Forebyggelse af fysiske angreb på pengeautomater

UDVIKLING AF EN EFFEKTIV TILGANG

EUCPN
EUROPEAN CRIME PREVENTION NETWORK

EMPACT

EUROPOL

“

It is only a matter of time before MOs emerging in one country spread to other countries. This clearly indicates the need for adoption of the preventive and operational measures at the European level with private, public and law-enforcement partners working closely together.

”

ANERKENDELSE

Dette dokument er resultatet af et samarbejde mellem sekretariatet i Den Europæiske Unions Agentur for Retshåndhævelsessamarbejde (Europol) og Det Europæiske Kriminalpræventive Net (EUCPN). Vi vil gerne takke eksperterne i angreb på fysiske angreb på pengeautomater, der har investeret tid og kræfter i at støtte udarbejdelsen af dette anbefalingsdokument. De bidrog ved at deltage i konferencen om forebyggelse af fysiske angreb på pengeautomater (januar 2019, Bruxelles) og levere vigtige oplysninger. Vi vil i særdeleshed gerne takke retshåndhævelsesagenturer fra EU- og ikke-EU-lande (tredjelande), den private sektor, herunder ATM Industry Association (ATMIA), BPost, Centrum voor Criminaliteitspreventie en Veiligheid (CCV), Diebold Nixdorf, the European Association for Secure Transactions Expert Group on ATM and [automatic teller safes] ATS Physical Attacks (EAST EGAP), European Intelligent Cash Protection Association (Euricpa), ING, Febelfin, NCR, Protect, SIOC Banking, Spinnaker, TMD Security og indenrigsministerierne i Belgien, Kroatien, Tyskland og Spanien.

Citation

This brochure was funded by the European Union's Internal Security Fund — Police.

INDHOLD

KONTEKST

På baggrund af et stigende antal fysiske angreb på pengeautomater og antallet af berørte europæiske lande organiserede Det Europæiske Kriminalpræventive Net (EUCPN) og Europol en konference (januar 2019) for at bringe de retshåndhævende myndigheder sammen med offentlige og private partnere for at se nærmere på forebyggelsen af denne type kriminalitet. Dette anbefalingsdokument opsummerer konklusionerne fra denne konference for at øge myndighedernes bevidsthed om fysiske angreb på pengeautomater og forebyggende foranstaltninger.

Et begrænset men alligevel voksende antal lande i Den Europæiske Union er bekymrede over fysiske angreb på pengeautomater. I 2017 blev det økonomiske tab i forbindelse hermed estimeret til over 30 millioner EUR i Europa. Nogle lande oplever fortsat et betydeligt antal fysiske angreb på pengeautomater, andre har oplevet en markant stigning i antallet af disse hændelser de sidste 2 år. Denne form for kriminalitet udvikler sig hurtigt. Nogle lande har haft succes med deres tilgang til at tackle fysiske angreb på pengeautomater og oplevede for nylig et markant fald i angreb. På den anden side oplevede lande, der tidligere ikke var påvirket, en pludselig stigning i fysiske angreb på pengeautomater i 2018 på grund af organiserede kriminelle grupper (OCG'er), der udvider deres territorium. Det er ikke kun banker, der er påvirket. Pengeautomater fra uafhængige udbydere angribes i stigende grad, fordi de ofte er placeret på mere sårbare steder eller placeringer.

Den brede vifte af forskellige metoder (*modi operandi* (MO'er)), som kriminelle bruger til at angribe pengeautomater, kan opdeles i to hovedkategorier: fysiske angreb på pengeautomater og pengeautomat-relaterede svindelangreb (dette inkluderer logiske og malwarerelaterede angreb på pengeautomater). Dette dokument fokuserer på fysiske angreb på pengeautomater: ulovlig indtrængen med fysiske midler i pengeautomater med henblik på at fjerne kontantbeholdningen. Ulovlig indtrængen kan gennemføres ved:

> **brug af sprængstoffer:** tyvene bruger gas eller faste sprængstoffer til fysisk at bryde pengeautomaten op og få adgang til kontanterne;

> **udtagning/rambuktyveri:** tyvene fjerner fysisk pengeautomaten fra installationsmiljøet, ofte ved brug af et avanceret køretøj;

> **angreb på stedet:** tyvene skærer gennem pengeskabet ved hjælp af råkraft, ofte ved brug af brækjern eller skæreværktøjer, såsom vinkelslibere, mukkerter eller autogenbrændere.

01 FAKTORER, DER ER AFGØRENDE FOR RESULTATET AF ET FYSISK ANGREB PÅ EN PENGEAUTOMAT

Der er ikke mange vellykkede angreb på pengeautomater; kun en tredjedel af angrebene lykkes. Men selv når angrebet ikke lykkes, er skaderne (f.eks. fra sprængstoffer) på bygningsstrukturer lige så vigtige at tage i betragtning, da de efterlader et utrygt miljø i nærheden af gerningsstedet for lokale beboere, beredskabspersonel og forbipasserende.

Hvorvidt et fysisk angreb lykkes, afhænger af en række faktorer, herunder; pengeautomatens egenskaber, planlægningen af angrebet samt gerningsmændenes erfaring og know-how.

1. Pengeautomaternes sårbarhed

De mest sårbare pengeautomater er dem, der er placeret udenfor (gennem muren (TTW)) eller dem, der står inde i bygninger. Ved angreb på en indendørs (uafhængig) pengeautomat foretrækker OCG'er pengeautomater beliggende i forretningsejendomme frem for pengeautomater beliggende i banklokaler, hvor der typisk er øget overvågning. Banker har primært pengeautomater placeret i eller uden for en

bankbygning. Bankernes fjernautomater på gaden eller i erhvervsejendomme såsom benzinstationer, supermarkeder, hoteller, kasinoer, lufthavne osv. spiller gradvist en større rolle, efterhånden som bankfilialer lukkes. Uafhængige udbydere driver pengeautomater som en selvstændig service. Deres pengeautomater er ofte placeret i detailforretninger, hoteller og rekreative områder, transportsteder (jernbanestationer, lufthavne osv.), offentlige bygninger og på gaden.

Efterhånden som online banking bliver mere populært, vil mange bankfilialer sandsynligvis lukke de kommende år, hvilket medfører et samlet fald i antallet af pengeautomater[1]. Dette kan dog medføre en stigning i antallet af bankernes fjernautomater og uafhængige udbyderes automater placeret på mere sårbare steder.

