Fysieke aanvallen op geldautomaten voorkomen

Ontwikkeling van een doeltreffende aanpak

Dankwoord
Dit document is het resultaat van een samenwerking tussen het Agentschap van de Europese Unie voor samenwerking op het gebied van rechtshandhaving (Europol) en het secretariaat van het Europees netwerk inzake criminaliteitspreventie (EUCPN). Wij willen de deskundigen inzake fysieke aanvallen op geldautomaten bedanken voor de tijd en moeite die zij geïnvesteerd hebben om mee te werken aan de totstandkoming van dit aanbevelingsdocument. Zij leverden hun bijdrage door aanwezig te zijn op de conferentie over de preventie van fysieke aanvallen op geldautomaten (januari 2019, Brussel) en door cruciale informatie te verstrekken. Onze dank gaat in het bijzonder uit naar de ordehandhavingsdiensten van EU- en niet-EU-landen ('derde'), de privésector waaronder de ATM Industry Association (ATMIA), BPost, het Centrum voor Criminaliteitspreventie en Veiligheid (CCV), Diebold Nixdorf, de European Association for Secure Transactions Expert Group on ATM and [automatic teller safes] ATS Physical Attacks (EAST EGAP), de European Intelligent Cash Protection Association (Euricpa), ING, Febelfin, NCR, Protect, SIOC Banking, Spinnaker en TMD Security, en de ministeries van Binnenlandse Zaken van België, Kroatië, Duitsland en Spanje.

Juridische informatie
De inhoud van deze publicatie geeft niet noodzakelijkerwijs de officiële mening weer van een EU-lidstaat of een agentschap of instelling van de EU of de Europese Gemeenschappen.

Inhoudsopgave

1 Context

Omdat steeds meer Europese landen steeds vaker geconfronteerd worden met fysieke aanvallen op geldautomaten, organiseerden het Europees netwerk inzake criminaliteitspreventie (EUCPN) en Europol in januari 2019 een congres, waar ordehandhavingsdiensten samen met publieke en particuliere partners bekeken hoe ze dit soort criminaliteit kunnen voorkomen. Dit aanbevelingsdocument vat de conclusies van die conferentie samen om zulke fysieke aanvallen op geldautomaten én mogelijke preventieve maatregelen onder de aandacht van overheden te brengen.

Alle verschillende methodes (*modi operandi* (MO)) die criminelen gebruiken om geldautomaten aan te vallen, kan men opdelen in twee grote categorieën: fysieke aanvallen en fraudeaanvallen (waaronder digitale aanvallen en aanvallen met malware op geldautomaten). Dit document gaat over fysieke aanvallen: geldautomaten met geweld kraken om het geld te ontvreemden. Kraken met geweld kan door:

- het gebruik van explosieven: aanvallers gebruiken een gas of vaste explosieven om fysiek in de kluis van de geldautomaat in te breken en toegang te krijgen tot het geld;
- rip-out/ram-raidaanvallen: aanvallers verwijderen fysiek de hele geldautomaat, vaak met behulp van een gespecialiseerd voertuig;
- in-situ-aanvallen: aanvallers breken met brute kracht in de kluis in, vaak met behulp van snij- of breekgereedschap zoals hoekslijpmachines, sloophamers of lasbranders.

Een beperkt maar groeiend aantal landen in de Europese Unie heeft af te rekenen met fysieke aanvallen op geldautomaten. Het financiële verlies in Europa voor 2017 wordt geschat op meer dan 30 miljoen euro. In een aantal landen lag het aantal fysieke aanvallen op geldautomaten al hoog, terwijl andere landen het aantal aanvallen de afgelopen twee jaar sterk heeft zien toenemen. Het gaat om een vorm van criminaliteit die snel evolueert. Enkele landen hebben fysieke aanvallen op geldautomaten met succes aangepakt, waardoor het aantal aanvallen er sterk is teruggevallen. Maar er zijn ook landen die in 2018 voor het eerst en in stijgende mate geconfronteerd werden met fysieke aanvallen op geldautomaten, omdat criminele organisaties hun territorium hebben uitgebreid. Niet alleen banken worden aangevallen, geldautomaten van onafhankelijke providers vormen steeds vaker een doelwit, omdat die zich vaak in kwetsbare gebouwen of locaties bevinden.

2 Factoren die het succes van een fysieke aanval op een geldautomaat bepalen

Aanvallen op geldautomaten zijn zelden succesvol, namelijk slechts in een derde van de gevallen. Maar ook een aanval die niet succesvol is, veroorzaakt heel wat schade (bijvoorbeeld door explosieven) aan gebouwen en infrastructuur, wat de omgeving van de plaats delict onveilig maakt voor omwonenden, eerstehulpverleners en voorbijgangers.

Het succes van een fysieke aanval hangt af van een aantal factoren, zoals de kenmerken van de geldautomaat, de organisatie van de aanval en de ervaring en kennis van de daders.

2.1 Kwetsbaarheid van geldautomaten

De meest kwetsbare geldautomaten bevinden zich buiten (in de muur) of in gebouwen. Wanneer criminele organisaties een (alleenstaande) geldautomaat binnen aanvallen, doen ze dat liever in commerciële gebouwen dan in bankgebouwen, aangezien die doorgaans sterker bewaakt worden. Banken beheren voornamelijk geldautomaten die zich in of buiten aan een bankkantoor bevinden. Doordat steeds meer bankkantoren worden gesloten, worden locaties die niet bij een bank gelegen zijn, in de straat en in commerciële handelsgebouwen zoals benzinestations, supermarkten, hotels, casino's, vliegvelden, enz. steeds belangrijker. Onafhankelijke providers beheren geldautomaten als een op zichzelf staande dienstverlening. Hun geldautomaten bevinden zich vaak in handelszaken, hotels, sport- en ontspanningsfaciliteiten, op transportlocaties (treinstations, luchthavens, enz.), in openbare gebouwen en op straat.

Door de toenemende populariteit van internetbankieren zullen er de komende jaren wellicht veel bankkantoren verdwijnen, waardoor het aantal geldautomaten in het algemeen zal dalen. ([1]) Maar dat zou kunnen leiden tot een stijging van het aantal niet-bankgerelateerde geldautomaten en onafhankelijk beheerde geldautomaten op kwetsbare locaties.

