Preprečevanje fizičnih napadov na bankomate

Razvijanje učinkovitega pristopa

Zahvala
Ta dokument je plod sodelovanja med Agencijo Evropske unije za sodelovanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (Europol) in sekretariata Evropske mreže za preprečevanje kriminala (EUCPN). Zahvaljujemo se strokovnjakom za fizične napade na bankomate, ki so vložili svoj čas in trud, da bi podprli nastanek tega svetovalnega poročila. Pomagali so z udeležbo na konferenci o preprečevanju fizičnih napadov na bankomate (Bruselj, januar 2019) in z zagotavljanjem ključnih informacij. Še posebej se zahvaljujemo organom kazenskega pregona iz držav članic EU in nečlanic EU (tretje države) ter predstavnikom zasebnega sektorja, kot so zlasti Združenje za bankomatsko sodelovanje (ATMIA), BPost, Centrum voor Criminaliteitspreventie en Veiligheid (CCV), Diebold Nixdorfom, Strokovna skupina za fizične napade na bankomate in blagajniške naprave (ATS) pri Evropskem združenju za varne transakcije (EAST EGAP), Evropska zveza za inteligentno varstvo gotovine (Euricpa), ING, Febelfin, NCR, Protect, SIOC Banking, Spinnaker, TMD Security in notranja ministrstva Belgije, Hrvaške, Nemčije in Španije.

Pravno obvestilo
Vsebina te publikacije ne odraža nujno mnenja katerekoli izmed držav članic EU ali kateregakoli organa ali inštitucije EU ali Evropske skupnosti.

Vsebina

1 Kontekst

Glede na to, da se povečujeta tako število fizičnih napadov na bankomate kot prizadetih evropskih držav, sta Evropska mreža za preprečevanje kriminala (EUCPN) ter Europol organizirala konferenco (januarja 2019), na kateri so organi pregona, javnost ter zasebni partnerji skupaj razmislili o tem, kako preprečiti takšen kriminal. To svetovalno poročilo povzema sklepe te konference, da bi oblastem predstavilo problematiko fizičnih napadov na bankomate ter preventivne ukrepe.

Širok nabor različnih metod (*modi operandi* (MO), ki jih kriminalci uporabljajo za napade na bankomate, lahko razdelimo na dve glavni kategoriji: fizični napadi na bankomate in z bankomati povezane goljufije (sem sodijo "logične" zlorabe in napadi z zlonamernimi programi). Ta referat se osredotoča na fizične napade: vdore v bankomat s fizičnimi sredstvi z namenom odtujitve denarja. Vdor se lahko izvede:

- z uporaba razstreliv: napadalci uporabijo plin ali trdna razstreliva, da bi fizično poškodovali bankomat in prišli do gotovine;
- z izruvanjem/vdor z vozilom: napadalci fizično odstranijo bankomat iz namestitvenega okolja, pogosto s pomočjo luksuznega vozila;
- z napadi in situ: napadalci vdrejo v sef z uporabo surove sile, pogosto z orodji za vlamljanje, kot so kotna brusilka, kovaško kladivo ali kisik-acetilenski plamen.

Omejeno, pa vendar rastoče število držav v Evropski uniji se spopada s fizičnimi napadi na bankomate. Po ocenah je finančna izguba leta 2017 v Evropi znašala več kot 30 milijonov evrov. Nekatere države beležijo znatno število fizičnih napadov na bankomate, druge pa precejšnje povečanje števila teh napadov v zadnjih 2 letih. To kriminalno področje se hitro razvija. Nekatere države so se uspešno spopadle s fizičnimi napadi na bankomate, zato se je tam njihovo število v zadnjem času znatno zmanjšalo. Po drugi stani pa so se prej neprizadete države leta 2018 soočile z nenadnim porastom fizičnih napadov na bankomate, ker so organizirane kriminalne združbe (OKZ) razširile svoje območje delovanja. Prizadete niso le banke, ampak vse pogosteje tudi bankomati neodvisnih ponudnikov, ki se pogosto nahajajo na ranljivejših lokacijah.

