Füüsiliste panga-automaadirünnakute ennetamine

TÕHUSA LÄHENEMISE VÄLJATÖÖTAMINE

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.

”

KINNITUS

See dokument on koostatud koostöös Euroopa Liidu Õiguskaitsekoostöö Ametiga (Europol)ja Euroopa kriminaalpreventsiooni võrgustiku (EUCPN) sekretariaadiga. Avaldame tänu füüsiliste pangaautomaadirünnakute ekspertidele, kes toetasid selle soovitusliku dokumendi loomist oma aja ja vaevaga. Nad andsid oma panuse, osaledes füüsiliste pangaautomaadirünnakute ennetamisekonverentsil (2019. aasta jaanuaris Brüsselis) ja andes elutähtsat teavet. Eelkõige soovime avaldada tänu EL-i ja mitte-EL-i („kolmandate“) riikide korrakaitseasutustele, erasektorile, sealhulgas Pangaautomaatide Tööstusharu Ühendus (ATMIA), BPost, Centrum voor Criminaliteitspreventie en Veiligheid(CCV), Diebold Nixdorf, Euroopa Turvaliste Tehingute Ühenduse ekspertrühm pangaautomaatide ja seifiautomaatide (ATS) füüsiliste rünnakute osas (EAST EGAP), Euroopa Intelligentse Sularahakaitse Ühendus (Euricpa), ING, Febelfin, NCR, Protect,SIOC Banking, Spinnaker, TMD Security ning Belgia, Horvaatia, Saksamaa ja Hispaania siseministeeriumid.

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

SISUKORD

KONTEKST

Seoses füüsiliste pangaautomaadirünnakute ja neist mõjutatud Euroopa riikide arvu kasvuga on Euroopa kriminaalpreventsiooni võrgustik (EUCPN) ja Europol korraldanud konverentsi (2019. aasta jaanuaris), tuues kokku korrakaitse ning avaliku jaerasektori partnerid, et käsitleda selle kuriteoliigi ennetustööd. Käesolev soovituslik dokument võtab kokku sellel konverentsil tehtud järeldused, et tõsta ametivõimude teadlikkust füüsilistest pangaautomaadirünnakutest ja nende ennetamise meetmetest.

Piiratud, kuid kasvavas arvus Euroopa Liidu riikides esineb probleem füüsiliste pangaautomaadirünnakutega. 2017. aastal oli neist tulenev rahaline kahju Euroopas hinnanguliselt üle 30 miljoni euro. Mõnedes riikides toimub jätkuvalt olulisel hulgal füüsilisi rünnakuid pangaautomaatidele, teistes on taoliste intsidentide arv viimase kahe aastaga oluliselt kasvanud. See kuriteovaldkond areneb kiiresti. Mõnede riikide lähenemine füüsiliste pangaautomaadirünnakute ennetamisele on olnud edukas ja viimasel ajal on rünnakud neis riikides oluliselt vähenenud. Teisest küljest on 2018. aastal tekkinud füüsiliste pangaautomaadirünnakute äkiline kasv riikides, kus neid varem ei esinenud, kuna kuritegelikud organisatsioonid on oma tegevuse neile territooriumidele laiendanud. Probleemist on mõjutatud mitte ainult pangad, vaid ka sõltumatute teenusepakkujate pangaautomaate rünnatakse aina enam, sest need asuvad sageli haavatavamates ruumides või kohtades.

Laia valiku erinevaid meetodeid (modusoperandi – MO)), mida kurjategijad pangaautomaatide ründamiseks kasutavad, saab jagada kahte suurde kategooriasse: füüsilised pangaautomaadirünnakud ja pangaautomaadiga seotud pettusrünnakud (nende hulgas on pangaautomaatide rünnakud arvutiloogika ja pahavara kaudu). Käesolev dokument keskendub füüsilistele pangaautomaadirünnakutele: füüsiliste vahenditega toime pandud ja jõudu kasutav sissetung pangaautomaatidesse, et eemaldada neist sularaha. Jõudukasutav sissetung võib toimuda järgmistel meetoditel:

> **lõhkeainetega rünnakud:** ründajad kasutavad gaasilisi või tahkeid lõhkeaineid, et saada füüsiliselt juurdepääs pangaautomaadi seifi sisemusele ja seal olevale sularahale;

> **väljarebimisega/rammimisega rünnakud:** ründajad eemaldavad pangaautomaadi füüsiliselt selle paigalduskohast, sageli kasutades selleks võimsat sõidukit;

> **kohapealsed rünnakud:** ründajad lõikavad seifi jõuga lahti, sageli kasutades lõike- või purustusvahendeid nagu nurklõikurid, sepavasarad või oksüatsetüleenpõletid.

01 FÜÜSILISE PANGAAUTOMAADIRÜNNAKU EDUKUSE MÄÄRAVAD TEGURID

Pangaautomaadirünnakute edukuse määr on madal; vaid kolmandik rünnakutest on edukad. Kuid isegi kui rünnak ebaõnnestub, on hoone konstruktsioonile tekitatud kahjustused (nt lõhkeainete tõttu) sama tähtsad, jättes endast kuriteopaiga lähedusse ebaturvalise keskkonna nii kohalikele elanikele, kiirreageerijatele kui möödujatele.

Füüsilise rünnaku edukus sõltub mitmetest teguritest, nende hulgas: pangaautomaadi omadused, pangaautomaadirünnaku korraldus ning kurjategijate kogemuste ja teadmiste tase.

1. Pangaautomaatide haavatavus

Kõige haavatavamad pangaautomaadid on need, mis asuvad hoone välisküljel (läbi seinapaigaldusega) või seisavad hoone sees. Hoonesisest (eraldi seisvat) pangaautomaati rünnates eelistavad kuritegelikud organisatsioonid ärihoonetes asuvaid pangaautomaate pankades asuvatele, sest pankades on valve tavaliselt tugevam. Pangad rakendavad peamiselt pangaautomaate, mis asuvad pangahoones või selle välisküljel. Kaugpanganduse asukohad tänavatel või kaupmeeste äriruumides nagu bensiinijaamades, supermarketites, hotellides, kasiinodes, lennujaamades jm on muutumas järg-järgult olulisemaks, sedamööda

kuidas pangakontoreid suletakse. Sõltumatud teenusepakkujad käitavad pangaautomaate eraldiseisva teenusena. Nende pangaautomaadid asuvad sageli jaekauplustes, majutus- ja vabaajakohtades, transpordikeskustes (raudteejaamad, lennujaamad jne), avalikes hoonetes ja tänavatel.

Kuna internetipangandus muutub üha populaarsemaks, siis suletakse eelseisvatel aastatel tõenäoliselt veel palju pangakontoreid, mis toob kaasa pangaautomaatide arvu üldise vähenemise[1]. Samas võib see tuua kaasa haavatavamates kohtades asuvate kaugpanganduse pangautomaatide ja sõltumatute teenusepakkujate pangaautomaatide arvu suurenemise.