([1]) Willem Pieter de Groen, Zachary Kilhoffer en Roberto Musmeci, *The future of EU ATM markets: impacts of digitalisation and pricing policies on business models*, CEPS-rapport, 2018

2.2 Organisatie van een aanval op een geldautomaat

De voorbereiding van een aanval kan enkele weken of zelfs maanden in beslag nemen. Daders moeten de nodige **hulpmiddelen en manschappen** verzamelen, zoals voertuigen, gereedschap en contactpersonen. **Voertuigen** zijn essentieel voor fysieke aanvallen op geldautomaten; daders verplaatsen zich vooral met de auto en ontsnappen na de aanval meestal met snelle voertuigen. Vaak zijn die gestolen, maar ze kunnen ook gehuurd of gekocht zijn (bijvoorbeeld via het internet). Het meeste **gereedschap** voor fysieke aanvallen op geldautomaten is vrij en legaal te verkrijgen in gewone winkels. Dat verlaagt de drempel nog om de stap te zetten naar deze vorm van criminaliteit. Voor speurders is het moeilijk om na te gaan waar gereedschap precies vandaan komt, wat maakt dat de risico's voor daders beperkt zijn. Criminele organisaties die op een internationaal niveau aanvallen op geldautomaten uitvoeren, hebben bijna altijd contactpersonen in het land van het doelwit (mensen die daar voor een bepaalde periode verblijven) of ze kunnen een "hit-and-run"-techniek toepassen. Die contactpersonen ondersteunen de criminele organisaties logistiek, en zorgen bv. voor onderdak, een voertuig of ander materiaal of verkennen doelwitten. Er zijn internationale daders die de logistiek en verkenning volledig overlaten aan de lokale contactpersonen en met het vliegtuig of over land enkel komen om de aanval uit te voeren.

Criminele organisaties **verkennen** vaak uitgebreid om een geschikt doelwit te vinden; ze noteren wanneer de geldautomaat wordt gevuld, leren de omgeving kennen, de technische kenmerken van de geldautomaat, de vluchtwegen en de aanwezige beveiliging, zoals bewakingscamera's, alarmsensoren en rolluiken.

Er zijn criminele organisaties die bepaalde zaken doen om **politie en beveiligingsdiensten op een verkeerd spoor** te zetten. Ze knoeien met alarmsystemen en openbare verlichting, zorgen voor afleiding, zetten wegblokkades op of proberen politievoertuigen te saboteren.

2.3 De ervaring en kennis van de daders

Fysieke aanvallen op geldautomaten zijn aantrekkelijk voor criminelen omdat het geld direct beschikbaar is en ze geen uitgebreid netwerk nodig hebben om gestolen goederen te verkopen. Het is een handig alternatief voor criminelen die al actief zijn in de georganiseerde vermogenscriminaliteit.

Criminele organisaties moeten de **nodige expertise en kennis** vergaren, aangezien dat bepalende factoren zijn voor het lukken of mislukken van een aanval. De vereiste expertise en kennis hangen sterk af van het **soort aanval.** Rip-out/ram-raid- en *in-situ*-aanvallen hebben een eenvoudige MO (voornamelijk durf en het gebruik van brute kracht), waardoor ze over het algemeen geen specifieke vaardigheden vereisen. Aanvallen met ontvlambare gassen of vaste explosieven vereisen meer deskundigheid.

Aanvallers zijn niet allemaal even **bekwaam**. Enerzijds zijn er zeer georganiseerde en ervaren groepen die binnen enkele minuten met succes een fysieke aanval op een geldautomaat kunnen uitvoeren. Zij hebben de situatie in de hand en zijn in staat om het risico voor zichzelf, en daardoor ook de nevenschade, te beperken. Maar er zijn ook opportunistische en minder georganiseerde groepen, die vaak falen en veel schade kunnen aanrichten aan de locatie en de gebouwen in de buurt. Een aantal van die minder georganiseerde criminele organisaties keert terug naar de traditionele vermogenscriminaliteit, omdat ze ontmoedigd worden door de preventieve maatregelen waar zij bij een aanval op een geldautomaat op botsen.

3 Nood aan een preventieve aanpak

Landen waar fysieke aanvallen op geldautomaten zelden succesvol zijn of waar het aantal fysieke aanvallen op geldautomaten afneemt, illustreren dat een succesvolle aanpak ter bestrijding van fysieke aanvallen op geldautomaten operationele en preventieve maatregelen combineert. Aangezien maar een beperkt aantal criminele organisaties zich toelegt op deze vorm van criminaliteit, daalt het aantal aanvallen sterk wanneer leden van zulke organisaties opgepakt en bestraft worden. Maar wanneer ze worden vrijgelaten, hervallen veel aanvallers van geldautomaten in hun activiteiten. Bovendien wordt de plaats van een opgepakte dader soms snel ingenomen door een groep. Daarom is er een grote behoefte aan preventieve maatregelen, bij voorkeur binnen een wettelijk kader. Bovendien weten we uit ervaring dat preventieve maatregelen in het ene land criminele organisaties naar meer kwetsbare doelwitten in andere landen kunnen duwen. Het is slechts een kwestie van tijd voordat MO die in één land ontstaan zich naar andere landen verspreiden. Dit geeft duidelijk aan dat **de preventieve en operationele maatregelen op Europees niveau moeten worden genomen**, waarbij particuliere en openbare spelers nauw samenwerken met de ordehandhavingsinstanties.

4 Preventie

Er is een duidelijke strategie nodig om dit soort criminaliteit te voorkomen en aan te pakken. In dit hoofdstuk bespreken we de drie stappen die doorgaans worden genomen bij fysieke aanvallen op geldautomaten of bij de voorbereiding om die te voorkomen.

Allereerst moet de **situatie worden ingeschat**; er moet een risicoprofiel opgesteld worden van de geldautomaten en hun omgeving, waarbij rekening wordt gehouden met de beschikbare hoeveelheid contant geld (mogelijke buit), het risico op nevenschade en het risico op persoonlijk letsel. Ten tweede moet er op basis van de risicobeoordeling een **preventieve strategie** worden ontwikkeld. Tot slot moeten de **preventieve maatregelen** worden ingevoerd.