2 Dejavniki, ki določajo uspešnost fizičnih napadov na bankomate

Stopnja uspešnosti napadov na bankomate je nizka; uspešnih je le ena tretjina napadov. Vendar je enako pomembna tudi škoda, ki na zgradbi nastane ob neuspešnem napadu (npr. zaradi razstreliva), saj ustvari nevarno okolje v bližini kraja kaznivega dejanja za lokalne prebivalce, osebe, ki se prve odzovejo na dogodek, ter mimoidoče.

Uspešnost fizičnih napadov je odvisna od številnih faktorjev, zlasti od značilnosti bankomata, organizacije napada na bankomat ter sposobnosti storilcev.

2.1 Ranljivost bankomatov

Najranljivejši so bankomati, ki se nahajajo zunaj (skozi zid (TTW)) in tisti, ki stojijo v zgradbah. Pri napadih na notranje (prostostoječe) bankomate imajo OKZ raje bankomate, ki se nahajajo v trgovskih prostorih, kot pa bankomate v bančnih prostorih, kjer je nadzor praviloma močnejši. Banke običajno upravljajo bankomate, ki se nahajajo v ali zunaj bančne zgradbe. Od banke oddaljene lokacije na ulicah ali v trgovskih prostorih, kot so bencinske postaje, veleblagovnice, hoteli, igralnice, letališča itd. postajajo vse pomembnejše zaradi zapiranja bančnih poslovalnic. Neodvisni ponudniki upravljajo bankomate kot samostojno storitev. Njihovi bankomati se nahajajo na maloprodajnih, turističnih, rekreacijskih in prometnih lokacijah (železniške postaje, letališča itd.) ter v javnih zgradbah in na ulici.

Naraščajoča priljubljenost spletnega bančništva lahko v prihodnjih letih privede do zapiranja mnogih bančnih poslovalnic ter zmanjšanja števila bankomatov ([1]) Hkrati pa bi se lahko zato povečalo število od bank oddaljenih bankomatov ter bankomatov neodvisnih ponudnikov na ranljivejših lokacijah.

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

2.2 Organizacija napada na bankomat

Priprava na napad lahko traja nekaj tednov ali celo mesecev. Storilci morajo zbrati potrebna **orodja in sredstva**, kot so vozila, oprema in kontaktne točke. **Vozila** so ključna sredstva za fizične napade na bankomate; storilci običajno potujejo z avtom, po napadu pa najpogosteje pobegnejo s hitrimi vozili. Slednja so pogosto ukradena, lahko pa so tudi najeta ali kupljena (npr. preko spleta). Večina **opreme** za fizične napade na bankomate je možno brez težav zakonito kupiti v običajnih trgovinah. To še znižuje prag za vstop na to kriminalno področje. Organi pregona težko izsledijo izvor orodja, zato je tveganje za storilce omejeno. OKZ, ki izvajajo napade na bankomate na mednarodni ravni, imajo skoraj vedno kontaktne točke v ciljni državi (ljudi, ki prebivajo tam v določenem obdobju) ali pa uporabijo tehniko "napadi in pobegni". Ti kontakti pomagajo OKZ z logistiko, kot je najem bivališča, nabava vozila ali druge opreme ter ogledovanje tarč. Nekateri mednarodni storilci logistiko in ogledovanje v celoti prepustijo lokalnim kontaktom ter le pripotujejo po cesti ali zraku in izvedejo napad na bankomat.

OKZ pogosto izvedejo temeljito **ogledovanje**, da bi našli ustrezne tarče; ugotavljajo, ob kateri uri se polni bankomat, kakšna je njegova okolica, tehnične lastnosti, kako lahko pobegnejo ter kateri varnostni ukrepi se izvajajo, recimo televizijske kamere zaprtega kroga (CCTV), alarmni senzorji in vratca.

Nekatere OKZ pred napadom izvedejo številne ukrepe za **oviranje organov pregona in varnostnih služb**. Onemogočajo alarmne sisteme in javno razsvetljavo, uporabljajo diverzije, postavijo cestne zapore ali poskušajo onesposobiti vozila organov pregona.