2. Planlægning af et angreb på en pengeautomat

Forberedelsen af et angreb kan tage op til flere uger eller endda måneder. De kriminelle skal indsamle de nødvendige **værktøjer og ressourcer,** såsom køretøjer, udstyr og kontaktpunkter. **Køretøjer** er et vigtigt værktøj ved fysiske angreb på pengeautomater; gerningsmændene kører primært i bil til stedet, og efter angrebet flygter de ofte med et hurtigt køretøj. Disse er ofte stjålet, men kan også lejes eller købes (f.eks. via internettet). Størstedelen af det **udstyr**, der anvendes ved fysiske angreb på pengeautomater, er let og lovligt tilgængelig i gængse butikker. Dette sænker yderligere tærsklen for at beskæftige sig med denne type kriminalitet. Det er vanskeligt for de retshåndhævende myndigheder at spore værktøjets oprindelsessted, så risikoen for gerningsmændene er begrænset. OCG'er, der beskæftiger sig med fysiske angreb på pengeautomater på internationalt niveau, har næsten altid kontaktpunkter i mållandet (folk, der bor der i en bestemt periode), eller alternativt kan de bruge en hit-and-run-strategi. Disse kontakter understøtter OCG'erne med logistik, såsom leje af bolig, indkøb af et køretøj eller andet udstyr og undersøgelsesmål. Nogle internationale gerningsmænd overlader logistikken og undersøgelserne fuldstændigt til de lokale kontakter og benytter sig af land- eller lufttransport for at udføre angrebet på pengeautomaten.

OCG'er udfører ofte omfattende **undersøgelser** for at identificere passende mål; vurdere det tidspunkt på dagen, hvor pengeautomaten er fyldt, pengeautomatens omgivelser, pengeautomatens tekniske specifikationer, flugtveje og sikkerhedsforanstaltningerne på stedet, såsom kameraovervågning, alarmsensorer og skodder.

Nogle OCG'er foretager en række handlinger for at **frustrere de retshåndhævende myndigheder og sikkerhedstjenester** før angrebet. De manipulerer med alarmsystemer og offentlig belysning, bruger omledningsteknikker, afspærrer veje eller forsøger at manipulere med de retshåndhævende myndigheders køretøjer.

3. Gerningsmændenes erfaring og know-how

Fysiske angreb på pengeautomater er attraktive for kriminelle, fordi pengene er straks tilgængelige, og der ikke er behov for et omfattende netværk til at sælge stjålne varer. Det er et belejligt alternativ for kriminelle, der allerede er aktive i organiseret berigelseskriminalitet.

OCG'er skal opnå den **påkrævede ekspertise og know-how**, da disse er en afgørende faktor for, hvorvidt et angreb lykkes. Den påkrævede ekspertise og know-how afhænger i høj grad af **angrebstypen**. Udtagning/rambuktyveri og angreb *på stedet* har en simpel MO (primært dristighed og brug af råkraft), så de kræver generelt ikke specifikke færdigheder. Angreb med brændbar gas og angreb med faste sprængstoffer kræver et højere ekspertiseniveau.

Gerningsmændene udviser forskellige **kompetenceniveauer**. På den ene side kan velorganiserede og erfarne grupper udføre et vellykket fysisk angreb på en pengeautomat inden for få minutter. De har kontrol over processen, og de er i stand til at begrænse risikoen for sig selv og dermed også begrænse følgeskaderne. På den anden side mislykkes mindre organiserede og opportunistiske grupper ofte i deres forsøg og kan forårsage betydelig skade på lokalerne og bygningerne i nærheden. Nogle af de mindre organiserede OCG'er antages at vende tilbage til traditionelle aktiviteter i forbindelse med organiseret berigelseskriminalitet, afskrækket af de forebyggende foranstaltninger, de ikke er i stand til at overvinde ved angreb på pengeautomater.

02 BEHOV FOR EN PRÆVENTIV INDSATS

Lande, hvor gerningsmændene oplever begrænset succes med fysiske angreb på pengeautomater, eller hvor antallet af fysiske angreb falder, er et bevis på, at en vellykket tilgang til at modvirke fysiske angreb på pengeautomater består af en kombination af operationelle og præventive foranstaltninger. Da antallet af OCG'er, der beskæftiger sig med denne type kriminalitet, er begrænset, reducerer anholdelser og den efterfølgende straf af OCG-medlemmer markant antallet af angreb. Men når de først er løsladt, genoptager mange pengeautomatrøvere deres aktiviteter igen. Derudover kan en gruppe nogle gange hurtigt erstatte den anholdte gerningsmand. Derfor er der et stærkt behov for præventive foranstaltninger, fortrinsvis forankret i lovgivningen. Erfaringen viser endvidere, at præventive foranstaltninger i ét land kan føre OCG'er mod mere sårbare mål i andre lande. Det er kun et spørgsmål om tid, før MO'er, der opstår i et land, spreder sig til andre lande. Dette viser tydeligt **behovet for vedtagelse af præventive og operationelle foranstaltninger på europæisk niveau** med private, offentlige og retshåndhævende partnere, der arbejder tæt sammen.

03 PRÆVENTIVE FORANSTALTNINGER

For at forhindre og håndtere denne type kriminalitet er der behov for en klar strategi. I dette kapitel giver vi en oversigt over de tre trin, der generelt gennemføres ved fysiske angreb på pengeautomater eller i arbejdet på at forhindre dem.

Først og fremmest **en vurdering af situationen**; der bør fastlægges en risikoprofil for pengeautomaterne og deres omgivelser under hensyntagen til mængden af disponible kontanter (muligt tyvegods), risikoen for sikkerhedsskader og risikoen for personskade. For det andet bør der, baseret på risikovurderingen, udvikles en **præventiv strategi.** Dernæst bør der implementeres **præventive foranstaltninger.**

1.Vurder situationen

OCG'er har tendens til enten at gå efter bestemte typer pengeautomater eller pengeautomater fra specifikke udbydere med funktioner, der letter angrebet. Derfor er det nødvendigt at udføre en grundig vurdering af risikoen for fysiske angreb på pengeautomater, fortrinsvis med øje for hele kontantsikkerhedskæden fra transit til levering til opbevaring i pengeautomaten. For at fastlægge risikoprofilen for hver pengeautomat skal et antal elementer analyseres, herunder følgende.