4.1 De situatie inschatten

Criminele organisaties richten hun pijlen doorgaans op specifieke soorten geldautomaten of op geldautomaten van specifieke providers, met kenmerken die een aanval makkelijker maken. Daarom is het nodig om het risico van fysieke aanvallen op geldautomaten grondig in te schatten, bij voorkeur ook de hele beveiligingsketen voor het geld, van vervoer tot levering en opslag in de geldautomaat. Om het risicoprofiel van elke geldautomaat op te stellen, moet een aantal elementen worden geanalyseerd, waaronder:

- De kenmerken van de locatie en de omgeving van de geldautomaat; gaat het om een automaat in de stad of op het platteland, wat is de bevolkingsdichtheid, zijn er politiebureaus, camera's voor automatische nummerplaatherkenning, bewakingscamera's in de buurt, enz.
- De plaats van de geldautomaat:
    - binnen of buiten een gebouw, in een bankkantoor of in een ander (bv. commercieel) gebouw, in de muur of vast aan een gebouw;
    - voor alleenstaande geldautomaten: of ze verankerd zijn of niet;
    - voor geldautomaten in de muur of aan een gebouw vastgemaakt: of er architecturale tekortkomingen zijn, hoe de opslag van het geld wordt georganiseerd, enz.;
- Het soort geldautomaat.
- De in de geldautomaat geïntegreerde beveiligingsfuncties;
- De hoeveelheid geld in de geldautomaat;
- Het soort fysieke aanvallen en de verwachte MO om de meest geschikte preventieve maatregelen te nemen;

– De reeds genomen beveiligings- en preventiemaatregelen (intelligente systemen voor de neutralisatie van bankbiljetten, camerabewaking, een rooksysteem (beperkte zichtbaarheid), enz.).

Andere elementen die moeten worden geëvalueerd zijn de mate van samenwerking met partners en stakeholders en de wetgeving. De samenwerking tussen ordehandhavingsdiensten, particuliere en publieke partners moet worden geëvalueerd om allianties te smeden in de strijd tegen criminaliteit. Mogelijk beschikt elke partner over interessante informatie die kan helpen om de situatie te beoordelen. De lokale politie of lokale autoriteiten zijn binnen dat kader bijzonder belangrijk. De wetgeving moet worden geëvalueerd in die zin dat er een wettelijk kader wordt gecreëerd voor preventie, het nemen van verplichte preventieve maatregelen, het opleggen van straffen voor aanvallen op geldautomaten, enz.

4.2 Een preventieve aanpak ontwikkelen

Zodra de situatie is beoordeeld, en de belangrijkste risicogebieden en de sterke en zwakke punten van de beveiliging van de geldautomaat zijn vastgesteld, kan er een strategie worden ontwikkeld (vaak op basis van een publiek-private samenwerking) en kunnen er preventieve en operationele tegenmaatregelen worden genomen. Preventieve maatregelen moeten gericht zijn op de intentie en capaciteiten van de daders. Daarvoor worden drie preventieve actiepijlers voorgesteld, gebaseerd op drie van de vijf strategieën voor de preventie van situationele criminaliteit door Clarke ([2]); de beloning kleiner maken, het risico voor de daders vergroten en het moeilijker maken om toegang te krijgen tot de buit.

Criminelen wegen het verwachte rendement af tegen de daaraan verbonden risico's (bv. bij een aanval op een geldautomaat). Als de kans op een snelle beloning kleiner en het risico voor de daders groter wordt, zullen hun verwachtingen en de drang om een fysieke aanval op een geldautomaat uit te voeren afnemen. Verdere maatregelen die de toegang tot de geldautomaat bemoeilijken, hebben betrekking op de capaciteiten van de daders. Opportunistische daders, die vaak falen, zullen hun aanvallen op geldautomaten staken. Professionele aanvallers zien hun kans op succes slinken, wat weer van invloed is op de rendement/risico-afweging.

([2]) Derek Cornish en Ronald V. Clarke, 'Opportunities, precipitators and criminal decisions: a reply to Wortley's critique of situationational crime prevention', *Crime prevention Studies 16* (2003), 41-96.

De preventieve strategie wordt aangevuld met parallelle maatregelen zoals een doeltreffende mediastrategie, vroegtijdige sociale preventie en maatregelen om het risico op nevenschade aan gebouwen te verminderen en om de veiligheid van omwonenden, eerstehulpverleners en voorbijgangers te waarborgen.

Er zijn ook andere manieren om de aanpak te structureren. In Nederland passen de autoriteiten het zogenoemde barrièremodel toe ([3]). Dit model identificeert de stappen die een crimineel moet zetten om een misdrijf te plegen. Het identificeert ook de partners en de kansen die het misdrijf mogelijk maken en het is een nuttig instrument om het proces van informatieverzameling over de vorm van criminaliteit te organiseren. Door elke stap te identificeren die nodig is om een fysieke aanval op een geldautomaat uit te voeren, kunnen de barrières geïdentificeerd worden om het misdrijf te voorkomen, en de beste partners om die barrières op te zetten. Het barrièremodel identificeert ook signalen om de publieke en private partners te waarschuwen voor fysieke aanvallen op geldautomaten en signalen die zij zelf kunnen sturen om de autoriteiten op de hoogte te stellen van hun vermoedens.

Er is een goed ontwikkelde strategie nodig om de risico's te beperken die gepaard gaan met preventieversterking. Preventieve maatregelen die zeer doeltreffend zijn in het ontmoedigen van amateurs en copycats hebben soms ongewenste gevolgen. Sommige groepen grijpen naar trial-and-error-methoden om kwetsbare geldautomaten te vinden, waarbij ze een spoor van beschadigde geldautomaten achterlaten. Gevaarlijkere en meedogenlozere criminele organisaties gaan in hun aanvallen driestere MO hanteren, zoals overstappen van gas op vaste explosieven.

Om een efficiënte reeks preventieve maatregelen door te voeren, is bewezen dat het nuttig is om een nationale autoriteit op te richten die de bevoegdheid heeft om op basis van een grondige analyse van de situatie specifieke maatregelen voor risicovolle geldautomaten op te leggen. Deze aanpak is in Frankrijk doeltreffend gebleken, vooral als er een wettelijk kader wordt vastgelegd en de maatregelen samen met de operationele maatregelen worden ingevoerd.

4.3 Preventieve maatregelen invoeren

([3]) Centrum voor Criminaliteitspreventie, barrièremodellen, www.barrieremodellen.nl

De in dit hoofdstuk voorgestelde maatregelen om fysieke aanvallen op geldautomaten te voorkomen, hebben in verschillende landen hun nut al bewezen. Zij zijn gebaseerd op de conclusies van de conferentie rond preventie en op preventieve maatregelen die actief worden gepromoot door internationale organisaties die werken rond de beveiliging van geldautomaten. Veel maatregelen zijn bekend. Verschillende landen hebben een aantal maatregelen al met succes ingevoerd. Maar vaak worden de voorgestelde maatregelen slechts gedeeltelijk ingevoerd en niet wettelijk verankerd.

Zoals hoger aangehaald, worden drie preventieve actiepijlers voorgesteld: de beloning kleiner maken, het risico voor de daders vergroten en het moeilijker maken om toegang te krijgen tot de buit.