2.3 Izkušnje in sposobnosti storilcev

Fizični napadi na bankomate so privlačni za kriminalce, saj je denar na voljo takoj ter ni potrebe po obsežni mreži za prodajo ukradenega blaga. To je priročna alternativa za kriminalce, ki so že dejavni na področju organiziranega premoženjskega kriminala.

OKZ si morajo pridobiti **znanje in sposobnosti**, saj je to odločilni faktor, ki vpliva na uspešnost napada. Potrebno znanje in sposobnosti so močno odvisni od **tipa napada**. Izruvanje in napadi *in situ*

imajo preprost MO (predvsem drznost in uporaba surove sile), zato načeloma ne zahtevajo posebnih spretnosti. Napadi z uporabo vnetljivega plina ali trdnih razstreliv zahtevajo višjo stopnjo znanja.

Napadalci kažejo različne **ravni sposobnosti**. Visoko organizirane in izkušene združbe lahko izvedejo uspešen napad na bankomat v nekaj minutah. Postopek imajo pod nadzorom ter so zmožne omejiti tveganje zase ter zato hkrati omejiti postransko škodo. Poskusi manj organiziranih ali priložnostnih združb pogosto niso uspešni in lahko obenem povzročijo znatno škodo na poslopju in sosednjih zgradbah. Nekatere manj organizirane OKZ se domnevno vrnejo k tradicionalnemu premoženjskemu kriminalu, saj zaradi preventivnih ukrepov niso uspešne pri napadih na bankomate.

3 Potreba po preventivnem pristopu

Primeri držav, kjer imajo storilci pri fizičnih napadih na bankomate nizko stopnjo uspešnosti in kjer se število fizičnih napadov na bankomate zmanjšuje, kažejo, da je uspešen pristop za preprečevanje fizičnih napadov na bankomate kombinacija operativnih in preventivnih ukrepov. Zaradi omejenega števila OKZ, dejavnih na tem kriminalnem področju, pridržanje in posledično kaznovanje članov OKZ znatno zmanjša število napadov. Toda po izpustu se mnogi napadalci na bankomate vrnejo k tej dejavnosti. Poleg tega združbe včasih hitro nadomestijo pridržanega storilca. Zato obstaja velika potreba po preventivnih ukrepih, po možnosti vključenih v zakonodajni okvir. Nadalje izkušnje kažejo, da zaradi preventivnih ukrepov v eni državi OKZ poiščejo ranljivejše tarče v drugih državah. Le vprašanje časa je, preden se MO, ki se pojavijo v eni državi, razširijo v druge države. To jasno kaže na **potrebo po sprejetju preventivnih in operativnih ukrepov na evropski ravni** ob tesnem sodelovanju zasebnih in javnih partnerjev ter organov pregona.

4 Preprečevanje

Za preprečevanje in spopadanje s to vrsto kriminala je potrebna jasna strategija. V tem poglavju bomo predstavili tri korake, ki se na splošno izvedejo pri soočanju s fizičnimi napadi na bankomate ali pri pripravi na njihovo preprečitev.

Prvi korak je **ocena situacije**; profil tveganja bankomata in njegove okolice je treba ugotoviti glede na dostopni znesek gotovine (potencialni plen), tveganje postranske škode in človeških poškodb. Drugi korak je razvoj **preventivne strategije** na podlagi ocene tveganja. Nazadnje je treba izvesti **preventivne ukrepe**.

4.1 Ocena situacije

OKZ običajno napadajo določene tipe bankomatov ali bankomate določenih ponudnikov z značilnostmi, ki olajšajo napad na bankomat. Zato je treba izvesti temeljito oceno tveganja za fizične napade na bankomate, po možnosti s celotno verigo za varnost gotovine od prevoza do dostave in hrambe v bankomatu. Za ugotovitev profila tveganja za posamezen bankomat morajo biti analizirani številni elementi, vključno z naslednjimi.