2. Pangaautomaadirünnaku ettevalmistused

Rünnakuettevalmistused võivad võtta kuni mitu nädalat või koguni mitu kuud. Kurjategijatelon vaja koguda kokku vajalikud **tööriistad ja ressursid** nagu sõidukid, varustus ja kontaktpunktid. **Sõidukid** on füüsilistepangaautomaadirünnakute puhul esmatähtis vahend; kurjategijad liiguvadpeamiselt autoga ja pärast rünnakut põgenevad nad kõige sagedamini, kasutadeskiireid sõidukeid. Sageli need varastatakse, aga võidakse ka rentida või osta (nt Interneti kaudu). Enamik füüsiliste pangaautomaadirünnakute jaoks vajaminevast **varustusest** on tavapoodides kergesti ja legaalselt saadaval. See langetab veelgi läve sellesse kuritegevuse valdkonda sisenemisel. Korrakaitsel on raske tööriista päritolu tuvastada, seepärast on kurjategija riskid piiratud. Füüsiliste pangaautomaadirünnakutega rahvusvahelisel tasandil tegelevatel kuritegelikel organisatsioonidel on peaaegu alati sihtriigis kontaktpunktid (isikud, kes elavad seal juba mõnda aega), teise variandina aga võivad nad kasutada ka tee-ja-põgene taktikat. Need kontaktid toetavad kuritegelikke organisatsioone logistikaga nagu majutuse üürimine, sõiduki ja muu varustuse hankimine ning sihtmärkide väljaotsimine. Mõned rahvusvahelised kurjategijad jätavad logistika ja sihtmärkide otsimise täielikult kohalike kontaktide hooleks ja reisivad vaid maantee- või lennutranspordiga kohale, et pangaautomaadirünnak toime panna.

Sageli tegelevad kuritegelikud organisatsioonid ulatusliku **sihtmärkide** otsimisega, et tuvastada sellised, mis neile sobivad; nad hindavad pangaautomaadi täitmise kellaaega, pangaautomaadiümbrust, tehnilisi näitajaid, põgenemisteid ja kehtestatud turvameetmeid nagukaameravalve (CCTV), andursignalisatsioon ja luugid.

Mõned kuritegelikud organisatsioonid rakendavad enne rünnaku sooritamist rea toiminguid, et **korrakaitset ja turvateenistusi häirida**. Nad rikuvad alarmsüsteeme ja tänavavalgustust, kasutavad diversioonitaktikaid, blokeerivad teid või püüavad korrakaitse sõidukeid rikkuda.

3. Kurjategijate kogemused ja teadmised

Füüsilised pangaautomaadirünnakud on kurjategijatele atraktiivsed, sest raha on kohe saadaval ja puudub vajadus ulatusliku võrgustiku järele, et varastatud kaubad maha müüa. See on mugav alternatiiv kurjategijatele, kes on juba varavastases kuritegevuses organiseeritud.

Kuritegelikel organisatsioonidel on vaja koguda **vajalikud ekspert- ja oskusteadmised**, sest need on teguriks, mis määrab rünnaku edu või ebaõnnestumise. Vajalikud ekspert- ja oskusteadmised sõltuvad tugevasti **rünnaku tüübist**. Väljarebimisega/rammimisegaja *kohapealsed* rünnakud toimuvad lihtsate meetoditega (peamiselt nahaalsuse ja nüri jõu abil), seega need enamasti erioskusi ei vaja. Süttiva gaasi ja tahkete lõhkeainetega rünnakud seevastu nõuavad kõrgemat oskuste taset.

Ründajatel on erinevad **pädevuse tasemed**. Ühelpool seisavad hästi organiseeritud ja kogenud grupid, kes suudavad eduka füüsilise pangaautomaadirünnaku minutitega lõpule viia. Nad hoiavad kogu protsessi kontrolli all ja suudavad oma riskid viia miinimumini, viies sellega miinimumini ka kaasnevad kahjustused. Teisel pool aga on vähem organiseeritud ja oportunistlikud grupid, kelle püüdlused sageli ebaõnnestuvad ja kes võivad selle käigus ruumidele ja naabruskonna hoonetelegi olulisi purustusi tekitada. Usutavasti naasevad mõned vähem organiseeritud kuritegelikud grupid traditsiooniliste varavastaste kuritegude juurde, sest heituvad ennetavatest meetmetest, mida nad pangaautomaate rünnates ületada ei suuda.

02 VAJADUS ENNETAVA LÄHENEMISE JÄRELE

Riigid, kus füüsiliste pangaautomaadirünnakute edukuse määr on madal või kus selliste rünnakute arv langeb, tõestavad, et edukas lähenemine füüsiliste pangaautomaadirünnakute vastases võitluses ühendab endas operatiivsed ja ennetavad meetmed. Kuna selles kuritegude valdkonnas tegutsevate kuritegelike organisatsioonide arv onpiiratud, vähendab nende liikmete vahistamine ja järgnev karistamine oluliselt rünnakute arvu. Samas jätkavad paljud pangaautomaadi ründajad vabanedes oma tegevust. Samuti suudab grupeering vahel oma arreteeritud liikme kiiresti asendada. Seepärast esineb tugev vajadus ennetavate meetmete järele, eelistatavalt kaasates need seadusandlusse. Lisaks näitavad kogemused, et ühes riigis rakendatavad ennetusmeetmed võivad suunata kuritegelikud organisatsioonid teistes riikides asuvate haavatavamate sihtmärkide poole. On ainult aja küsimus, millal ühes riigis tekkivad kuriteomeetodid levivad ka teistesse riikidesse. See näitab selgesti **vajadust rakendada kogu Euroopa tasandil** ennetavaid ja operatiivseid meetmeid nii erasektori, avaliku sektori kui korrakaitse partnerite tihedas koostöös.

03 ENNETUS

Seda tüüpi kuritegude ennetamiseks ja nende vastu võitlemiseks on vaja selget strateegiat. Selles peatükis anname ülevaate kolmest sammust, mida tavaliselt rakendatakse, kui puututakse kokku füüsiliste pangaautomaadirünnakutega või valmistutakse neid ennetama.

Esiteks eelkõige **olukorra hindamine**; pangaautomaatide ja nende ümbruse kohta tuleb koostada riskiprofiil, võttes arvesse saadaoleva sularaha hulga (võimaliku saagi), kaasnevate kahjustuste riski ja isikutele kehavigastuste tekitamise riski. Teiseks tuleb riskihinnangu alusel koostada **ennetav strateegia**. Ja lõpuks tuleb ellu viia **ennetavad meetmed**.

1. Olukorra hindamine

Kuritegelikud organisatsioonid kipuvad valima sihtmärkideks kas konkreetset tüüpi pangaautomaate või konkreetsete tarnijate pangaautomaate, millel on pangaautomaadirünnakuid soodustavad omadused. Seepärast on vaja läbi viia põhjalik riskihindamine seoses füüsiliste pangaautomaadirünnakutega, eelistatavalt kaasates kogu sularaha turva-ahela alates transiidist kuni kohaletoomiseni ja pangaautomaati panekuni. Iga pangaautomaadi kohta riskiprofiili koostamiseks tuleb analüüsida rida elemente, nende hulgas alljärgnevad.