- Kendetegnene ved stedet og pengeautomatens omgivelser; placering i byen eller på landet, befolkningstæthed, nærhed til politistationer, automatisk nummerpladegenkendelseskameraer (ANPR) i nærheden, overvågningskameraer i nærheden osv.
- Pengeautomatens placering:
  - inde i eller uden for en bygning, i en bankfilial eller i et fjerntliggende lokale (f.eks. erhvervsbygning), indbygget eller knyttet til en bygning,
  - for en fritstående pengeautomat: hvorvidt den er forankret eller ej,
  - for pengeautomater indbygget i eller knyttet til en bygning: hvorvidt der er arkitektoniske svagheder, hvordan kontantopbevaring er organiseret osv.
- Pengeautomattypen.
- Sikkerhedsfunktionerne i pengeautomaten.
- Mængden af kontanter i pengeautomaten.
- Den type fysiske angreb på pengeautomater og MO, man bør forvente, for først at træffe de mest passende præventive foranstaltninger.
- Sikkerheds- og præventive foranstaltninger, der allerede er truffet (intelligente systemer til neutralisering af pengesedler (IBNS), overvågningskameraer, sikkerhedståge (synlighedsreduktion) -system osv.).

Yderligere elementer, der skal evalueres, er samarbejdet med partnere og interessenter samt lovgivningen. Samarbejdet mellem retshåndhævende myndigheder, private og offentlige partnere bør evalueres for at skabe alliancer til bekæmpelse af kriminalitet. Det er muligt, at hver partner besidder interessante oplysninger for at bidrage til vurderingen af situationen. Det lokale politi eller lokale myndigheder er særlig vigtige inden for denne ramme. Lovgivningen skal evalueres med henblik på at etablere en retlig ramme for forebyggelse, træffe obligatoriske forebyggende foranstaltninger, idømmelse af straf for angreb på pengeautomater osv.

2. Udvikling af en præventiv tilgang

Når situationen er blevet vurderet og de vigtigste risikoområder samt styrken og svaghederne i sikkerheden omkring pengeautomater er blevet fastlagt, kan der udvikles en strategi (bygger ofte på offentlig-privat samarbejde) og præventive og operationelle modforanstaltninger kan indføres. Præventive foranstaltninger bør sigte mod at mindske gerningsmændenes intentioner og færdigheder. For at opnå dette foreslår Clarke tre akser med præventive handlinger baseret på tre ud af fem strategier af situationelle kriminalitetsforebyggende foranstaltninger[2]; at mindske fordelene, øge risikoen for gerningsmændene og øge indsatsen for at få adgang til tyvegodset.

Kriminelle opvejer det forventede afkast mod de forbundne risici (f.eks. med et angreb på en pengeautomat). Når chancen for at få en let belønning reduceres og risikoen for gerningsmændene øges, sænkes deres forventninger og ønske om at udføre et fysisk angreb på en pengeautomat. Yderligere foranstaltninger, der øger den nødvendige indsats for at få adgang til en pengeautomat, påvirker gerningsmændenes muligheder. Opportunistiske gerningsmænd, der ofte mislykkes i deres forsøg, holder op med at udføre angreb på pengeautomater. For professionelle gerningsmænd reduceres succesraten, hvilket igen påvirker afkast/risikobalancen.

Parallelle foranstaltninger, såsom en effektiv mediestrategi, tidlig social forebyggelse og foranstaltninger til at reducere risikoen for følgeskader på bygninger og til at garantere sikkerheden for lokale beboere, beredskabspersonel og forbipasserende fuldender den præventive strategi.

Der findes også andre måder at strukturere tilgangen. I Holland anvender myndighederne den såkaldte barriere-model[3]. Denne model identificerer de trin, en kriminel skal tage for at begå en forbrydelse. Den identificerer desuden partnerne og de muligheder, der muliggør forbrydelsen, og det er et nyttigt instrument til at organisere informationsindsamlingsprocessen på kriminalitetsområdet. Ved at identificere alle de trin, der er nødvendige for at udføre et fysisk angreb på en pengeautomat, kan barrierer for at hindre forbrydelsen og de bedste partnere til at opsætte disse barrierer identificeres. Barrieremodellen identificerer også signaler, der skal advare de offentlige og private partnere om fysiske angreb på pengeautomater og signaler, de selv kan udsende for at underrette myndighederne om deres mistanke.

En veludviklet strategi er nødvendig for at afbøde de risici, der følger med at styrke forebyggelsen. Præventive foranstaltninger, der er meget effektive til at afskrække amatører og kopiforbrydere, har somme tider uønskede bivirkninger. Nogle grupper prøver sig frem for at finde sårbare pengeautomater og efterlader et spor af beskadigede pengeautomater. Farligere og mere hensynsløse OCG'er er begyndt at bruge mere voldelige MO'er, såsom at gå fra at bruge gas til faste sprængstoffer i deres angreb.

For at etablere en effektiv række præventive foranstaltninger er det bedste praksis at oprette en national myndighed med beføjelse til at pålægge specifikke foranstaltninger for højrisiko-pengeautomater, baseret på en grundig analyse af situationen. Denne fremgangsmåde har vist sig at være effektiv i Frankrig, især hvis der etableres en retlig ramme, og foranstaltningerne implementeres sammen med operationelle foranstaltninger.

3. Implementering af præventive foranstaltninger

Foranstaltningerne, der blev introduceret i dette kapitel for at forhindre fysiske angreb på pengeautomater, har vist sig at være nyttige i forskellige lande. De er baseret på konklusionerne fra forebyggelseskonferencen og på præventive tiltag, der aktivt fremmes af internationale organisationer, der er aktive inden for pengeautomatsikkerhed. Mange foranstaltninger er velkendte. Flere lande har allerede implementeret en række foranstaltninger med succes. Imidlertid implementeres de foreslåede foranstaltninger kun delvist og forankres ikke i lovgivningen.

Som nævnt ovenfor foreslås tre akser med forebyggende handlinger: reduktion af fordelene, øget risikoen for gerningsmændene og øget den krævede indsats for at få adgang til plyndringen.

3.1 Reducering af fordelene

Reduktion af fordelene ved kriminelle handlinger er den første akse i at forhindre fysiske angreb på pengeautomater. Så længe opfattelsen af 'lette penge' vedvarer, vil kriminelle forsøge sig med denne type kriminalitet. Ved at reducere mængden af disponible kontanter og enten fjerne eller ødelægge kontanterne, reduceres mulighederne for at der er interessant tyvegods. Lavere forventninger reducerer den kriminelles ønske om at beskæftige sig med denne type kriminalitet.

