Position Paper: Electronic Crimes Task Force

De digitalisering van onze samenleving heeft geleid tot nieuwe kansen, maar ook tot nieuwe dreigingen. Steeds meer Nederlanders worden geconfronteerd met digitale criminaliteit, wat leidt tot financiële schade en gevoelens van onveiligheid. Deze vorm van criminaliteit raakt niet alleen individuele slachtoffers, maar ondermijnt ook het bredere vertrouwen in digitale diensten en het betalingsverkeer als vitale infrastructuur. Fraudeurs misbruiken legitieme diensten van banken, zoals het uitvoeren van betalingen en verplaatsen van frauduleus verkregen geld. Dit vraagt om een stevige, gezamenlijke aanpak van digitale criminaliteit waarin publieke en private partijen hun krachten bundelen.

Sinds 2011 werken banken[1], politie en Openbaar Ministerie binnen de Electronic Crimes Task Force (ECTF) intensief samen om digitale criminaliteit effectief te bestrijden. De ECTF volgt de ontwikkelingen en nieuwe werkwijzen van criminelen nauwgezet en komt in actie zodra mensen slachtoffer worden van online fraude of High Tech Crime[2]. Bij de banken wordt door veiligheidsexperts een onderzoek ingesteld naar het incident, waarna het bewijs en digitale sporen via een aangifte bij de politie terechtkomt. Dit stelt de politie in staat een opsporingsonderzoek te starten. Hiermee voorkomt de Task Force dat er nieuwe slachtoffers vallen, verstoort het de werkwijze van criminelen én zorgt de Task Force ervoor dat bestaande slachtoffers genoegdoening krijgen doordat de daders strafrechtelijk worden vervolgd.

De ECTF geeft het volgende mee aan voor het rondetafelgesprek op 1 oktober:

- De Electronic Crimes Task Force (ECTF) is een bewezen publiek-private samenwerking tussen banken, politie en OM;
- Juridische beperkingen verhinderen effectieve samenwerking, waardoor opsporing vertraagt, criminelen netwerken uit het zicht blijven en daardoor slachtoffers blijven vallen;
- Wijs de ECTF aan als samenwerkingsverband onder de Wet gegevensverwerking door samenwerkingsverbanden (WGS) via een AMvB;
- Dit biedt de juridische basis om Nederlanders beter te beschermen tegen digitale criminaliteit, door gerichtere opsporing en de mogelijkheid om criminele netwerken effectief te doorbreken.

Uitdagingen ECTF

De ECTF levert een belangrijke bijdrage aan de opsporing van digitale criminaliteit, maar loopt tegen serieuze beperkingen aan die de effectiviteit van de taskforce onder druk zetten. Banken mogen onderling weinig informatie delen over gevallen van fraude en High Tech Crime. Doordat criminelen hun activiteiten bewust verspreiden over meerdere banken, heeft elke bank slechts een deel van het criminele netwerk in beeld. Je kunt het vergelijken met een puzzel: elke bank heeft een stukje, maar ze mogen die stukjes niet samenleggen. Hierdoor blijft waardevolle informatie liggen bij individuele banken, zonder dat zij zich er bewust van zijn dat een andere bank over aanvullende informatie beschikt. Banken worden beperkt in het waarschuwen van andere banken voor lopende incidenten en actieve criminele netwerken, waardoor het voorkomen van nieuwe slachtoffers ernstig wordt belemmerd. Ook de politie heeft onvoldoende informatie om de puzzel te kunnen leggen. De politie heeft bij de start van online

[1] ABN AMRO, ING, Rabobank, ASN bank, Triodos, International Card Services, Nederlandse Vereniging van Banken

[2] Dit zijn geavanceerde en complexere vormen van digitale criminaliteit waarbij vaak sprake van aanvallen op de vitale infrastructuur of betrokkenheid van (vermoedelijk) statelijke actoren

fraude onderzoeken vaak een ontoereikende informatiepositie omdat alleen de informatie vanuit de aangifte van het slachtoffer bekend is. Politiemedewerkers binnen de ECTF hebben vervolgens vaak geen of een beperkte opsporingsindicatie en mogen daardoor geen informatie vorderen bij de banken. Onderzoeken lopen daardoor onnodig vroegtijdig vast. In het gunstigste geval kan de opsporing actie ondernemen op basis van het gefragmenteerde beeld, wat in het beste geval kan leiden tot het vinden van enkele digitale criminelen. Als gevolg hiervan wordt het gezamenlijke doel van de ECTF, het tegengaan van digitale criminaliteit, slechts beperkt gerealiseerd, blijven criminele netwerken onder de radar en blijven er slachtoffers vallen.