- Pangaautomaadi asukoha ja ümbruse iseloomulikud jooned; kas tegemist on linnalise või maapiirkonnaga; rahvastiku tihedus, politseijaoskondade lähedus, automaatse numbrituvastusega liikluskaamerad naabruskonnas, valvekaamerad ümbruskonnas jne.
- Pangaautomaadi asukoht:
  - hoone sees või välisküljel, pangakontoris või kaugpanganduse asukohas (nt äripinnal), hoonekonstruktsioonidesse sisse ehitatud või nende külge kinnitatud,
  - eraldiseisvate pangaautomaatide korral: kas nad on ankurdatud või mitte,
  - hoone konstruktsioonidesse sisse ehitatud või nende külge kinnitatud pangaautomaatide korral: kas on arhitektuurilisi nõrku kohti, kuidas on sularaha hoidmine korraldatud jne.
- Pangaautomaadi tüüp.
- Pangaautomaadi sisse ehitatud turvasfunktsioonid.
- Pangaautomaadis oleva sularaha hulk.
- Füüsiliste pangaautomaadirünnakute tüüp ja kuriteomeetodid, et rakendada kõige sobivamad ennetusmeetmed esimesena.
- Turva- ja ennetusmeetmed, mis on juba rakendatud (intelligentsed pangatähtede neutraliseerimissüsteemid (IBNS), valvekaamerad, turvaudu (nähtavuse vähendamise) süsteem jne).

Veel tuleb hinnata selliseid elemente nagu koostöö määr partnerite ja sidusrühmadega ning seadusandlus. Hinnata tuleb koostööd korrakaitse, erasektori ja avaliku sektori partnerite vahel, et luua liidud kuritegevuse vastu võitlemiseks. On võimalik, et igal partneril on huvitavat teavet, mida olukorra hindamisse anda. Kohalik politsei ja kohalikud ametkonnad on selles raamistikus eriti olulised. Hinnata tuleb seadusandlust, et panna paika ennetustöö õigusraamistik, rakendades kohustuslikke ennetusmeetmeid, mõista pangaautomaadirünnakute toimepanijad süüdi jne.

2. Ennetava lähenemise väljatöötamine

Kui olukord on hinnatud ja pangaautomaadi turvalisusega seonduvad peamised riskid ning tugevad ja nõrgad küljed on välja selgitatud, siis saab välja töötada strateegia (sageli põhineb see avaliku ja erasektori koostööl) ning panna paika ennetavad ja operatiivsed vastumeetmed. Ennetavad meetmed peaksid olema suunatud kurjategijate innukuse ja võimekuse vähendamisele. Selle saavutamiseks pakutakse välja kolm ennetavate tegevuste telge, mis põhinevad kolmel viiest situatsioonilise kuriteo ennetuse strateegiast, mille väljatöötajaks on Clarke[2] : kurjategijate tulu vähendamine, nende riski suurendamine ja saagile juurdepääsemiseks vajaliku pingutuse suurendamine.

Kurjategijad tasakaalustavad omavahel oodatavat tulu ja sellega kaasnevaid riske (nt pangaautomaadirünnaku korral). Kurjategijate jaoks hõlpsa tasu saamise võimaluste vähendamine ja riski suurendamine alandab nende ootusi ja soovi panna toime füüsiline pangaautomaadirünnak. Täiendavad meetmed, mis suurendavad pangaautomaadile juurdepääsu saamiseks vajalikku pingutust, mõjutavad kurjategija võimekust. Oportunistlikud kurjategijad, kes sageli oma katsetes ebaõnnestuvad, lõpetavad pangaautomaadirünnakute toimepanemise. Professionaalsete pangaautomaadiründajate puhul väheneb nende edukuse määr, mis mõjutab taas nende tulu/riskibilanssi.

Lisaks sellele täiendavad ennetusstrateegiat paralleelsed meetmed, nagu tõhus meediastrateegia, varajane sotsiaalne ennetus ja meetmed, et vähendada hoonetele kaasnevate kahjustuste ohtu ning tagada kohalike elanike, kiirreageerijate ja möödujate ohutus.

On ka teisi võimalikke viise lähenemise struktureerimiseks. Madalmaades kohaldavad ametiasutused nn barjäärimudelit[3]. See mudel näitab samme, mida kurjategija peab kuriteo toimepanemiseks tegema. Samuti tuvastab see partnerid ja võimalused, mis võimaldavad kuritegevust, ning see on kasulik vahend, mille abil korraldada teabekogumisprotsessi selle kuriteovaldkonna kohta. Tuvastades iga sammu, mis on vajalik füüsilise pangaautomaadirünnaku toimepanemiseks, on võimalik tuvastada kuriteo takistamise tõkked ja parimad partnerid nende tõkete püstitamiseks. Barjäärimudel tuvastab ka signaalid, mis teavitavad avalikke ja erasektori partnereid füüsilistest pangaautomaadirünnakutest, ning signaalid, millega nad saavad ise ametiasutusi oma kahtlustest teavitada.

Selleks et leevendada riske, mis kaasnevad ennetuse tugevdamisega, on vaja hästi väljatöötatud strateegiat. Ennetavatel meetmetel, mis on väga tõhusad amatööride ja jäljendajate tõrjumisel, on mõnikord soovimatuid mõjusid. Mõned grupid pöörduvad katseeksituse meetodite poole, et leida haavatavaid pangaautomaate, jättes endast maha rea kahjustatud pangaautomaate. Ohtlikumadja halastamatumad kuritegelikud organisatsioonid hakkavad kasutamavägivaldsemaid meetodeid, näiteks lähevad oma rünnakutes üle gaasilt tahketelelõhkeainetele.

Tõhusate ennetusmeetmete kogumi loomiseks on parim praktika luua riiklik asutus, millel on õigus kehtestada eriabinõusid kõrge riskiga pangaautomaatides, lähtudes olukorra põhjalikust analüüsist. See lähenemisviis on osutunud tõhusaks Prantsusmaal, eriti kui kehtestatakse õiguslik raamistik ja rakendatakse meetmeid koos operatiivmeetmetega.

3. Ennetusmeetmete rakendamine

Käesolevas peatükis kehtestatud meetmed füüsiliste pangaautomaadirünnakute vältimiseks on tõestanud oma kasulikkust erinevates riikides. Need põhinevad ennetuskonverentsi järeldustel ja ennetavatel meetmetel, mida aktiivselt edendavad rahvusvahelised organisatsioonid, kes tegutsevad pangaautomaatide turvalisuse vallas. Paljud meetmed on hästi tuntud. Mitmed riigid on paljusid neist meetmetest juba edukalt rakendanud. Kuid sageli rakendatakse kavandatavaid meetmeid ainult osaliselt ja need ei sisaldu õigusaktides.

Nagu eespool mainitud, pakutakse välja kolm ennetavate meetmete telge: vähendada kurjategijate tulusid, suurendada nende riski ja suurendada saagile juurdepääsemiseks vajalikku pingutust.

3.1 Tulude vähendamine

Kuritegudest saadava tulu vähendamine on esimene telg füüsiliste pangaautomaadirünnakute ennetamisel. Seni kuni püsib arusaam „lihtsast rahast“, tegelevad kurjategijad seda tüüpi kuritegevusega. Saadaoleva sularaha hulga alandamine ja kas sularaha eemaldamine või hävitamine vähendab võimalusi, et kurjategijad saaksid sealt huvitavat saaki. Vähenenud ootused alandavad kurjategija soovi tegeleda seda tüüpi kuritegevusega.