Reduktion af kontantbeløbet

En foranstaltning til at reducere fordelene er at sænke det disponible kontantbeløb i en pengeautomat. Ideelt set bør dette beløb begrænses til det nødvendige beløb for én dags transaktioner. Samarbejde mellem banker kunne sikre omkostningseffektiviteten. I Holland har et antal banker samarbejdet om at oprette et bankuafhængigt netværk af pengeautomater, kaldet 'Geldmaat'. Målet med samarbejdet er at sikre tilgængelighed, overkommelighed og sikkerhed for kontanter. Dette vil sandsynligvis føre til en reduktion i antallet af pengeautomater. Hver hæveautomat vil dog ikke indeholde flere kontanter men genopfyldes i stedet oftere. Antallet af genopfyldninger tilpasses behovet.

Da gerningsmændene for hovedsageligt angriber pengeautomater mellem kl. 03.00 og 04.00, anbefales det på det kraftigste for fritstående pengeautomater (for det meste beliggende i erhvervsbygninger og offentlige lokaler, som er mere sårbare), at tømme pengeautomaten og flytte kontanter til et pengeskab, når dagen er omme. Et advarselsskilt kan informere offentligheden om, at pengeautomaten ikke har kontanter om natten. Den næste dag kan pengeautomaten så genopfyldes uden for offentlighedens skue og med aflåste lokaler. Dette system er implementeret i Frankrig, hvor lovgivningen forpligter detailforhandlere med en fritstående pengeautomat i butikken til at tage kontanter ud om natten og efterlade pengeautomaten åben. For andre pengeautomater kan den indeholdte mængde reduceres ved at øge påfyldningsfrekvensen.

Ødelæg tyvegodset og gør pengene sporbare

Intelligente systemer til neutralisering af pengesedler (IBNS) er en første teknik til at neutralisere fordelene. Disse systemer farver sedlerne med blæk for at markere dem som stjålne. Sporstof og markører kan tilføjes IBNS-blækket. I øjeblikket bruges disse markører hovedsageligt til kriminaltekniske formål, idet de knytter pengesedlen til gerningsstedet og øger gerningsmændenes risiko for at blive pågrebet. Selvom IBNS er en effektiv præventiv foranstaltning, er der visse overvejelser.

Den Europæiske Centralbank refunderer ikke farvede sedler[4] (siden 2003), men en række af de nationale

centralbanker i EU's medlemsstater gør det fortsat. Farvede sedler genindføres også i det juridiske system via kasinoer. IBNS udgør en ekstra forhindring for kriminelle men ville være meget mere effektiv, hvis det var umuligt for kriminelle at bruge farvede pengesedler i EU. For at opnå dette bør farvede sedler ikke accepteres af de nationale centralbanker. Der kan gøres undtagelser for specifikke omstændigheder, f.eks. en seddel, der er farvet under en falsk aktivering. Det er også vigtigt at rådgive befolkningen om ikke at godtage farvede sedler. På den mere langsigtede bane skal pengeseddelacceptorer registrere farvede sedler, og de bør installeres i banker og i erhvervsbygninger som kasinoer, bilvask osv. Registrering af blækket er vanskeligt og dyrt, men en omkostningseffektiv løsning kan være at installere infrarøde systemer, der registrerer sedler farvet med infrarøde markører. Disse systemer har vist sig at være effektive og er en bedste praksis i Belgien og Frankrig. Når sedler med infrarøde markører introduceres i pengeautomaten, accepterer ('sluger') pengeautomaten pengene, men indsætter dem ikke på en konto. Personen, der indfører de farvede pengesedler, bør også registreres.

Der er visse andre overvejelser ved implementering af IBNS-løsninger. Flere producenter leverer en række forskellige IBNS-løsninger med forskellige aktiveringsmekanismer og forskellige typer blæk. En første overvejelse vedrører det faktum, at ikke alle typer IBNS-aktiveringsteknologier kan imødegå alle trusler. Nogle IBNS'er er meget velegnede til udtagnings-/rambuktyverier, angreb *på stedet* og gasangreb, men fungerer ikke i tilfælde af et angreb med faste sprængstoffer eller omvendt. Derfor skal den valgte teknologi overvejes grundigt.

En anden overvejelse er hvilken type blæk, der skal anvendes. I Belgien er der angivet nationale minimumskrav til IBNS (sikkerhed, farvet procentdel, ikke vaskbar osv.), og uafhængige test bekræfter, at systemet opfylder de nationale standarder og fungerer i henhold til producentens påstande. Det er vigtigt at teste rigtige pengesedler, fordi der er billigere blæk på markedet, der fungerer godt med forfalskede/falske pengesedler, men ikke med ægte pengesedler: dette betyder, at blækket kan fjernes fra ægte pengesedler ved at vaske dem. Derudover anbefales det, at der tilsættes en kriminalteknisk markør til blækket, hvilket gør det muligt at undersøge en forbindelse mellem farvede pengesedler og et bestemt gerningssted.

Bedste praksis viser, at IBNS kan være meget effektiv, især i kombination med andre præventive foranstaltninger. I 2015 indførte Frankrig en ny lov med paragraffer om installation af IBNS'er og brug af blæk med unikt DNA. Det er det franske militærpoliti (gendarmerie), der på baggrund af en risikovurdering beslutter, hvor IBNS og andre foranstaltninger skal implementeres. Da den nye lovgivning styrkede den præventive og operationelle tilgang, faldt antallet af angreb fra 300 i 2013 til 50 i 2018.

En anden teknik under udvikling til at ødelægge tyvegodset er brugen af **lim**. Limens effektivitet er blevet påvist i Holland, men implementerings- og driftsomkostninger er store i øjeblikket. Desuden kan lim udgøre en brandfare, hvis systemet ikke aktiveres før et angreb, da spredning af limpartikler i luften kan frembringe en brændbar blanding. Denne metode er endnu ikke klar til markedet, men kan være en løsning i fremtiden.

3.2 Forøg risikoen

En anden akse til forebyggelse af fysiske angreb på pengeautomater er at afskrække potentielle gerningsmænd fra at begå forbrydelser ved at øge risikoen for afsløring og straf. Ud over risikoen for fysisk personskade ved brug af sprængstoffer til angreb på pengeautomater, er fængselsstraf den største risiko for en kriminel, når vedkommende tages på fersk gerning eller som resultat af en efterforskning. For at reducere de potentielle gerningsmænds ønske om at udføre angreb skal risikoen for afsløring og straf øges. For samfundet er pågribelse og retsforfølgelse af kriminelle naturligvis også en særdeles effektiv præventiv metode, hvis der efterfølgende idømmes en straf, som vi har set i flere lande.