4.3.1 De beloning kleiner maken

De eerste pijler om aanvallen op geldautomaten te voorkomen, is het kleiner maken van de beloning. Zolang het beeld van 'easy money' blijft bestaan, zal deze vorm van criminaliteit populair blijven. Als de hoeveelheid geld wordt beperkt, vernietigd of onbruikbaar gemaakt, wordt de kans op een interessante buit kleiner. En als de buit minder aanlokkelijk is, zal men minder geneigd zijn om over te gaan tot een aanval.

4.3.1.1 *Minder geld beschikbaar maken*

Een van de maatregelen om de beloning kleiner te maken is minder geld in de geldautomaat stoppen. In het ideale geval is er maar zoveel geld beschikbaar als er voor één dag nodig is. Als banken samenwerken, kan dit kosteneffectief gebeuren. In Nederland hebben enkele banken samen een bankonafhankelijk netwerk van geldautomaten opgezet onder de naam 'Geldmaat'. Het doel van de samenwerking is ervoor zorgen dat contant geld beschikbaar, toegankelijk, betaalbaar en veilig is. Dit zal er waarschijnlijk toe leiden dat een aantal geldautomaten verdwijnen. Elke geldautomaat zal echter niet meer geld bevatten, maar wel vaker worden bijgevuld. De frequentie van bijvullen zal naar behoefte worden aangepast.

Aangezien geldautomaten meestal tussen 03.00 en 04.00 uur worden aanvallen, wordt voor alleenstaande geldautomaten (meestal in commerciële en openbare gebouwen, die kwetsbaarder zijn) sterk aangeraden om de geldautomaat op het einde van de dag leeg te maken en het geld naar een kluis te brengen. Een bordje kan duidelijk maken dat de geldautomaat 's nachts geen geld bevat.

De volgende dag moet de geldautomaat uit het zicht van klanten en met het gebouw op slot bijgevuld worden. Dit systeem wordt al toegepast in Frankrijk, waar winkeliers met een alleenstaande geldautomaat in de winkel wettelijk verplicht zijn om die 's avonds leeg te maken en open te laten staan. Voor andere geldautomaten kan het beschikbare geld laag gehouden worden door vaker bij te vullen.

4.3.1.2 *De buit onbruikbaar maken of het geld traceerbaar maken*

Intelligente systemen voor de neutralisatie van bankbiljetten (IBNS) zijn een eerste manier om een buit onbruikbaar te maken. Deze systemen bevlekken de bankbiljetten met inkt om ze als gestolen te markeren. Aan de IBNS-inkt kunnen nog tracers en markers toegevoegd worden. Op dit moment worden zulke markers vooral gebruikt voor forensische doeleinden, waarbij het bankbiljet wordt gelinkt aan de plaats delict en het risico voor de daders om gepakt te worden groter wordt. Het IBNS is een doeltreffende preventieve maatregel, maar met enkele bedenkingen.

De Europese Centrale Bank vergoedt bevlekte bankbiljetten niet meer [4](sinds 2003), maar een aantal nationale centrale banken van EU-lidstaten wel nog. Ook via casino's worden bevlekte biljetten weer in het legale circuit opgenomen. Een IBNS creëert een extra obstakel voor criminelen, maar zou veel doeltreffender zijn als het voor criminelen onmogelijk was om bevlekte biljetten in de EU te gebruiken. Daarvoor zouden de nationale centrale banken geen bevlekte biljetten meer mogen aanvaarden. Uitzonderingen kunnen gemaakt worden voor specifieke gevallen, bv. voor biljetten die bevlekt zijn tijdens een foutieve activering. Het is ook belangrijk om de bevolking erop te wijzen geen bevlekte biljetten aan te nemen. Op langere termijn zouden automaten die biljetten ontvangen bevlekte biljetten moeten herkennen, en geplaatst moeten worden in banken en in commerciële gebouwen zoals casino's, wasstraten, enz. Inkt detecteren is moeilijk en duur. Een kosteneffectieve oplossing zou kunnen zijn om infraroodsystemen te installeren die biljetten met infrarode markers herkent. Deze systemen hebben hun doeltreffendheid al bewezen in bijvoorbeeld België en Frankrijk. Wanneer biljetten met infraroodmarkering in de geldautomaat worden ingevoerd, zal de geldautomaat het geld accepteren ('inslikken') maar op een rekening zetten. Er zou ook bijgehouden moeten worden wie de bevlekte bankbiljetten inbrengt.

Wanneer men IBNS gebruikt, zijn er nog een aantal zaken waar men rekening mee moet houden. Er zijn meerdere fabrikanten die verschillende IBNS-oplossingen aanbieden met verschillende activeringsmechanismen en verschillende soorten inkt. Een eerste bedenking is dat niet alle soorten

---

([4]) Europese Centrale Bank Besluit van de Europese Centrale Bank betreffende de denominaties, specificaties, reproductie, vervanging en het uit circulatie nemen van eurobankbiljetten, 2003.

IBNS-activeringstechnologieën alle bedreigingen kunnen tegengaan. Bepaalde IBNS werken heel goed bij rip-out/ramraidaanvallen, *in-situ*-aanvallen en gasaanvallen, maar werken niet bij een aanval met vaste explosieven en vice versa. Daarom moet men goed nadenken over de technologie die men kiest.

Een andere bedenking gaat over het type inkt dat men kiest. In België zijn de nationale minimumvereisten voor IBNS (veiligheid, percentage vlekken, niet afwasbaar enz.) vastgelegd, en onafhankelijke tests bevestigen dat het systeem voldoet aan de nationale normen en functioneert volgens de beweringen van de fabrikant. Het is belangrijk om te testen met echte bankbiljetten, omdat er goedkopere soorten inkt op de markt zijn die goed werken met vervalste bankbiljetten, maar niet met echte: dat betekent dat de inkt van echte bankbiljetten gehaald kan worden door ze te wassen. Daarnaast wordt aanbevolen om een forensische marker aan de inkt toe te voegen, zodat bevlekte bankbiljetten gelinkt kunnen worden aan een specifieke plaats delict.

De praktijk toont dat IBNS zeer doeltreffend kan zijn, vooral in combinatie met andere preventieve maatregelen. In 2015 voerde Frankrijk nieuwe wetgeving in, waaronder artikelen betreffende de installatie van IBNS en het gebruik van inkt met uniek DNA. Het is de Franse militaire politie (gendarmerie) die op basis van een risicobeoordeling beslist waar IBNS en andere maatregelen moeten worden ingevoerd. Sinds de nieuwe wetgeving de preventieve en operationele aanpak heeft versterkt, is het aantal aanvallen gedaald van 300 in 2013 tot 50 in 2018.