Sularahahulga vähendamine

Üks meede tasu vähendamiseks on vähendada pangaautomaadis saadaolevat rahasummat. Ideaalis peaks see summa piirduma vajaliku summaga ainult üheks kauplemispäevaks. Pankadevaheline koostöö võib tagada kulutasuvuse. Madalmaades tegi mitu panka koostööd, et luua pankadest sõltumatu pangaautomaatide võrk, mida nimetatakse „Geldmaat“. Koostöö eesmärk on tagada sularaha saadavalolek, kättesaadavus, taskukohasus ja turvalisus. See toob tõenäoliselt kaasa pangaautomaatide arvu vähenemise. Samas ei sisalda iga pangaautomaat rohkem sularaha, vaid seda täiendatakse sagedamini. Täitmiste arv kohandatakse vastavalt vajadusele.

Kuna seaduserikkujad ründavad pangaautomaate enamasti ajavahemikus 03:00 kuni 04:00, on tungivalt soovitatav eraldiseisvate pangaautomaatide puhul (enamasti asuvad need äripindadel ja avalikes hoonetes, mis on haavatavamad) tühjendada pangaautomaat päeva lõpus ja viia sularaha ohutusse kohta. Hoiatussilt võib avalikkusele teatada, et pangaautomaadis ei ole öösel sularaha. Järgmisel päeval tuleb pangaautomaat täiendada väljaspool klientide nägemisulatust ja hoida sel ajal ruumid lukus. Seda süsteemi rakendatakse Prantsusmaal, kus õigusaktid kohustavad jaemüüjaid, kellel on kaupluses eraldiseisev pangaautomaat, võtma raha ööseks välja ja jätma pangaautomaadi avatuks. Muude pangaautomaatide puhul võib neis hoitavaid summasid vähendada, suurendades täitmissagedust.

Saagi rikkumine ja raha jälitatavaks muutmine

Intelligentsed pangatähtede neutraliseerimissüsteemid (IBNS) on esimene meetod saagi rikkumiseks. Need süsteemid määrivad pangatähti tindiga, et märkida need varastatuks. IBNS-tindile saab lisada jälgitavaid aineid ja markereid. Hetkel kasutatakse neid markereid peamiselt kohtueksperti isi eesmärkidel, sidudes pangatähe kuriteopaigaga ja suurendades kurjategija riski vahele jääda. Kuigil BNS on tõhus ennetav meede, tuleb siiski mõnda aspekti kaaluda.

Euroopa Keskpank ei hüvita määritud pangatähti[4] (alates 2003. aastast), kuid mitmed ELi liikmesriikide keskpangad siiski teevad seda. Määritud pangatähed tuuakse seaduslikku süsteemi uuesti sisse ka kasiinode kaudu. IBNS loob kurjategijatele lisatakistuse, kuid oleks palju tõhusam, kui kurjategijatel on võimatu määritud pangatähti EL-is kasutada. Selle saavutamiseks ei tohiks riikide keskpangad määritud pangatähti vastu võtta. Erandeid võib teha konkreetsete asjaolude puhul, nagu

näiteks valehäire ajal määritud pangatähed. Samuti on oluline soovitada elanikkonnal määritud pangatähti mitte aktsepteerida. Pikaajalisemas perspektiivis peaksid pangatähtede loendamis- ja tuvastusseadmed määritud pangatähti tuvastama ning need seadmed tuleks paigaldada pankadesse ja äripindadele nagu kasiinod, autopesulad jne. Tindi tuvastamine on raske ja kallis, kuid kulutõhusaks lahenduseks võiks olla infrapunasüsteemide paigaldamine, mis tuvastavad infrapunamarkeritega määritud pangatähti. Need süsteemid on oma tõhusust tõestanud ning on Belgias ja Prantsusmaal parimaks praktikaks. Infrapunamarkeritega pangatähtede sisestamisel pangaautomaat aktsepteerib raha („neelab“ selle), kuid ei krediteeri seda kontole. Registreerida tuleks ka määritud pangatähti sisestav isik.

On veel mõningaid aspekte, mida BNS-lahenduste paigaldamisel tuleks kaaluda. Mitmed tootjad pakuvad erinevaid BNS-lahendusi, millel on erinevad aktiveerimismehhanismid ja erinevat tüüpi tint. Esimene aspekt puudutab asjaolu, et mitte igat liiki BNS-tehnoloogia ei suuda võidelda kõigi ohtude vastu. Mõned IBNS-is töötavad väga hästi väljarebimisega/rammimisega rünnakute, *kohapealsete* ja gaasiga rünnakute puhul, kuid ei toimi tahke lõhkeainega rünnaku korral või vastupidi. Seetõttu tuleks tehnoloogia valikut hästi kaaluda.

Teine aspekt, mida arvesse võtta, on tindi tüübi valik. Belgias on kehtestatud IBNS-ide riiklikud miinimumnõuded (ohutus, määritud pangatähtede protsent, mittepestavus jne) ning sõltumatud katsed tõendavad, et süsteem vastab riiklikele standarditele ja toimib vastavalt tootja väidetele. On oluline kontrollida reaalseid pangatähti, sest turul on odavamaid tinte, mis toimivad hästi võltsitud pangatähtedega, kuid mitte tõelistega: see tähendab, et tinti saab ehtsatelt pangatähtedelt pesemise teel eemaldada. Lisaks sellele on soovitatav tindile lisada kohtueksperti võimaldav marker, mis laseb uurida seost määritud rahatähtede ja konkreetse kuriteopaiga vahel.

Parim tava näitab, et IBNS võib olla väga tõhus, eriti kombinatsioonis teiste ennetusmeetmetega. 2015. aastal kehtestas Prantsusmaa uued õigusaktid, sealhulgas artiklid IBNS-ide paigaldamise ja unikaalse DNA-ga tindi kasutamise kohta. Prantsuse sõjaväepolitsei (gendarmerie) on see, kes riskihinnangu põhjal otsustab, kus IBNS-i ja muid meetmeid tuleb rakendada. Kuna uued õigusaktid tugevdasid ennetavat ja operatiivset lähenemisviisi, vähenesrünnakute arv 300-lt 2013. aastal 50-le 2018. aastal.

Veel üks arendatav tehnika saagi rikkumiseks on **liimi** kasutamine. Liimi efektiivsust tõestati Hollandis, kuid selle rakendamise ja kasutamise kulud on hetkel suured. Liim võib olla tuleohtlik, kui süsteem ei aktiveeru enne rünnakut, kuna liimiosakeste hajumine õhus võib tekitada põleva segu. See meetod ei ole veel turuvalmis, kuid võib olla lahendus tulevikuks.