Informationsdeling

Nøglen til afsløring og straf af pengeautomatrøvere er udveksling af oplysninger mellem alle interessenter i kampen mod fysiske angreb på pengeautomater, herunder pengeautomatudbydere, retshåndhævende myndigheder (politi, anklager osv.), offentlige myndigheder, producenter af både pengeautomater og sikkerheds- og beskyttelsesanordninger, professionelle sammenslutninger, pengeautomatudbydere (banker og uafhængige udbydere), sikkerhedsfirmaer og alarmcentre. Ideelt set finder dette sted på både nationalt og internationalt plan.

Tidlig afsløring af et kommende fysisk angreb på en pengeautomat er vanskeligt. Kun i tilfælde med næsten fejlfri informationsudveksling på internationalt plan mellem retshåndhævende partnere og private partnere (sikkerhedsfirmaer og pengeautomatudbydere) er tidlig afsløring muligt. En lang række indikatorer skal overvåges, herunder tidlige advarselsmeddelelser mellem de retshåndhævende myndigheder vedrørende OCG'er i bevægelse, information om ('varme') køretøjer, der er blevet brugt i angreb på pengeautomater, oplysninger fra sikkerhedsfirmaer eller lokale vagtværn om mistænkelig opførsel registreret i nærheden af pengeautomaten, mistænkelige transaktioner opdaget af pengeautomatudbydere og andre registreringsmetoder. Andre mulige politiinitiativer til tidlig afsløring er overvågning af stjålne biler, producenter og distributører af sprængstoffer og virksomheder, der har tilladelse til at bruge sprængstoffer. Den nødvendige indsats for at opnå tidlig afsløring er krævende, og der er ingen garanti for succes. Derfor er retshåndhævelsesaktioner før et angreb sjældne.

Hvis tidlig afsløring ikke er muligt, kan alarmcentre hurtigt udsende en advarsel i tilfælde af et fysisk angreb på en pengeautomat. For at muliggøre indgriben skal der aftales og oprettes nationale regler og protokoller til hurtig kommunikation mellem alarmcentre og retshåndhævende myndigheder. I tilfælde af enten tidlig afsløring eller information i realtid skal den retshåndhævende myndighed altid evaluere timingen og den bedste mulighed for at gribe ind. Det er særdeles vanskeligt at pågribe de kriminelle på fersk gerning og det kan føre til farlige situationer, da nogle OCG'er er meget voldelige og bruger tunge våben.

Af hensyn til den vellykkede efterforskning efter et fysisk angreb på en pengeautomat skal de retshåndhævende myndigheder kommunikere med alle interessenter, da en af dem kunne besidde oplysninger, der bidrager til opklaringen af forbrydelsen. Naturligvis er kommunikation og samarbejde med de primære ofre, bankerne eller andre pengeautomatudbydere nødvendige: de har adgang til data, der er vigtige for efterforskningen. For pengeautomatudbyderen vil information fra de retshåndhævende myndigheder bidrage til at forbedre de præventive foranstaltninger. Kontakter med professionelle sammenslutninger og producenter viser sig endvidere at være nyttige: de udsender ofte sikkerhedsadvarsler, som andre interesserede interessenter kan abonnere på. Pengeautomatproducenter har et godt overblik over de forskellige typer angreb på pengeautomater og de tilsvarende styrker og svagheder ved præventive foranstaltninger. De er meget villige til at bidrage med oplysninger til politiet om de tekniske aspekter ved pengeautomaterne og de anvendte MO'er.

Grænseoverskridende samarbejde er vigtigt: lande bør dele information (om mistænkte, dømte pengeautomatrøvere, MO'er, mistænkelige køretøjer, billeder af angreb osv.), ikke kun til støtte for efterforskningen, men også fordi mistænkte, der er dømt i et andet land, kan dømmes for genovertrædelser/recidiv.

Endelig kunne oprettelsen af en database med retstekniske data (f.eks. forskellige typer IBNS-blæk, sporstoffer og markører eller beskyttelsesglas på pengeautomater) på europæisk niveau, der er tilgængelig for retshåndhævende myndigheder, udgøre et vigtigt bidrag til efterforskninger og forbinde mistænkte til et bestemt gerningssted. Standardisering af teknologier på internationalt niveau er ofte utilstrækkelig: i forbindelse med konferencen i januar 2019 gjorde nogle deltagere opmærksom på, at standardisering på EU-niveau af blæk og kriminalitetskoder i høj grad vil kunne lette efterforskningen.

Overvågningskameraer og aflytningsudstyr

Billed- og lyddata fra kameraovervågningssystemer og aflytningsudstyr kan understøtte både realtidsregistrering af et angreb (f.eks. for at forhindre fysisk skade på beredskabspersonel, der ankommer til gerningsstedet) og efterfølgende undersøgelser (f.eks. til at identificere gerningsmændene og deres MO). Billeder fra overvågningskameraer kan kombineres med billeder fra offentlige og andre kameraovervågningssystemer i nærheden af pengeautomater og trafikradaroptagelser for at give et mere komplet billede af gerningsmændene og deres MO.

Billeder fra overvågningskameraer er dog ofte af dårlig kvalitet eller opbevares dårligt. Billederne skal være af tilstrækkelig kvalitet til at muliggøre identificering af en person. Igen ville europæiske standarder for sikkerhedsovervågningskameraer lette efterforskningen. Da gerningsmændene ofte deaktiverer overvågningskameraerne forud for et angreb, kan installation af ikke-synlige overvågningskameraer eller aflytningsudstyr i realtid også overvejes.

Straf og rehabilitering af kriminelle

Konsekvent og alvorlig straf har vist sig at have en præventiv virkning. Når en OCG anholdes, har det en øjeblikkelig effekt på antallet af pengeautomatangreb.