In de tussentijd worden de digitale criminelen steeds slimmer, sneller en professioneler. Ze kunnen meer slachtoffers tegelijk benaderen, maken gebruik van AI en passen zich flexibel aan op de opsporing: als één methode wordt ontdekt, schakelen ze snel over op een andere. De ECTF mist die snelheid. Enerzijds doordat de politie belangrijke informatie mist en een versnipperd beeld aangeleverd krijgt. Anderzijds doordat de gegevensuitwisseling tussen banken en politie via een aangifte en vordering verloopt en dit veel tijd kost. Hierdoor ontstaat vertraging in de opsporing, terwijl snelheid juist essentieel is om bij incidenten digitale sporen veilig te stellen en criminelen te ontmaskeren.

In de praktijk betekent dit dat digitale criminelen op grote schaal hun gang kunnen gaan, terwijl burgers steeds vaker slachtoffer worden zonder dat daders worden opgespoord. Door trage en omslachtige gegevensuitwisseling ontbreekt het aan snelheid en slagkracht. Hierdoor blijven digitale sporen onbenut en krijgen slachtoffers zelden genoegdoening. Ze zien dat hun zaak blijft liggen en ervaren dat de daders hun praktijken voortzetten zonder merkbare consequenties.

Wat is nodig?

- **Fraude vereist snelle actie.** In tegenstelling tot veel andere veiligheidsthema's wordt in de aanpak van fraude incidentgericht gewerkt, waarbij een snelle respons vanuit de taskforce op het incident cruciaal is.
- **Een meer geïntegreerde aanpak van criminaliteit, waarbij informatie uit verschillende bronnen gecombineerd kan worden.** Een geïntegreerde aanpak is nodig omdat digitale criminaliteit zich verspreidt over meerdere partijen, waardoor cruciale informatie versnipperd raakt. Door gegevens uit verschillende bronnen te combineren, ontstaat een volledig beeld van criminele netwerken en kan sneller en gerichter worden opgetreden.
- **De mogelijkheid vanuit politie om deelnemers van de ECTF in een vroeg stadium, bijvoorbeeld tijdens een vooronderzoek, voorafgaand aan een vordering, laagdrempeliger te bevragen over fraude-incidenten.** Dit maakt het mogelijk om sneller te handelen bij signalen van criminaliteit, en vergroot de kans dat opsporingsonderzoeken succesvol kunnen worden gestart én afgerond.
- **Meer ruimte voor vroegtijdige waarschuwing en preventie.** Banken moeten elkaar binnen de ECTF kunnen waarschuwen voor incidenten, zodat criminele netwerken sneller worden herkend en nieuwe slachtoffers kunnen worden voorkomen. Dit vraagt om heldere kaders voor informatie-uitwisseling en samenwerking, zonder dat dit ten koste gaat van privacy.

Hoe bereiken we dit?

Om dit te bereiken, bepleiten wij dat de ECTF wordt aangewezen als samenwerkingsverband onder de Wet gegevensverwerking door samenwerkingsverbanden (WGS), via een algemene maatregel van bestuur (AMvB). Dit stelt de ECTF in staat om deze ernstige vorm van criminaliteit effectiever aan te pakken, wat zal bijdragen aan de maatschappelijke veiligheid. Deze wettelijke verankering biedt de noodzakelijke juridische basis voor een effectieve, geïntegreerde aanpak van online fraude en High Tech Crime. Want alleen een krachtig netwerk kan criminele netwerken doorbreken.

Contactgegevens: *L. van Meijgaard*
Adviseur ECTF: meijgaard@nvb.nl