3.2 Riski suurendamine

Teine telg füüsiliste pangaautomaadirünnakute ennetamiseks on heidutada potentsiaalseid kurjategijaid kuritegusid toime panemast, suurendades nende avastamis- ja karistusohtu. Lisaks füüsilise vigastuse riskile, kui pangaautomaadirünnakus kasutatakse lõhkeainet, on kurjategija peamine risk vanglakaristus, kui ta tabatakse kas teolt või pärast uurimist. Selleks, et alandada potentsiaalsete kurjategijate tegutsemissoovi, tuleb suurendada nende avastamise ja karistamise riski. Ühiskonna jaoks on kurjategijate püüdmine ja süüdimõistmine muidugi samuti väga tõhus ennetusmeetod, eeldusel et sellele järgneb karistamine, nagu oleme näinud mitmes riigis.

Teabe jagamine

Pangaautomaadi ründajate tuvastamise ja karistamise võti on teabevahetus füüsiliste pangaautomaadirünnakute vastase võitluse kõigi sidusrühmade vahel, kaasa arvatud pangaautomaatide tootjad, korrakaitseasutused (politsei,prokuratuur jne), riigiasutused, nii pangaautomaatide kui ka turva- jakaitseseadmete tootjad, pangaautomaatide tarnijad, kutseliidud, (pangad ja sõltumatud tarnijad), turvaettevõtted ja häirekeskused. Ideaalis toimuks see nii riiklikul kui rahvusvahelisel tasandil.

Eelseisva füüsilise pangaautomaadirünnaku varajane avastamine on raske. Ainult juhul, kui toimub peaaegu veatu infovahetus rahvusvahelisel tasandil korrakaitsepartnerite ja erasektori partnerite (turvafirmade ja pangaautomaaditarnijate) vahel, on varajane avastamine võimalik. Tuleb jälgida paljusid erinevaid näitajaid, sealhulgas korrakaitseasutuste vahelisi varajase hoiatamise teateid, et kuritegelikud organisatsioonid on liikvel, teavet („kuumade“) sõidukite kohta, mida kasutati pangaautomaadirünnakutes, turvaettevõtetelt või naabrivalvetelt saadud teavet pangaautomaadi ümbrusestuvastatud kahtlase käitumise kohta, pangaautomaaditarnijate tuvastatud kahtlastetehingute kohta ja muud avastamismeetodid. Muud võimalikud

politseimeetmed varajaseks avastamiseks on varastatud autode, lõhkematerjalide tootjate ja levitajate ning lõhkeainete kasutamiseks luba omavate ettevõtete jälgimine. Varajaseks avastamiseks vajalikud jõupingutused on ressursinõudlikud ega taga edu, mistõttu korrakaitsealased sekkumised enne rünnakut on haruldased.

Kui varajane avastamine ei ole võimalik, saavad häirekeskused füüsilise pangaautomaadirünnaku korral anda kiiresti hoiatuse. Sekkumise võimaldamiseks tuleb kokku leppida ja kehtestada riiklikud eeskirjad ja protokollid häirekeskuste ning korrakaitseorganite vaheliseks kiireks suhtluseks. Varajase avastamise või reaalajas teabe saamise korral tuleb korrakaitseorganitel alati hinnata sekkumise ajastust ja parimat võimalust sekkuda. Kurjategijate teolt tabamine on väga raske ja võib viia ohtlike olukordadeni, sest mõned kuritegelikud organisatsioonid on väga vägivaldsed ja kasutavad raskerelvi.

Edukaks uurimiseks pärast füüsilise pangaautomaadirünnaku toimumist peavad korrakaitseametnikud suhtlema kõigi sidusrühmadega, sest igaüks neist võib omada teavet, mis aitab uurimisele kaasa. Loomulikult on vajalik teabevahetus ja koostöö peamiste ohvrite, pankade või muude pangaautomaaditarnijatega: neil on juurdepääs andmetele, mis on uurimise jaoks olulised. Pangaautomaatide tarnija jaoks aitab korrakaitselt saadav teave parandada ennetusmeetmeid. Lisaks osutuvad kasulikuks kontaktid kutseliitude ja tootjatega: sageli saadavad nad turvateateid, mille saajateks saavad end registreerida ka teised huvitatud sidusrühmad. Pangaautomaatide tootjatel on hea ülevaade erinevate pangaautomaadirünnakute tüüpidest ning neile vastavatest ennetavate meetmete nõrkustest ja tugevustest. Nad on väga valmis toetama politseid teabega pangaautomaatide tehniliste aspektide ja kasutatud kuriteomeetodite kohta.

Piiriülene koostöö on oluline: riigid peaksid jagama teavet (kahtlustatavate, süüdimõistetud pangaautomaadiründajate, kuriteomeetodite, kahtlaste sõidukite, rünnakust salvestatud piltide jms kohta) ning seda mitte ainult uurimisetoetuseks, vaid ka seetõttu, et ühes riigis süüdimõistetud kahtlusaluseid saab teises riigis korduvkuritegude/retsidivismi eest karistada.

Ja lõpetuseks: Euroopa tasandil andmebaasi loomine, mis on korrakaitseorganitele kättesaadav ja mis sisaldab kohtueksperti isi andmeid (nt erinevat tüüpi IBNS-i tintide, jälitusainete ja markerite või pangaautomaadi kaitseklaaside kohta), võiks anda uurimisele tugeva toetuse ja siduda kahtlusalused konkreetse kuriteopaigaga. Tehnoloogiate standardimine rahvusvahelisel tasandil on sageli ebapiisav: 2019. aasta jaanuari konverentsil mainisid osalejad, et tindi ja kuriteomarkerite EL-i tasandil standardimine võib oluliselt uurimist hõlbustada.

Valvekaamerad ja pealtkuulamisseadmed

Valvekaameratest ja pealtkuulamisseadmetest saadud pildi- ja heliandmed võivad toetada rünnaku reaalajas tuvastamist (nt et vältida kuriteopaigale saabuvate kiirreageerijate füüsilisi vigastusi) ja järgnevaid uurimisi (nt kurjategijate ja nende meetodite tuvastamiseks). Kohapealsete valvekaamerate kujutisi saab kombineerida avalikest ja muudest pangaautomaadi ümbruses asuvatest valvekaameratest, samuti liiklusradaritest saadud kaadritega, et anda terviklikum pilt kurjategijatest ja nende meetoditest.

Samas on valvekaamerate kujutised sageli halva kvaliteediga või halvasti salvestatud. Kujutised peaksid olema piisavalt kvaliteetsed, et võimaldada isiku tuvastamist. Jällegi hõlbustaks uurimist turvakaameratele Euroopa standardite kehtestamine. Ja veel: kuna kurjategijad rikuvad sageli enne rünnakut valvekaamerad, võiks kaaluda ka peidetud valvekaamerate või reaalajas pealtkuulamisseadmete paigaldamist.

Karistus ja õigusrikkuja rehabilitatsioon

Järjekindlal ja rängal karistusel on tõestatult ennetav mõju. Kuritegeliku organisatsiooni vahistamine mõjutab kohe pangaautomaadirünnakute arvu. Samas viib pangaautomaadiründajate vanglast vabanemine aga sageli rünnakute uue tõusuni. See tähendab, et lühikesed karistused viivad selleni, et kurjategijad muutuvad väga kiiresti taas aktiivseks. Füüsilise pangaautomaadirünnaku tüübi eest kurjategijatele mõistetavad miinimum- ja maksimumkaristused on liikmesriigiti erinevad. Mõned usuvad, et rängemad karistused heidutavad potentsiaalseid kurjategijaid. Samas näitavad teadusuuringud[5], et karistuste raskusastme suurendamine ei suurenda tingimata nende hoiatavat mõju. Seetõttu võib olla huvitav uurida paranduslikke (ja õigusrikkujatele keskenduvaid) rehabilitatsiooniprogramme, et vähendada kõrget retsidivismi.