Imidlertid medfører løsladelsen af pengeautomatrøvere ofte også til en ny bølge af angreb. Det betyder, at korte domme medfører, at gerningsmændene meget hurtigt er aktive igen. Minimum- og maksimumstraffen for kriminelle, der er dømt for hver type af fysiske angreb på pengeautomater, varierer mellem medlemsstaterne. Nogle mener, at længere straffe vil afskrække potentielle gerningsmænd. Imidlertid viser videnskabelig forskning[5] at forlængede straffe ikke nødvendigvis forstærker den afskrækkende effekt. Derfor kan det være interessant at se nærmere på fængselsrehabiliterings- (og lovovertræder-baserede) programmer for at reducere den høje recidivisme.

3.3 Forøg indsatsen

Den tredje akse for at forhindre fysiske angreb på pengeautomater omfatter handlinger, der gør det mere krævende for en gerningsmand at udføre den kriminelle handling.

Sikring af et kriminalitetsbestandigt miljø

Hvis risikovurderingen (jf. ovenstående) viser, at en pengeautomat er placeret i et højrisikomiljø, skal den afmonteres og overføres til et område med lav eller mellemhøj risiko. Dette er bestemt tilfældet, hvis analysen viser, at bygningen vil kunne kollapse, hvis en pengeautomat angribes med sprængstoffer. Lovgivning kan implementeres for at håndhæve sådanne foranstaltninger i højrisikotilfælde. Udover at reducere antallet af pengeautomater i højrisikomiljøer, bør kontantløse betalinger tilskyndes med henblik på at reducere behovet for pengeautomater.

Hvis det ikke er muligt at overføre pengeautomaten, skal der træffes flest mulige sikkerhedsforanstaltninger: f.eks. brugen af pullerter, lygtepæle og andet gadeinventar til at begrænse adgangen til bygningen, systemer til standsning af køretøjer, installation af tilstrækkelig gadebelysning, øget synlig eller skjult overvågning og tyverisikringsanordninger såsom et system til neutralisering af pengesedler. Når en pengeautomat angribes på et sted, der ikke er angivet med høj risiko, skal det identificeres som sådan, og der skal træffes ekstra sikkerhedsforanstaltninger. De nye faktorer skal tages med i risikovurderingsværktøjet for at opdatere det. Evalueringen af denne risiko bør være en tilbagevendende aktivitet.

Forstærkning af pengeautomaterne

Pengeautomatproducenter tilbyder et standardudvalg af pengeautomater, der har et antal sikkerhedsfunktioner, der er klassificeret i henhold til Den Europæiske Standardiseringsorganisations (CEN) sikkerhedsklasser. Generelt har pengeautomater en CEN-mærkning, der spænder fra den lavere kvalitet CEN1 til den højeste, CEN4. Funktioner, såsom automatens styrke og modstand mod angreb bestemmer kvaliteten. Gasmodstand tilbydes for det meste som ekstrafunktion (CEN-GAS). Standardmodellerne kan forstærkes med yderligere beskyttelsesforanstaltninger. Normalt installerer tredjeparter disse funktioner for at sikre overholdelse af lokal lovgivning og tilpasning af basismodellen til lokale kunders krav. Ekstra sikkerhedsfunktioner omfatter forskellige sensorer til aktivering af et gasneutraliseringssystem eller IBNS i tilfælde af et angreb *på stedet* eller angreb med sprængstoffer og forbedrede lukkere og bokslåse for at forhindre uautoriseret adgang til pengeskabet, hvor hovedlukkeren kompromitteres. Til bærbare, fritstående pengeautomater er det vigtigt at bruge forankringssystemer, der giver ekstra beskyttelse mod røveri/rambuktyveri. Sporingssystemer kan integreres i pengeautomaten for at støtte efterforskerne, når pengeautomaten transporteres andetsteds forud for åbning.

Arkitektoniske foranstaltninger

Ved installation af en pengeautomat foreslås det at bruge maskiner, hvor adgangen sidder på bagsiden. I dette tilfælde skal gerningsmanden ind i bygningen og opnå adgang til bagsiden af maskinen for at stjæle kontanterne. Bærbare, fritstående pengeautomater er de mest sårbare. En reduktion af antallet af disse pengeautomater vil øge sikkerheden. En forpligtelsen til at installere pengeautomater i et tyverisikret rum reducerer automatisk brugen af fritstående pengeautomater.

Tågesystem

En tågekanon fylder hurtigt et rum med en tæt tåge, så gerningsmanden ikke kan se noget. Denne sikkerhedståge gør det ofte umuligt at udføre angrebet på pengeautomaten. I det mindste bremser systemet gerningsmanden og giver mere tid til, at politiet kan gribe ind. Sikkerhedstågesystemet er tilsluttet alarmsystemet og kan aktiveres på to måder. Det kan udløses automatisk af alarmsensorer, såsom bevægelsessensorer

(om natten) eller lukkermanipuleringssensorer i pengeautomaten. Det kan også aktiveres af et alarmcenter for at undgå for mange falske alarmer. Ved udendørs pengeautomater indbygget i væggen kan tågesystemet installeres på bagsiden af pengeautomaten for at fylde det bagvedliggende rum med tåge og sørge for, at gerningsmændene ikke kan se noget.

Tågesystemer kan give punktbeskyttelse af en pengeautomat placeret i et åbent rum på eksempelvis tankstationer, supermarkeder osv. Derved undgås det, at tågen fylder hele området. Tågebeskyttelsen fungerer bedst, når tågen kommer fra forskellige vinkler, eller når den fylder rummet bag pengeautomaten i tilfælde

af rambuktyveri. Der testes løbende for at se, om tågekanoner kan installeres i selve pengeautomaten i stedet for i det rum, hvor pengeautomaten er placeret. DNA-markører, der farver gerningsmændene og deres tøj, kan tilføjes tågen.

3.4 Parallelle foranstaltninger

For at sikre en effektiv gennemførelse af de ovennævnte præventive foranstaltninger bør et antal parallelle foranstaltninger overvejes. Disse foranstaltninger er nødvendige for at muliggøre eller styrke en holistisk præventiv og operationel tilgang til at håndtere fysiske angreb på pengeautomater.

Lovgivning

I en række lande pålægger lovgivningen pengeautomatudbydere at træffe præventive foranstaltninger. I andre lande sikrer etablering af aftaler mellem banker og retshåndhævende myndigheder en velfungerende tilgang til at håndtere fysiske angreb på pengeautomater. Områder, hvor lovmæssige foranstaltninger kan overvejes, omfatter:

- forankring af præventive foranstaltninger;
- juridiske rammer, der muliggør samarbejde mellem retshåndhævende myndigheder og offentlige og private partnere;
- en gentænkning af strafudmålingen, hvis dommene for gerningsmændene bag fysiske angreb på pengeautomater er for korte.