Een andere techniek in ontwikkeling om de buit onbruikbaar te maken is het gebruik van **lijm**. De doeltreffendheid van lijm is in Nederland bewezen, maar de implementatie- en exploitatiekosten zijn nog hoog. Bovendien kan lijm brandgevaarlijk zijn als het systeem niet wordt geactiveerd vóór een aanval, aangezien de verspreiding van lijmdeeltjes in de lucht een brandbaar mengsel kan geven. Deze methode is nog niet marktrijp, maar zou een oplossing voor de toekomst kunnen zijn.

4.3.2 Het risico vergroten

Een tweede pijler voor de preventie van fysieke aanvallen op geldautomaten is potentiële daders afschrikken door het risico te vergroten dat ze opgespoord en bestraft worden. Naast het risico op lichamelijk letsel bij het gebruik van explosieven voor een aanval, is het grootste risico voor een crimineel een celstraf wanneer hij op heterdaad wordt betrapt of na een onderzoek wordt gevat. Om potentiële daders af te schrikken, moet het risico om gevat en gestraft te worden vergroot worden.

Voor de samenleving is criminelen oppakken en veroordelen natuurlijk ook zeer doeltreffend als preventie als er een straf volgt, zoals we in verschillende landen hebben gezien.

4.3.2.1 *Informatie-uitwisseling*

Cruciaal voor het opsporen en bestraffen van geldautomaatdieven is de uitwisseling van informatie tussen alle partijen in de strijd tegen fysieke aanvallen op geldautomaten, waaronder ordehandhavingsdiensten (politie, openbare aanklager, enz.), overheidsinstanties, zowel fabrikanten van geldautomaten als van beveiligings- en beschermingsmiddelen, beroepsverenigingen, providers van geldautomaten (banken en onafhankelijke providers), beveiligingsbedrijven en alarmcentrales. In het ideale geval gebeurt dit zowel op nationaal als op internationaal niveau.

Een fysieke aanval op een geldautomaat vroegtijdig op het spoor komen is moeilijk. Enkel bij een vrijwel foutloze informatie-uitwisseling op internationaal niveau tussen de ordehandhavingsdiensten en particuliere partners (beveiligingsbedrijven en providers van geldautomaten) is zoiets mogelijk. Een groot aantal indicatoren moet opgevolgd worden, waaronder vroegtijdige waarschuwing tussen ordehandhavingsdiensten over criminele organisaties die onderweg zijn, informatie over ('snelle') voertuigen die bij aanvallen zijn gebruikt, informatie van beveiligingsbedrijven of buurtwachten over verdacht gedrag in de omgeving van de geldautomaat, verdachte transacties die providers van automaten vaststellen, en andere opsporingsmethodes. Andere mogelijke politiemaatregelen voor vroegtijdige opsporing zijn het volgen van gestolen auto's, fabrikanten en verdelers van explosieven en bedrijven die explosieven mogen gebruiken. De inspanningen voor vroegtijdige opsporing zijn veeleisend en geen garantie op succes, zodat interventies van ordehandhavingsdiensten vóór een aanval zeldzaam zijn.

Als vroegtijdige detectie niet mogelijk is, kunnen alarmcentrales snel een waarschuwing uitsturen in geval van een fysieke aanval op een geldautomaat. Om een interventie mogelijk te maken, moeten er nationale regels en protocollen voor snelle communicatie tussen alarmcentrales en ordehandhavingsdiensten afgesproken en vastgelegd worden. In het geval van vroegtijdige opsporing of realtime-informatie zullen ordehandhavingsdiensten altijd de timing en beste kans voor interventie moeten inschatten. Het is erg moeilijk om criminelen op heterdaad te betrappen, en het kan gevaarlijke situaties creëren, omdat sommige criminele organisaties heel gewelddadig zijn en zware wapens gebruiken.

Voor een succesvol onderzoek na een fysieke aanval op een geldautomaat moeten ordehandhavers communiceren met alle belanghebbenden, aangezien elk van hen informatie kan hebben die bijdraagt aan het succes van een onderzoek. Uiteraard is communicatie en samenwerking met de primaire slachtoffers, de banken of andere providers van geldautomaten, noodzakelijk: zij hebben toegang tot gegevens die van belang zijn voor het onderzoek. Voor de provider zal informatie van de ordehandhavingsdiensten helpen om preventieve maatregelen te verbeteren. Bovendien blijken contacten met beroepsverenigingen en fabrikanten nuttig: zij sturen vaak waarschuwingsberichten waarvoor andere geïnteresseerde partijen zich kunnen inschrijven. Fabrikanten van geldautomaten hebben een goed overzicht van de verschillende soorten aanvallen op geldautomaten en de zwakke en sterke punten van de preventieve maatregelen. Zij zijn zeer bereid om de politie te helpen met informatie over de technische aspecten van de geldautomaten en de toegepaste MO.

Grensoverschrijdende samenwerking is cruciaal: landen moeten informatie delen (over verdachten, veroordeelde geldautomaatdieven, MO, verdachte voertuigen, beelden van aanslagen, enz.), niet alleen om het onderzoek te helpen, maar ook opdat verdachten die in een ander land al veroordeeld zijn bestraft kunnen worden voor recidivisme.

Tot slot zou een databank op Europees niveau, die toegankelijk is voor ordehandhavingsdiensten en forensische gegevens bevat (bv. over verschillende soorten IBNS-inkt, tracers en markers of beschermend glas voor geldautomaten), van groot nut kunnen zijn voor speurders en verdachten kunnen linken aan een specifieke plaats delict. Het normaliseren van technologieën op internationaal niveau gaat vaak niet ver genoeg: op de conferentie in januari 2019 gaven deelnemers aan dat een normalisatie van inkt en crimetags op EU-niveau het werk van speurders aanzienlijk zou vereenvoudigen.

4.3.2.2 *Camerabewaking en afluisterapparatuur*

Het beeld en geluid van camerabewakingssystemen en afluisterapparatuur kunnen zowel de opvolging tijdens de aanval (bv. om te voorkomen dat eerstehulpverleners die ter plaatse komen gewond raken) als het daaropvolgende onderzoek (bv. om de daders en hun MO te identificeren) ondersteunen. De camerabeelden kunnen ondersteund worden met beelden van openbare en andere camerabewakingssystemen in de buurt van de geldautomaat en beelden van verkeersradars om een vollediger beeld te geven van de daders en hun MO.