3.3 Pingutuse suurendamine

Füüsiliste pangaautomaadirünnakute ennetamise kolmas telg sisaldab meetmeid, mis muudavad kuriteo toimepanemise raskemaks.

Kuritegevust takistava keskkonna tagamine

Kui riskihindamine (vt eelpool) näitab, et pangaautomaat asub kõrge riskiga keskkonnas, tuleks asukoht likvideerida ja pangaautomaat madala või keskmise riskiga alasse üle viia. Asi onkindlasti nii, kui analüüs näitab, et hoone võib kokku kukkuda, kui pangaautomaati rünnatakse lõhkeaineid kasutades. Kõrge riskitasemega juhtudel selliste meetmete kohustuslikuks muutmiseks võib rakendada õigusakte. Lisaks kõrge riskiga keskkondades asuvate pangaautomaatide arvu vähendamisele tuleks innustada sularahata maksete tegemist, et vähendada vajadust pangaautomaatide järele.

Kui pangaautomaati ei ole võimalik üle viia, tuleks võtta maksimaalselt turvameetmeid: nt kasutada rammimisvastaseid pollareid, tänavavalgustusposte ja muud tänavamööblit, et piirata ligipääsu hoonele, samuti sõidukite peatamise süsteeme, paigaldada piisav tänavavalgustus, suurem avalik või varjatud valveningiga vargusvastased seadmed, nagu näiteks pangatähtede rikkumise süsteem. Kui rünnak toimub kohas, mida ei tuvastatud kõrge riskina, tuleks see lugeda kõrgeks riskiks ja lisada täiendavad turvameetmed. Uued tegurid tuleks riskihindamise vahendis selle ajakohastamiseks arvesse võtta. Selline riski ümberhindamine peaks olema korduv toiming.

Pangaautomaatide tugevdamine

Pangaautomaatide tootjad pakuvad standardset valikut pangaautomaate, millel on mitmeid turvaelemente, mis on hinnatud vastavalt Euroopa Standardikomitee (CEN) turvanõuetele. Üldiselt on pangaautomaatidel CEN-märgistus vahemikus madalaimast klassist CEN1-st kuni kõrgeima, CEN4-ni. Märgistuse taseme määravad sellised omadused nagu korpuse tugevus ja vastupidavus rünnaku suhtes. Gaasikindlust pakutakse enamasti valikuna (CEN-GAS). Standardmudeleid saab täiendada täiendavate kaitsemeetmetega. Tavaliselt paigaldavad neid meetmeid kolmandad isikud, et tagada vastavus kohalikele õigusaktidele ja kohandada põhimudelit kohalike klientide nõuetele. Täiendavad turvaelemendid hõlmavad mitmesuguseid andureid gaasi neutraliseerimissüsteemi või IBNS-i aktiveerimiseks lõhkeainetega kohapealse rünnaku korral ning täiustatud luuke ja seifilukke, et vältida volitamata juurdepääsu seifile *olukorras,* kus pealuuk on rikutud. Kaasaskantavate, eraldiseisvate pangaautomaatide puhul on oluline kasutada ankurdussüsteeme, mis pakuvad lisakaitset väljarebimisega/rammimisega rünnakute vastu. Pangaautomaati saab kaasata jälgimissüsteeme, et toetada uurijaid, kui pangaautomaat transporditakse enne avamist teise asukohta.

Arhitektuurilised meetmed

Pangaautomaadi paigaldamisel soovitatakse kasutada tagant juurdepääsuga seadet. Sel juhul peab kurjategija sisenema hoonesse ja saama ligipääsu seadme tagaosale, et varastada sularaha. Kaasaskantavad, eraldiseisvad pangaautomaadid on kõige haavatavamad. Nende pangaautomaatide arvu vähendaminesuurendaks turvalisust. Kohustus paigaldada pangaautomaadid sissemurdmiskindlasse ruumi vähendaks automaatselt eraldiseisvate pangaautomaatide kasutamist.

Udusüsteem

Udukahur täidab ruumi kiiresti tiheda uduga, nii et sissetungija ei näe midagi. See turvaudu teeb pangaautomaadirünnaku läbiviimise sageli võimatuks. Halvimal juhul see süsteem vähemalt aeglustab kurjategijat, jättes aega politsei sekkumiseks. Turvaudusüsteem on ühendatud häiresüsteemiga ja seda saab aktiveerida kahel viisil. Selle võivad automaatselt käivitada alarmiandurid, näiteks liikumisandurid (öösel) või pangaautomaadi luugiga manipuleerimise andurid. Selle saab aktiveerida ka häirekeskus, et vältida liiga palju valehäireid. Läbi seina paigaldatud ja hoone välisküljel paiknevate pangaautomaatide korral saab udusüsteemi rakendada pangaautomaadi tagaküljel, et täita ruum seadme taga uduga ja viia kurjategijate jaoks nähtavus nullini.

Udusüsteemidega saab korraldada ka pangaautomaadi kohtkaitset bensiinijaamades, supermarketites jm avatud ruumides. Sellega välditakse kogu ala uduga täitmist. Udukaitse on kõige edukam siis, kui udu tuleb erinevatest nurkadest või kui see täidab rammimisega rünnakute puhul pangaautomaadi

taguse ruumi. Praegu tehakse katseid, et näha, kas udukahureid saab paigaldada pangaautomaati endasse, mitte ruumi, kus pangaautomaat asub. Udule võib lisada

DNA markereid, mis määrivad kurjategijaid ja nende riideid.

3.4 Paralleelsed meetmed

Eespool nimetatud ennetusmeetmete tõhusa ja toimiva rakendamise tagamiseks tuleb kaaluda mitmeid paralleelseid meetmeid. Need meetmed on hädavajalikud, et võimaldada või tugevdada terviklikku ennetavat ja operatiivset lähenemisviisi, et võidelda füüsiliste pangaautomaadirünnakute vastu.

Seadusandlus

Mitmes riigis kohustab seadusandlus pangaautomaatide tarnijaid võtma kasutusele ennetavaid meetmeid. Teistes riikides tagab pankade ja korrakaitseasutuste vaheliste paktide ja lepete kehtestamine hästitoimiva lähenemisviisi, et füüsiliste pangaautomaadirünnakute vastu võidelda. Valdkonnad, kus võib kaaluda regulatiivseid meetmeid, on järgmised:

- ennetavate meetmete kaasamine;
- õigusraamistikud, mis võimaldavad koostööd korrakaitse ning avaliku ja erasektori partnerite vahel;
- karistuse määramise ümberhindamine, kui kurjategijatele füüsiliste pangaautomaadirünnakute eest mõistetud karistused on liiga väikesed.