Imidlertid er det ofte kun bankinstitutter, der er forpligtet til at overholde loven, og uafhængige pengeautomatudbydere er ikke bundet af disse love eller aftaler. Dette er et velkendt svagt punkt i lovgivningen.

Nogle lande implementerer ingen lovgivning men prøver at overtale pengeautomatudbyderne til at træffe præventive foranstaltninger ved at rette deres opmærksomhed på kriminalitetsområder og tendenser: i lande med et stort antal uafhængige banker viser dette sig at være særlig vanskeligt.

Det er altafgørende at sikre, at den effektive implementering af de præventive foranstaltninger inkluderer ændringer i lovgivning og regulering både på nationalt og internationalt niveau, der binder alle typer pengeautomatudbydere. Ideelt bør lovgivningen tilpasses på EU-niveau for at undgå, at stærke præventive foranstaltninger, der er forankret i lovgivningen i et land, fører OCG'erne til andre lande med mindre streng regulering.

Mediestrategi

En anden vigtig akse i den præventive strategi er en veletableret mediestrategi, der sigter mod at mindske forventningerne og ønsket for pengeautomatrøvere om at beskæftige sig med denne form for kriminalitet. Den lave succesrate og de høje risici for gerningsmændene skal understreges; kommunikation om fordelene ('tyvegodset') eller detaljer om pengeautomatangrebet, såsom den berørte pengeautomattype, eller MO skal undgås. På den anden side er det nødvendigt med omfattende kommunikation om anholdelser af mistænkte og den følgende straf efter en dom.

Forbedret samarbejde

Forbedret samarbejde og informationsudveksling er blevet nævnt i vid udstrækning, men kan ikke understreges nok. Operativ informationsudveksling på internationalt niveau er Europols kernevirksomhed. Foruden denne informationsudveksling viste forebyggelseskonferencen det klare behov for øget flerniveau- og tværfagligt samarbejde og informationsdeling mellem alle relevante interessenter, herunder retshåndhævende agenturer, offentlige myndigheder, pengeautomatproducenter samt sikkerheds- og beskyttelsesanordninger, faglige sammenslutninger, pengeautomatudbydere (banker og uafhængige udbydere), sikkerhedsfirmaer og alarmcentre. Dette skal omfatte det lokale, nationale og internationale niveau.

Reduktion af risikoen for følgeskader

I tilfælde af angreb med faste sprængstoffer vil nogle

OCG'er efterlade materiale. Dette kan skabe farlige situationer for beredskabspersonel eller civile (der enten bor i nærheden eller passerer forbi). Deres sikkerhed skal garanteres. Som det er tilfældet i Belgien, skal protokoller og procedurer, der følges af beredskabspersonel (både fra retshåndhævende myndigheder og pengeautomatudbydere), udvikles og tilpasses hinanden. En anden bedste praksis i den forbindelse er eksemplet med Holland, hvor brug af optagelser fra overvågningskameraer fra pengeautomatangrebet bruges til at vurdere situationen. Der kan indgås aftaler med alarmcentre for at gøre disse billeder umiddelbart tilgængelige.

Social forebyggelse

OCG'er er ofte på udkig efter at rekruttere unge. Der kan iværksættes projekter, der hindrer disse rekrutteringsprocesser på et tidligt stadie. Politi og socialarbejdere bør være opmærksomme på disse processer og kan gribe ind ved personligt at nærme sig de potentielle gerningsmænd.

04 KONKLUSION

I de sidste 2 år er antallet af europæiske lande, der er berørt af fysiske angreb på pengeautomater, steget. I den forbindelse har Europol og EUCPN samarbejdet for at indsamle de bedste foranstaltninger til bekæmpelse og forebyggelse af denne form for kriminalitet.

En vellykket tilgang til at modvirke fysiske angreb på pengeautomater består af en kombination af operationelle og præventive foranstaltninger, fortrinsvis forankret i lovgivningen. For at undgå, at stærke foranstaltninger i et land leder OCG'er mod mere sårbare lande, anbefales det at vedtage disse foranstaltninger på europæisk niveau.

For at forebygge og tackle denne type kriminalitet bør der fastlægges en klar strategi i tre trin: vurdering af situationen, udvikling af en præventiv tilgang baseret på risikovurderingen og gennemførelsen af de præventive foranstaltninger.

Risikovurderingen for fysiske angreb på pengeautomater skal omfatte pengeautomatens egenskaber og omgivelser, samarbejdet med partnere og interessenter for at skabe alliancer til bekæmpelse af denne type kriminalitet og evaluering af den præventive og juridiske ramme. Når situationen er vurderet, bør der etableres en strategi, der bygger på offentligt-privat samarbejde samt præventive og operationelle modforanstaltninger. Formålet med de præventive foranstaltninger er at mindske gerningsmændenes intentioner og færdigheder til at udføre et fysisk angreb på en pengeautomat. For at opnå dette foreslås tre akser med præventive handlinger: reducer fordelene, forøg risikoen og forøg indsatsen. Parallelle foranstaltninger bør fuldføre den præventive strategi. Oprettelsen af en national myndighed med beføjelse til at pålægge disse nødvendige foranstaltninger er bedste praksis.

Ved at **reducere fordelene** mindskes den kriminelles ønske om at beskæftige sig med denne form for kriminalitet. En foranstaltning til at mindske den kriminelles forventninger er at reducere kontantbeløbet i pengeautomaten ved at begrænse den genopfyldte kontantbeholdning til det, der svarer til 1 dags transaktioner, eller tømme de (mest sårbare) pengeautomater om natten. En anden metode er at ødelægge tyvegodset og gøre pengene sporbare. I denne sammenhæng kan IBNS, der farver sedlerne og markerer dem som stjålet, anvendes. Denne metode er mest effektiv, når det er umuligt for de kriminelle at bruge disse penge eller at genindføre disse sedler i det lovlige kontantsystem. Dette kan opnås ved at banker og offentligheden ikke godtager farvede sedler til betaling og ved at installere seddelacceptorer, der kan registrere og afvise farvede sedler. I den forbindelse har investeringen i infrarøde systemer, der registrerer farvede sedler med infrarøde markører vist sig at være en omkostningseffektiv løsning i Belgien og Frankrig. Ved installation af IBNS bør de enkelte lande grundigt overveje de valgte aktiveringsmekanismer, minimumskravene til neutralisering af pengesedlerne og tilføjelse af en retsteknisk markør i blækket.