De kwaliteit van camerabeelden laat vaak wel te wensen over, of ze worden slecht opgeslagen. De kwaliteit van de beelden moet goed genoeg zijn om iemand te kunnen identificeren. Ook hier zouden Europese normen voor beveiligingscamera's het onderzoek vergemakkelijken. Omdat daders camera's vaak uitschakelen voor een aanval, kan men ook overwegen om niet-zichtbare camerabewaking of realtime-afluisterapparatuur te plaatsen.

4.3.2.3 *Bestraffing en rehabilitatie van daders*

Consequente en strenge straffen blijken preventief te werken. Een criminele organisatie oppakken heeft een onmiddellijk effect op het aantal aanvallen op geldautomaten. Maar wanneer geldautomaatdieven weer worden vrijgelaten, stijgt het aantal aanvallen vaak ook weer. Conclusie: met korte straffen zijn daders zeer snel weer actief. De minimum- en maximumstraf voor daders die veroordeeld worden verschillen voor elk soort fysieke aanval van lidstaat tot lidstaat. Sommigen geloven dat zwaardere straffen potentiële daders zullen afschrikken. Maar wetenschappelijk onderzoek ([5]) heeft aangetoond dat een zwaardere straf niet noodzakelijk meer afschrikt. Daarom kan het interessant zijn om te kijken naar correctionele (en op de dader gerichte) rehabilitatieprogramma's om de hoge mate van recidive terug te dringen.

4.3.3 Het moeilijker maken

De derde pijler om fysieke aanvallen op geldautomaten te voorkomen bevat acties die het voor een dader moeilijker maken om het misdrijf te plegen.

4.3.3.1 *Een kraakbestendige omgeving creëren*

Als uit de risicobeoordeling (zie hierboven) blijkt dat een geldautomaat zich in een risicovolle omgeving bevindt, moet de geldautomaat worden verplaatst naar een locatie met een laag of middelhoog risico. Dat is zeker het geval als uit de analyse blijkt dat het gebouw zou kunnen instorten als een geldautomaat wordt aangevallen met explosieven. Via nieuwe wetgeving zouden zulke maatregelen in risicogevallen afgedwongen kunnen worden. Het aantal geldautomaten in

([5]) David Weisburd, David P. Farrington and Charlotte Gill, 'Conclusion: What Works in Crime Prevention Revisited', David Weisburd, David P. Farrington and Charlotte Gill, *What works in Crime Prevention and Rehabilitation*. Cambridge: Springer, 2016, 311.

risico-omgevingen moet niet alleen beperkt worden, men moet ook cashloze betalingen aanmoedigen om ervoor te zorgen dat er minder behoefte is aan geldautomaten.

Als de geldautomaat niet verplaatst kan worden, moet een maximum aan veiligheidsmaatregelen genomen worden, zoals: antirampalen, lantaarnpalen en ander straatmeubilair om de toegang tot het gebouw te beperken, systemen om voertuigen te stoppen, goede straatverlichting, meer zichtbaar of discreet toezicht en antidiefstalmaatregelen zoals een systeem om bankbiljetten te vernietigen. Wanneer een geldautomaat wordt aangevallen op een locatie die niet als risicolocatie bekend stond, moet die als dusdanig bestempeld worden en extra beveiligd worden. Met de nieuwe factoren moet rekening gehouden worden in de tool voor risicobeoordeling om die bij te werken. Deze beoordeling van het risico zou op regelmatige basis moeten gebeuren.

4.3.3.2 *De geldautomaten verstevigen*

Fabrikanten van geldautomaten hebben een standaardaanbod van geldautomaten met een aantal veiligheidskenmerken die zijn ingedeeld op basis van de graden van beveiliging van het Europees Comité voor Normalisatie (CEN). Doorgaans hebben geldautomaten een CEN-markering die varieert van de lagere graad CEN1 tot de hoogste graad CEN4. Eigenschappen zoals stevigheid en resistentie tegen aanvallen bepalen de graad. Gasbestendigheid is meestal een optie (CEN-GAS). De standaardmodellen kunnen uitgebreid worden met extra beveiligingsmaatregelen. Meestal installeren derden zulke functies om te voldoen aan lokale wetgeving of om het basismodel aan de behoeften van lokale klanten aan te passen. Extra veiligheidskenmerken zijn onder meer verschillende sensoren om een gasneutralisatiesysteem of IBNS te activeren in het geval van een *in-situ*-aanval of aanval met explosieven, en geavanceerde rolluiken en kluisvergrendelingen om ongeoorloofde toegang te voorkomen wanneer het hoofdrolluik is geforceerd. Voor draagbare, alleenstaande geldautomaten is het belangrijk om verankering te gebruiken die extra beschermt tegen rip-out/ram-raidaanvallen. De geldautomaat kan uitgerust worden met een traceersysteem, zodat speurders de geldautomaat kunnen volgen wanneer die wordt verplaatst voor hij wordt geopend.

4.3.3.3 *Bouwkundige maatregelen*

Bij het plaatsen van een geldautomaat wordt aangeraden om automaten met toegang aan de achterkant te gebruiken. Daders moeten dan het gebouw betreden om toegang te krijgen tot de

achterkant van de automaat en het geld te stelen. Draagbare, alleenstaande geldautomaten zijn het kwetsbaarst. Als er minder van dit soort automaten zijn, vergroot de veiligheid.. Het aantal alleenstaande geldautomaten zou automatisch verminderen, als er verplicht wordt om geldautomaten in een kraakbestendige ruimte te installeren.

4.3.3.4 *Rooksysteem*

Een rookkanon vult een kamer snel met dichte rook, waardoor een indringer niets meer ziet. Zo'n beveiligingsrook maakt het vaak onmogelijk om de aanval uit te voeren. Het systeem zal de indringer op z'n minst vertragen en de politie de tijd geven om in te grijpen. Het rooksysteem is verbonden met het alarmsysteem en kan op twee manieren worden geactiveerd. Het kan automatisch worden geactiveerd door alarmsensoren zoals bewegingsmelders ('s nachts) of sensoren die beweging van de rolluiken detecteren. Het kan ook door een alarmcentrale geactiveerd worden om te vermijden dat er te vaak loos alarm is. Bij geldautomaten in de muur kan het rooksysteem aan de achterkant van de automaat worden geplaatst om die ruimte te vullen met rook en het zicht van indringers te beperken.