Kuid sageli peavad neid seadusi ja kokkuleppeid täitma ainult pangandusasutused ning sõltumatutele pangaautomaatide tarnijatele need ei ole siduvad. See on reguleerivates õigusraamistikes ühine nõrk punkt.

Mõned riigid ei rakenda mingeid eeskirju, vaid püüavad veenda pangaautomaatide tarnijaid võtma kasutusele ennetavaid meetmeid, tõstes nende teadlikkust kuritegevuse valdkondadest ja suundumustest; riikides, kus on suur hulk sõltumatuid panku, osutub see eriti raskeks.

On hädavajalik tagada, et ennetusmeetmete tõhus rakendamine hõlmaks muudatusi õigusaktides ja eeskirjades nii riiklikul kui ka rahvusvahelisel tasandil, mis on siduvad kõigile pangaautomaatide tarnijate tüüpidele. Ideaalis tuleks õigusaktid viia vastavusse kogu EL-i tasandil, et vältida seda, et üheriigi seadusandluses sisalduvad tugevad ennetusmeetmed suunavad kuritegelikud organisatsioonid teistesse riikidesse, kus on vähem ranged eeskirjad.

Meediastrateegia

Teine oluline telg ennetavas strateegias on hästi väljakujunenud meediastrateegia, mille eesmärgiks on vähendada pangaautomaadiründajate ootusi ja soovi nende kuritegudega tegeleda. Tuleb rõhutada madalaid edukuse määrasid ja kurjategijate suuri riske, avaldada teavet kuritegeliku tulu („saak“) kohta või üksikasju pangaautomaadirünnaku kohta, nagu näiteks rünnatud pangaautomaadi tüüp või ebaõnnestunud kuriteomeetod. Teisest küljest on vajalik ulatuslik meediakajastus kahtlusaluste vahistamiste ja nende süüdimõistmisele järgneva karistuse kohta.

Tõhustatud koostöö

Tõhustatud koostööd ja teabevahetust on juba ulatuslikult mainitud, kuid selle tähtsust pole võimalik üle hinnata. Operatiivne teabevahetus rahvusvahelisel tasandil on Europoli põhitegevus. Lisaks sellele teabevahetusele näitas ennetuskonverents selget vajadust suurendada valdkonnaülest ning mitmetasandilist koostööd ja teabevahetust kõigi asjaomaste sidusrühmade vahel, nende hulgas korrakaitseasutused, riigiasutused, pangaautomaatide ning turva- ja kaitseseadmete tootjad, kutseliidud, pangaautomaatide tarnijad (pangad ja sõltumatud pakkujad), turvaettevõtted ja häirekeskused. See peab hõlmama kohalikku, riiklikku ja rahvusvahelist tasandit.

Kaasnevate kahjude riski vähendamine

Tahke lõhkeainega rünnakute korral jätavad mõned kuritegelikud organisatsioonid lõhkeainet maha. See võib tekitada ohtlikke olukordi kiirreageerijatele või tsiviilisikutele (kes elavad naabruses või mööduvad sealt). Nende ohutus tuleb tagada. Nagu Belgias, tuleb välja töötada reeglid ja protseduurid, mida kiirreageerijad peavad järgima (nii korrakaitse kui ka pangaautomaatide tarnijate poolsed), ning need tuleb omavahel vastavusse viia. Teine hea tava selles kontekstis on Madalmaade näide, kus olukorra hindamiseks kasutatakse valvekaamerate salvestisi pangaautomaadirünnakust. Häirekeskustega saab sõlmida kokkuleppeid, et teha need pildid kohe kättesaadavaks.

Sotsiaalne ennetus

Sageli otsivad kuritegelikud organisatsioonid noori inimesi, keda värvata. Võib luua projekte, et neid

värbamisprotsesse varases etapis takistada. Politsei-ja sotsiaaltöötajad peaksid olema nende protsesside suhtes tähelepanelikud ja sekkuma, lähenedes võimalikele kurjategijatele isiklikult.

04 KOKKUVÕTTEKS

Viimase kahe aasta jooksul suurenes füüsilistest pangaautomaadirünnakutest mõjutatud Euroopa riikide arv. Sellega seoses tegid Europol ja EUCPN koostööd, et koguda parimaid meetmeid selle kuritegevuse liigiga võitlemiseks ja selle ennetamiseks.

Edukas lähenemisviis füüsiliste pangaautomaadirünnakute vastu võitlemiseks koosneb operatiivsete ja ennetavate meetmete kombinatsioonist, mis on eelistatavalt kaasatud seadusandlikku raamistikku. Vältimaks seda, et tugevad meetmed ühes riigis suunavad kuritegelikke organisatsioone haavatavamatesse riikidesse, on soovitatav rakendada need meetmed kogu Euroopa tasandil.

Seda liiki kuritegevuse ennetamiseks ja selle vastu võitlemiseks tuleks kehtestada selge strateegia kolmes etapis: olukorra hindamine, riskihindamisel põhineva ennetava lähenemisviisi väljatöötamine ja ennetusmeetmete rakendamine.

Füüsiliste pangaautomaadirünnakute riski hindamine peaks hõlmama pangaautomaadi ja selle ümbruse omadusi, koostööd partnerite ja sidusrühmadega, et luua selle kuritegevusega võitlemiseks liidud, ning ennetus- ja õigusraamistiku hindamist. Pärast olukorra hindamist tuleks kehtestada avaliku ja erasektori koostööle tuginev strateegia ning ennetavad ja operatiivsed vastumeetmed. Ennetavate meetmete eesmärk on vähendada kurjategija soovi ja võimekust panna toime füüsiline pangaautomaadirünnak. Selle saavutamiseks pakutakse välja kolm ennetavate meetmete telge: vähendada kurjategijate tulu, suurendada nende riski ja suurendada nende vajalikku pingutust. Ennetava strateegia täiendamiseks tuleks rakendada paralleelsed meetmed. Parim praktika on luua riiklik asutus, millel on õigus neid vajalikke meetmeid kehtestada.

Tulu vähendades väheneb kurjategija soov sellelaadseid kuritegusid toime panna. Üks meede, et vähendada kurjategijate ootusi, on sularahasumma vähendamine pangaautomaadis, piirates sularaha lisamist nii, et see on piisav ainult üheks päevaks, või tühjendades (kõige haavatavamad) pangaautomaadid ööseks täielikult. Teine meetod on saak rikkuda ja raha jälitatavaks muuta. Sellega seoses võib rakendada IBNS-i, mis määrib pangatähed ja märgib need varastatuks. See meetod on kõige tõhusam siis, kui kurjategijatel on võimatu sellist raha kulutada või neid pangatähti seaduslikku sularahasüsteemi uuesti sisse viia. Seda on võimalik saavutada nii, et pangad ja avalikkus ei võta määritud pangatähti maksete tegemiseks vastu ning paigaldatakse pangatähtede loendamis- ja tuvastusseadmed, mis suudavad määritud pangatähti tuvastada ja neid tagasi lükata. Sellega seoses on Belgias ja Prantsusmaal tasuvaks lahenduseks osutunud investeering infrapunasüsteemidesse, mis tuvastavad infrapunamarkeritega määritud pangatähti. IBNS-ide paigaldamisel peaksid riigid põhjalikult kaaluma valitud aktiveerimismehhanisme, rahatähtede neutraliseerimise miinimumnõudeid ja tindile kohtuekspertiisis tuvastatava markeri lisamist.

