hun organisatie structuur, een Open-Bron gemeenschapsnetwerk, lijkend op, en wellicht afgeleid van, de Open-Source software-industrie.
Het is een, vanuit zichzelf, vernieuwende structuur, die resulteert in besluitvorming cycli die, significant korter zijn dan die van overheidsdiensten. Omdat deze groeperingen geen zwaartepunt hebben - een leiderschap structuur of een ideologie - zijn zij bijna immuun voor de toepassing van conventionele machtsmiddelen. De overheid treft hier geen gelijkwaardige tegenstander aan, maar een zichzelf aanpassend los netwerk van Open-Bron criminelen..

Het tweede inzicht

Symbiose Misdaad Terrorisme.
.
Het samengaan van internationale misdaad en terrorisme creëert een voedingsbodem en het wereldwijde podium voor nieuwe vijanden. Globalisering heeft de ontwikkeling van de misdaad economie gevoed, met een technologisch ondersteunde multinationale distributie keten waar alles kan, van mensen handel (Oost-Europa) tot drugs (Azië en Zuid-Amerika), geplagieerde goederen (Zuid-oost Azië), wapens (Centrale Azië) en witwassen van geld (overal).

De terrorisme misdaad symbiose wordt krachtiger wanneer beschouwd naast de ontwikkelingen in terrorisme. Terroristen hebben de bekwaamheid ontwikkeld om landen strategisch te bevechten - zonder massavernietigingswapens. Deze methode heet "systeem verstoring", een eenvoudige manier om kritische netwerken (elektriciteit, olie, gas, water, communicatie en vervoer) die het moderne leven mogelijk maken, aan te vallen. Deze verstoringen zijn bedoeld om het de overheid onmogelijk te maken aan haar zorgplicht naar de burgers te voldoen en zodoende burgerlijke ongehoorzaamheid en politieke chaos te veroorzaken.

De voorbeelden van systeem verstoring zijn voorspellend. Indien deze techniek word toegepast op de elektrische en olie-gassystemen in Rusland, Saudi-Arabië of ergens in het doelenrijk Westen, bijvoorbeeld op de overbelaste communicatie systemen, zouden wij al snel een begin van economische en politieke chaos zien. Het is nog verontrustender als wij de economische asymmetrie beschouwen: Een aanval op een oliepijpleiding kost ongeveer 2000 dollar en veroorzaakt 500 miljoen schade.

Het derde Inzicht

Overheden in discussie met en over zichzelf.

De groei van virtuele gemeenschappen - de groeiende criminele economieën, en innovatieve netwerken met hyper efficiënte wapens - zullen snel het publiek vertrouwen in onze (staats) veiligheidssystemen ondermijnen. Dit proces is reeds begonnen. Wij zien met de regelmaat van de klok verstoring van ons olieaanbod in Irak, Nigeria, Venezuela en Colombia; angst in de markt is nu de bepalende factor van de hogere prijzen geworden. Maar als die systeem verstoringen verder gaan, zal de schade de structuur van onze maatschappij aantasten. Departementen als Justitie en Defensie, die zich zelf na 11 september steeds vaker van brevetten van onvermogen voorzien zullen meer en meer als verouderd gezien worden.

Onvermijdelijk zal er een serie van aanvallen met grens overschrijdende gevolgen binnen onze westerse grenzen zijn. De departementen verantwoordelijk voor Veiligheid zijn, ondanks nieuwe (extra) wettelijke observatie mogelijkheden, niet in staat om bedreigingen tegen ons te isoleren en uit te schakelen. In, voor "iedere malloot", zichtbare gevallen van aanstaande systeemverstoring geeft de overheid geen blijk van handelen of herkenning van de dreiging. Nieuwe immigratie wetgeving, verplichte gegevensopslag en verbetering van grenscontrole, zijn wellicht politiek gewichtige onderwerpen, maar zijn net zo doeltreffend als de Chinese muur en de Maginot linie. De inhaalslagen die de overheid middels het Openbaar Ministerie, de opsporingsdiensten en toezichthouders na 9/11 heeft gemaakt zullen slechts voldoende zijn om de gestelde doelen te halen. Helaas zijn de doelen vanwege een verkrampte organisatie niet aangepast aan de nieuwe tegenstander.

Flexibele tegenstander! – Flexibele overheid?

De overheid zal zich flexibeler moeten opstellen om de juiste informatie m.b.t. georganiseerde Open Bron criminaliteit aan te trekken, verzamelen en te kunnen analyseren. "Slechts" starre ambtelijke hiërarchieën en politiek staan dan nog in de weg van noodzakelijke vernieuwende trajecten met korte besluitvorming cycli, gebruikmakend van bestaande (multi) nationale wetgevingen. Het blijkt weinig zin te hebben om een innovatieve afdeling onder een toevallig volgens anciënniteit in aanmerking komende ambtenaar te laten functioneren, maar waar vind je dan een ambtenaar die ruime ervaring met anonimiteit en flexibiliteit binnen gemeenschapsnetwerken heeft, eentje die bijvoorbeeld 10 uur per week onder een andere identiteit in een virtuele wereld zoals Second Life doorbrengt?

Publiek private samenwerking

Daarbij komt dat alle noodzakelijke informatie m.b.t. georganiseerde Open Bron Criminaliteit in de markt te verkrijgen is en het best via marktmechanisme kan worden verzamelt en geïnventariseerd, hopelijk nog voordat het tot excessen of systeem verstoringen zal leiden.

[1] *de 419 Unit stuurt ongeveer 3200 experts aan, verspreid over meer dan 69 landen. En word gesponsord door Ultrascan Advanced Global Investigations*
[2] *280 tot 1187 kleine, diverse en autonome groepen van fanatiekelingen en misdadigers, gebaseerd op getallen van de onderzochte, van origine, Nigeriaanse criminele netwerken.*

Als U reageert op dit discussie stuk wilt U dan ook onderstaande vragen beantwoorden:

1. Begrijpt U wat in dit stuk met Open Bron Criminaliteit word bedoeld? Ja/nee
2. Weet U wat Open-Source software ontwikkeling is? Ja/nee

2.2 Noem één gevolg, van Open-Source software ontwikkeling, voor de gevestigde orde in de software markt, zoals Microsoft?

3. Wat zijn in het stuk belangrijke kenmerken van nieuwe Criminele Netwerken?
4. Hoeveel uren per week of maand heeft U besteed in gemeenschappelijke virtuele werelden?
5. Hoe vaak per week of maand heeft U deel genomen aan discussies via publieke discussie fora?