Rooksystemen kunnen geldautomaten gericht beveiligen in open ruimtes in benzinestations, supermarkten, enz. Zo wordt niet de hele ruimte met rook gevuld. Beveiliging met rook heeft de meeste kans op succes wanneer de rook uit verschillende hoeken komt of de ruimte achter de geldautomaat vult in het geval
van een ram-raidaanval. Er lopen tests om te zien of er in de geldautomaat zelf rookkanonnen kunnen worden geplaatst, in plaats van in de ruimte waar de geldautomaat zich bevindt. Aan de rook kunnen DNA-markers worden toegevoegd die de indringers en hun kleren bevlekken.

4.3.4 Parallelle maatregelen

Om ervoor te zorgen dat bovenstaande preventieve maatregelen efficiënt en doeltreffend worden ingevoerd, moet een aantal parallelle maatregelen overwogen worden. Die maatregelen zijn essentieel om een holistische preventieve en operationele aanpak van fysieke aanvallen op geldautomaten mogelijk te maken of te versterken.

4.3.4.1 *Wetgeving*

In een aantal landen zijn providers van geldautomaten bij wet verplicht om preventieve maatregelen te nemen. In andere landen zorgen verdragen en overeenkomsten tussen banken en ordehandhavingsinstanties voor een goede aanpak van fysieke aanvallen op geldautomaten. Domeinen waar regelgevende maatregelen kunnen worden overwogen zijn onder andere:

- integratie van preventieve maatregelen;
- wettelijke kaders om samenwerking tussen ordehandhavingsinstanties en publieke en private partners mogelijk te maken;
- aanpassing van de strafmaat als die voor daders van fysieke aanvallen op geldautomaten te laag zou zijn.

Vaak zijn echter alleen banken verplicht om zich aan wetten en akkoorden te houden, en onafhankelijke providers van geldautomaten niet. Het is bekend dat dit vaak een zwak punt is in een wetgevend kader.

Sommige landen voeren geen enkele wetgeving in, maar proberen providers van geldautomaten te overtuigen om preventieve maatregelen te nemen door hen bewust te maken van de gevaren en trends: in landen met een groot aantal onafhankelijke banken blijkt dit bijzonder moeilijk te zijn.

Het is absoluut noodzakelijk om ervoor te zorgen dat de effectieve invoering van preventieve maatregelen wijzigingen aan wet- en regelgeving omvat, zowel op nationaal als op internationaal niveau, die bindend zijn voor alle soorten providers van geldautomaten. In het ideale geval is de wetgeving dezelfde in de hele EU, zodat strenge preventieve maatregelen in één land criminele organisaties niet naar landen met een minder strenge wetgeving duwen.

4.3.4.2 *Mediastrategie*

Een andere belangrijke pijler in de preventieve strategie is een doeltreffende mediastrategie die de verwachtingen en drang van aanvallers moet drukken om over te gaan tot een aanval op een geldautomaat. Er moet benadrukt worden dat de kans op succes klein is en het risico voor de daders groot is; communicatie over de beloning ('buit') of details over de aanval, zoals het soort geldautomaat dat aangevallen is of de MO, moet vermeden worden. Anderzijds moet er uitgebreid bericht worden over arrestaties van verdachten en de straffen na een veroordeling.

4.3.4.3 *Verbeterde samenwerking*

We hebben al uitvoerig gesproken over verbeterde samenwerking en informatie-uitwisseling, maar dat zijn zaken die niet genoeg benadrukt kunnen worden. Operationele informatie-uitwisseling op internationaal niveau is de corebusiness van Europol. Naast informatie-uitwisseling wees de conferentie over preventie op een duidelijke behoefte aan meer multidisciplinaire samenwerking en informatie-uitwisseling op meerdere niveaus tussen alle relevante partijen, waaronder ordehandhavingsinstanties, overheden, fabrikanten van geldautomaten en beveiligings- en beschermingsapparaten, beroepsverenigingen, providers van geldautomaten (banken en onafhankelijke providers), beveiligingsbedrijven en alarmcentrales. Daartoe moeten ook het lokale, nationale en internationale niveau behoren.

4.3.4.4 *Het risico op nevenschade verkleinen*

Bij aanvallen met vaste explosieven laten sommige criminele organisaties materiaal achter. Dit kan leiden tot gevaarlijke situaties voor eerstehulpverleners of burgers (die in de buurt wonen of langskomen). Hun veiligheid moet gegarandeerd worden. Net als in België moeten er protocollen en procedures ontwikkeld en op elkaar afgestemd worden voor eerstehulpverleners (zowel die van de ordehandhaving als van providers van geldautomaten). Een ander goed voorbeeld in die context is dat van Nederland, waar bewakingsbeelden van de aanval gebruikt worden om de situatie in te schatten. Er kunnen met alarmcentrales afspraken gemaakt worden om zulke beelden meteen ter beschikking te stellen.

4.3.4.5 *Sociale preventie*

Criminele organisaties gaan vaak op zoek naar nieuwe jonge krachten. Er zouden projecten opgestart kunnen worden om zulke zoektochten in een vroeg stadium te dwarsbomen. De politie en welzijnswerkers moeten aandachtig zijn voor zulke zaken en zouden kunnen ingrijpen door potentiële daders persoonlijk aan te spreken.

5 Conclusies

De laatste 2 jaar krijgen steeds meer Europese landen af te rekenen met fysieke aanvallen op geldautomaten. Europol en het EUCPN werken samen om de beste maatregelen te verzamelen om deze vorm van criminaliteit te bestrijden en voorkomen.

Een succesvolle aanpak van fysieke aanvallen op geldautomaten combineert operationele en preventieve maatregelen, bij voorkeur binnen een wettelijk kader. Om te voorkomen dat strenge maatregelen in één land criminele organisaties naar meer kwetsbare landen duwen, wordt aangeraden om deze maatregelen op Europees niveau te nemen.

Om deze vorm van criminaliteit te voorkomen en aan te pakken moet een duidelijke strategie worden opgesteld in drie stappen: de beoordeling van de situatie, de ontwikkeling van een preventieve aanpak op basis van de risicobeoordeling en de invoering van de preventieve maatregelen.

De risicobeoordeling voor fysieke aanvallen op geldautomaten moet rekening houden met de kenmerken van de geldautomaat en zijn omgeving, de samenwerking met partners en stakeholders om allianties te smeden in de strijd tegen deze vorm van criminaliteit, en de evaluatie van het preventieve en wettelijke kader. Zodra de situatie is beoordeeld, moet een strategie worden vastgelegd op basis van publiek-private samenwerking en preventieve en operationele tegenmaatregelen. Het doel van preventieve maatregelen is om de intentie en capaciteit van daders om een geldautomaat fysiek aan te vallen te fnuiken. Daarvoor worden drie preventieve actiepijlers voorgesteld: de beloning kleiner maken, het risico vergroten en een aanval moeilijker maken. Parallelle maatregelen moeten de preventieve strategie ondersteunen. Het is bewezen dat het nuttig is om een nationale instantie op te richten die de bevoegdheid heeft om deze noodzakelijke maatregelen op te leggen.