Meetmed, mis heidutavad potentsiaalseid kurjategijaid kuritegusid toime panemast, **suurendades avastamis- ja karistusohtu**, on teine telg füüsiliste pangaautomaadirünnakute ennetamisel. Pangaautomaadiründajate avastamise ja karistamise võtmeks on teabe kogumine ja jagamine kõigi sidusrühmade vahel nii riiklikul kui ka rahvusvahelisel tasandil. Teabevahetus kvaliteetsete valvekaamerapiltide ja heliandmete näol võib suurendada varajase avastamise ja eduka uurimise võimalusi. Vältimaks, et valvekaamerad või pealtkuulamisseadmed enne rünnakut rikutakse, võib kaaluda varjatud valvekaamerate

või reaalajas pealtkuulamisseadmete paigaldamist. Kohtueksperti andmebaasi loomine ja tehnoloogiate standardimine Euroopa tasandil võiks oluliselt hõlbustada rahvusvahelist koostööd ja uurimist. Kui õigusrikkujad on tabatud ja süüdi mõistetud, võib olla huvitav uurida paranduslikke (ja õigusrikkujatele keskendunud) rehabilitatsiooniprogramme, et vähendada kõrget retsidivismi.

Kolmas telg füüsiliste pangaautomaadirünnakute ennetamisel sisaldab meetmeid, et **suurendada pingutust**, mida kurjategija vajab kuriteo sooritamiseks. Pangaautomaadi paigaldamine kuriteokindlasse keskkonda, kus on maksimaalsed turvameetmed, muudab pangaautomaadi ründamise korrarikkujate jaoks ressursinõudlikumaks. Lisaks saab standardset pangaautomaadi kaitset täiendada mitmete lisaturvaelementidega. Peale nende meetmete saab ka udusüsteemi paigaldamisega kurjategijat heidutada või vähemalt tema rünnakut aeglustada.

Eespool nimetatud meetmeid tugevdavad mitmed **paralleelsed meetmed**, näiteks õigusliku raamistiku loomine, mis kohustab kõiki pangaautomaatide tarnijaid rakendama ennetusmeetmeid, samuti hästitoimiva meediastrateegia väljatöötamine, koostöö tõhustamine kohalikul, riiklikul ja rahvusvahelisel tasandil, kiirreageerijate suunised, et vähendada kaasnevate kahjude riski, ning investeeringud sotsiaalsesse ennetusse, et õõnestada kurjategijate värbamisprotsesse.

Factsheet

SOOVITUSED ENNETAVAKS LÄHENEMISVIISIKS: ÜLEVAADE

Tuleb töötada välja tõhus reaktsioon füüsiliste pangaautomaadirünnakute ennetamiseks

Olukorra hindamine

> Tuvastatakse pangaautomaatide riskiprofiil oma riigis/piikonnas

> Tuvastatakse partnerid ja huvirühmad füüsiliste pangaautomaadirünnakute vastases võitluses ja hinnake koostööd

> Hinnatakse riiklikul ja rahvusvahelisel tasandil õigusraamistikku füüsiliste pangaautomaadirünnakute vastu võitlemiseks.

Ennetava lähenemise väljatöötamine

> Tehakse kindlaks (peamised) käsitletavad riskid ja prioriteedid

> Tehakse kindlaks parimad ennetusmeetmed nende riskide katmiseks, kaaludes kolme peamist telge.

> Tehakse kindlaks paralleelsed ennetusmeetmed, mis on vajalikud, et rakendatud ennetusmeetmeid tugevdada.

Ennetavad meetmed, mida on võimalik võtta, et:

01

Reduce the awards

> Vähendatakse sularahasummat.
  - Pangaautomaat tühjendatakse ööseks.
  - Suurendatakse täitmiste arvu/sagedust.
> Saak rikutakse.
  - Intelligentsed pangatähtede neutraliseerimissüsteemid (IBNS).
  - Infrapunamärgised IBNS-tindis pangatähtede tuvastamiseks pangatähtede aktsepteerijate poolt.
  - Arendamisel: liim.

02

Increase the risk

> Piiriülene teabe jagamine:
  - võimaliku pangaautomaadirünnaku varajaseks või reaalajas tuvastamiseks,
  - operatiivse lähenemisviisi tugevdamiseks,
  - korduvate õigusrikkumiste eest süüdimõistmine,
  - kohtuekspertiisiandmete vahetamine Euroopa tasandil.
> Valvekaamerad ja pealtkuulamisseadmed.
> Tegude eest karistamine ja õigusrikkuja rehabilitatsioon.

03

Increase the effort

> Kuritegevust tõkestava keskkonna tagamine.
  - Kõrge riskiga pangaautomaatide asukoha muutmine.
  - Turvameetmed: füüsilised takistused, valve jne.
> Pangaautomaatide tugevdamine luukidega, mis on gaasiliste või tahkete lõhkeainete suhtes vastupidavad, jne.
> Ehituslikud meetmed, näiteks tagumine juurdepääs seadmetele.
> Turvaudusüsteemid.

Paralleelsed meetmed ennetava lähenemisviisi tugevdamiseks

> Tõhusad õigusaktid, sealhulgas ennetavad meetmed füüsiliste pangaautomaadirünnakute vastu, tegude eest süüdimõistmine jne.

> Tõhus meediastrateegia, mis heidutab kurjategijaid.

> Kõikide sidusrühmade (avaliku sektori, erasektori, korrakaitse) vaheline tõhustatud koostöö võitluses füüsiliste pangaautomaadirünnakutega.

> Kiirreageerijatele või tsiviilisikutele (nt naabruses elavatele või mööduvatele isikutele) kaasnevate kahjude riski vähendamine.

> Sotsiaalne ennetus, millega välditakse noorte värbamist (seda tüüpi) kuritegevusse.

ENDNOTES

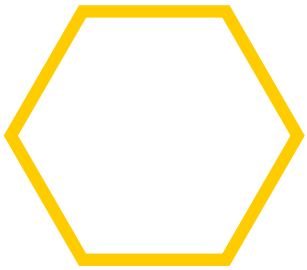
1 Willem Pieter de Groen, Zachary Kilhoffer ja Roberto Musmeci, „*The future of EU ATM markets: impacts of digitalisation and pricing policies on business models*“, CEPS aruanne, 2018

2 Derek Cornish ja Ronald V. Clarke, “*Opportunities, precipitators and criminal decisions: areply to Wortley’s critique of situational crime prevention*”, Crime prevention Studies 16 (2003), 41-96.

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

4 Euroopa Keskpanga otsus seoses euro rahatähtede vääringute, tehniliste näitajate, reprodutseerimise, vahetamise ja tagasivõtmisega, 2003.

5 David Weisburd, David P. Farrington ja Charlotte Gill, „Conclusion: What Works in Crime Prevention Revisited“, David Weisburd,David P. Farrington ja 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