En anden akse til forebyggelse af fysiske angreb på pengeautomater er at afskrække potentielle gerningsmænd fra at begå forbrydelser ved at **øge risikoen** for afsløring og straf. Nøglen til afsløring og straf af pengeautomatrøvere er indsamling og udveksling af oplysninger mellem alle interessenter, både på nationalt og internationalt plan. Informationsudveksling af billeder fra overvågningskameraer af høj kvalitet og lyddata

kan øge chancerne for tidlig afsløring og en vellykket efterforskning. For at undgå at overvågningskameraer eller aflytningsudstyr deaktiveres før angrebet, kan det overvejes at installere ikke-synlige overvågningskameraer eller aflytningsudstyr i realtid. Oprettelsen af en kriminalteknisk database og standardisering af teknologier på europæisk niveau kunne i høj grad lette det internationale samarbejde og efterforskninger. Hvis gerningsmændene pågribes og idømmes en straf, kan det være interessant at se nærmere på fængselsrehabiliterings- (og lovovertræder-baserede) programmer for at reducere den høje recidivisme.

Den tredje akse for at forhindre fysiske angreb på pengeautomater omfatter foranstaltninger til at **øge den indsats**, som en gerningsmand må yde for at udføre den kriminelle handling. Hvis en pengeautomat installeres i et kriminalitetsbestandigt miljø med flest mulige sikkerhedsforanstaltninger, vil det gøre det mere krævende for de kriminelle at angribe en pengeautomat. Desuden kan standardbeskyttelsen af pengeautomater forbedres med en række ekstra sikkerhedsfunktioner. Oven på disse foranstaltninger kan installationen af et tågesystem afskrække gerningsmanden eller i det mindste bremse angrebet.

Et antal **parallelle foranstaltninger** vil styrke de ovennævnte foranstaltninger, såsom at skabe en juridisk ramme, der forpligter alle pengeautomatudbydere at implementere de præventive foranstaltninger, udvikle en veletableret mediestrategi, det forbedrede samarbejde på lokalt, nationalt og internationalt niveau, retningslinjer for beredskabspersonel for at mindske risikoen for følgeskader og investeringer i social forebyggelse for at underminere de kriminelle rekrutteringsprocesser.

Factsheet

ANBEFALINGER TIL EN PRÆVENTIV TILGANG: OVERSIGT

Udvikl et effektivt svar for at forhindre fysiske angreb på pengeautomater

Vurder situationen

> Vurder risikoprofilen for pengeautomater i dit land/ region

> Identificer partnere og interessenter i kampen mod fysiske angreb på pengeautomater og evaluer samarbejdet

> Evaluer de juridiske rammer for at tackle fysiske angreb på pengeautomater på nationalt og internationalt niveau.

Udvikl en præventiv tilgang

> Fastlæg de (primære) risici, der skal afdækkes, og prioriteterne

> Fastlæg de bedste præventive foranstaltninger til at afdække disse risici ved at overveje tre hovedakser.

> Fastlæg de parallelle præventive foranstaltninger, der er nødvendige for at styrke de præventive foranstaltninger, der er truffet.

Præventive foranstaltninger, der kan træffes:

01

Reducering af fordelene

> Reducer kontantbeløbet
  - Sørg for, at pengeautomaten er tom om natten.
  - Forøg antallet/hyppigheden af genopfyldninger.
> Ødelæg tyvegodset.
  - Intelligente systemer til neutralisering af pengesedler (IBNS)
  - Infrarøde markører i IBNS-blæk til at registrere farvede sedler fra seddelacceptorer.
  - Under udvikling: lim.

02

Forøg risikoen

> Grænseoverskridende informationsdeling for:
  - tidlig afsløring eller afsløring i realtid af et muligt angreb på en pengeautomat,
  - styrkelse af den operationelle tilgang,
  - idømmelse af straf til serieforbrydere,
  - udveksling af retstekniske data på europæisk niveau.
> Overvågningskameraer og aflytningsudstyr.
> Straf og rehabilitering af kriminelle.

03

Forøg indsatsen

> Sikring af et kriminalitetsbestandigt miljø.
  - Overførsel af pengeautomater i højrisikoområder til en ny placering.
  - Sikkerhedsforanstaltninger: fysiske forhindringer, overvågning osv.
> Forstærkning af pengeautomater med lukkere, modstandsdygtige over for gas eller faste sprængstoffer osv.
> Arkitektoniske foranstaltninger såsom maskiner, hvor adgangen sidder på bagsiden
> Sikkerhedstågesystemer.

Parallel measures to strenghten the preventive approach

> Effektiv lovgivning, herunder præventive foranstaltninger mod fysiske angreb på pengeautomater, efterfølgende straf osv.

> Effektiv mediestrategi, der afskrækker gerningsmændene.

> Forbedret samarbejde mellem alle interessenter (offentlige, private, retshåndhævende myndigheder) i kampen mod fysiske angreb på pengeautomater.

> Reducer risikoen for følgeskader på beredskabspersonel eller civile (f.eks. dem, der bor i nærheden eller passerer forbi).

> Social forebyggelse, hvor det undgås, at unge rekrutteres til at begå (denne type) kriminalitet.

ENDNOTES

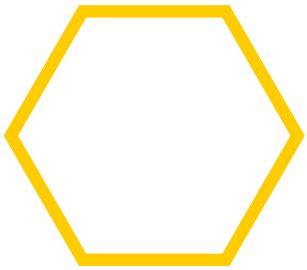
1 Willem Pieter de Groen, Zachary Kilhoffer & Roberto Musmeci, *The future of EU ATM markets: impacts of digitalisation and pricing policies on business models*, CEPS-rapport, 2018

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

3 Centrum voor Criminaliteitspreventie, barrieremodellen, www.barrieremodellen.nl

4 European Central Bank decision of the European Central Bank, The denominations, specifications, reproduction, exchange and withdrawal of euro banknotes, 2003.

5 David Weisburd, David P. Farrington & 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.



CONTACT DETAILS

EUCPN Secretariat
Phone: +32 2 557 33 30
Email: eucpn@ibz.eu
Website: www.eucpn.org, www.europol.europa.eu

TWITTER.COM/EUCPN
FACEBOOK.COM/EUCPN
LINKEDIN.COM/COMPANY/EUCPN