Als **de beloning kleiner wordt**, zal men minder geneigd zijn om zich op deze vorm van criminaliteit toe te leggen. Eén manier om de verwachtingen van daders te temperen, is ervoor zorgen dat er net genoeg geld aanwezig is of bijgevuld wordt als er voor één dag nodig is, of om de (meest kwetsbare) geldautomaten 's nachts leegmaken. Een andere manier is om de buit onbruikbaar te maken en het geld traceerbaar te maken. In dat verband kan het IBNS, dat de bankbiljetten bevlekt en als gestolen markeert, worden toegepast. Deze methode is vooral doeltreffend wanneer het voor criminelen onmogelijk is om dit geld uit te geven of opnieuw in het legale circuit in te voeren. Dat kan wanneer banken en de bevolking bevlekte biljetten niet aanvaarden voor betaling en wanneer er automaten worden geplaatst die bevlekte biljetten herkennen en weigeren. In België en Frankrijk is het in dit

opzicht een kosteneffectieve maatregel geweest om te investeren in infraroodsystemen die biljetten met infraroodmarkering herkent. Als landen een IBNS invoeren, moeten ze goed nadenken welke activeringsmechanismen ze kiezen, wat de minimumvereisten zijn voor het neutraliseren van bankbiljetten en of ze een forensische marker willen toevoegen aan de inkt.

De tweede pijler voor de preventie van fysieke aanvallen op geldautomaten is het afschrikken van potentiële daders door **het risico te vergroten** dat ze opgespoord en bestraft worden. Cruciaal voor het opsporen en bestraffen van geldautomaatdieven is het verzamelen van informatie en de uitwisseling ervan tussen alle partijen, zowel op nationaal als internationaal niveau. Het uitwisselen van goede beelden en geluiden van bewakingssystemen kan helpen om een aanval vroegtijdig op te sporen of met succes te onderzoeken. Om te voorkomen dat bewakingscamera's of afluisterapparatuur worden uitgeschakeld voor de aanval, kan er overwogen worden om niet-zichtbare camerabewaking of realtime-afluisterapparatuur te plaatsen. Het aanleggen van een forensische databank en een normalisatie van technologieën op Europees niveau zou de internationale samenwerking en het werk van speurders ten goede komen. Als daders worden gevat en veroordeeld, kan het interessant zijn om te kijken naar correctionele (en op de dader gerichte) rehabilitatieprogramma's om de hoge mate van recidive terug te dringen.

De derde pijler voor de preventie van fysieke aanvallen op geldautomaten omvat maatregelen die het voor daders **moeilijker maken** om de aanval uit te voeren. Een geldautomaat in een kraakbestendige omgeving met een maximum aan beveiligingsmaatregelen maakt het voor daders moeilijker om een aanval uit te voeren. Bovendien kunnen aan de standaardbescherming van een geldautomaat nog een aantal extra beveiligingsfeatures toegevoegd worden. En bovenop deze maatregelen kan de plaatsing van een rooksysteem de dader afschrikken of de aanval minstens vertragen.

Al deze maatregelen moeten ondersteund worden door een aantal **parallelle maatregelen**, zoals een wettelijk kader dat alle providers van geldautomaten verplicht om de preventieve maatregelen in te voeren, een doeltreffende mediastrategie, verbeterde samenwerking op lokaal, nationaal en internationaal niveau, richtsnoeren voor eerstehulpverleners om het risico op nevenschade te beperken, en een investering in sociale preventie om criminele rekruteringsprocessen te dwarsbomen.

6 Aanbevelingen voor een preventieve aanpak: overzicht

Doeltreffend handelen om fysieke aanvallen op geldautomaten te voorkomen

De situatie inschatten

Een risicoprofiel opstellen van geldautomaten in uw land/regio
Partners en stakeholders in de strijd tegen fysieke aanvallen op geldautomaten identificeren en de samenwerking evalueren
Het wettelijke kader voor de aanpak van fysieke aanvallen op geldautomaten evalueren op nationaal en internationaal niveau.

Een preventieve aanpak ontwikkelen

De (grootste) te dekken risico's en de prioriteiten bepalen
Aan de hand van drie kernpijlers de beste preventieve maatregelen bepalen om deze risico's te dekken.
Parallelle preventieve maatregelen bepalen die nodig zijn om de genomen preventieve maatregelen te ondersteunen

Preventieve maatregelen die genomen kunnen worden om		
De beloning kleiner te maken	Het risico te vergroten	Een aanval te bemoeilijken
– Minder geld beschikbaar maken. o De geldautomaat 's nachts leegmaken. o Vaker/frequenter bijvullen. – De buit onbruikbaar maken. o Intelligente systemen voor de neutralisatie van bankbiljetten (IBNS). o Infraroodmarkering in IBNS-inkt zodat automaten bevlekte biljetten herkennen. o In ontwikkeling: lijm.	– Grensoverschrijdende informatie-uitwisseling om: o een mogelijke aanval op een geldautomaat vroegtijdig of in realtime op te sporen, o de operationele aanpak te versterken, o recidivisten te veroordelen, o forensische gegevens op Europees niveau uit te wisselen. – Bewakingscamera's en afluisterapparatuur. – Resulterende bestraffing en rehabilitatie van daders.	– Een kraakbestendige omgeving creëren. o Kwetsbare geldautomaten verplaatsen. o Beveiligingsmaatregelen: fysieke belemmeringen, toezicht enz. – Geldautomaten versterken met rolluiken die bestand zijn tegen gas of vaste explosieven enz. – Bouwkundige maatregelen zoals automaten met toegang aan de achterkant. – Rooksystemen.

Parallelle maatregelen om de preventieve aanpak te ondersteunen

- Doeltreffende wetgeving, inclusief preventieve maatregelen tegen fysieke aanvallen op geldautomaten, resulterende veroordeling, enz.
- Een doeltreffende mediastrategie die daders ontmoedigt.
- Verbeterde samenwerking tussen alle partijen (publiek, privaat, ordehandhaving) in de strijd tegen fysieke aanvallen op geldautomaten.
- Het risico op nevenschade voor eerstehulpverleners of burgers (bv. omwonenden of voorbijgangers) verkleinen.
- Sociale preventie waarbij wordt verhinderd dat jongeren worden gerekruteerd voor deze vorm van criminaliteit.