- Značilnosti lokacije in okolice bankomata, kot je to, ali gre za mesto ali podeželje, gostota prebivalstva, bližina policijske postaje, kamere za avtomatsko prepoznavo registrskih tablic (ANPR) v soseski, CCTV v bližini, itd.
- Lokacija bankomata:
    - v ali zunaj zgradbe, v bančni poslovalnici ali v oddaljenem (npr. trgovskem) prostoru, vgrajen ali pritrjen na zgradbo,
    - za prostostoječi bankomat: ali je zasidran ali ne,
    - za bankomate, vgrajene ali pritrjene na zgradbo: ali ima arhitekturne slabosti, kako je organizirana hramba gotovine itd.
- Tip bankomata.
- Varnostne funkcije bankomata.
- Količina gotovine v bankomatu.
- Pričakovani tip fizičnega napada in MO, da bi najprej izvedli najustreznejše preventivne ukrepe.
- Že izvedeni varnostni in preventivni ukrepi (inteligentni sistem za nevtralizacijo bankovcev (IBNS), CCTV, varnostna megla (zmanjšanje vidljivosti) itd.)

Nadaljnji elementi, ki jih je treba oceniti, so stanje sodelovanja s partnerji in zainteresiranimi stranmi ter zakonodajo. Za oblikovanje zavezništev za boj proti kriminalu je treba oceniti sodelovanje med organi pregona, zasebnimi in javnimi partnerji. Možno je, da vsak partner razpolaga z zanimivimi podatki, ki lahko pripomorejo k oceni situacije. Še posebej pomembni sta pri tem lokalna policija in lokalni organi. Potrebno je ovrednotenje zakonodaje z vidika oblikovanja pravnega okvira za preprečevanje napadov na bankomate, sprejemanja obveznih preventivnih ukrepov, izrekanje kazni za same napade itd.

4.2 Razvoj preventivnega pristopa

Ko se oceni situacijo in določi glavna območja tveganja ter prednosti in slabosti varnosti bankomata, se lahko razvije strategija (pogosto na podlagi javno-zasebnega sodelovanja) ter sprejmejo preventivni in operativni protiukrepi. Cilj preventivnih ukrepov bi moral biti zmanjšanje namena in zmožnosti storilcev. Za dosego tega se predlagajo tri osi preventivnih dejanj na podlagi treh izmed petih Clarkovih ([2]) strategij za situacijsko preprečevanje kriminala; zmanjšanje izkupička, povečanje tveganja za storilca ter povečanje napora, ki ga je treba vložiti za dostop do plena.

Kriminalci tehtajo med pričakovanim dobičkom in prisotnim tveganjem (npr. pri napadu na bankomat). Zmanjšanje možnosti za lahek izkupiček in povečanje tveganja za storilce zmanjša njihova pričakovanja in željo po fizičnem napadu na bankomat. Nadaljnji ukrepi, ki povečajo napor, ki ga je treba vložiti za dostop do bankomata, vplivajo na zmožnosti storilcev. Priložnostni storilci, katerih poskusi so pogosto neuspešni, prenehajo z napadi na bankomate. Pri profesionalnih napadalcih na bankomate se stopnja uspešnosti zmanjša, kar posledično vpliva na razmerje med dobičkom in tveganjem.

Preventivno strategijo dopolnijo še vzporedni ukrepi, kot je učinkovita medijska strategija, zgodnja socialna preventiva in ukrepi za zmanjšanje tveganja postranske škode na zgradbah in zagotovitev varnosti lokalnih prebivalcev, oseb, ki se prve odzovejo na dogodek, ter mimoidočih.

Obstajajo še drugi načini za oblikovanje pristopa. Na Nizozemskem so oblasti uporabile t. i. model oviranja ([3]). S tem modelom se prepoznajo koraki, ki jih mora kriminalec storiti za izvedbo kaznivega

([2]) Derek Cornish in 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

dejanja. Z njim se prepozna tudi partnerje in priložnosti, ki omogočajo kaznivo dejanje, hkrati pa je uporaben instrument za organizacijo procesa zbiranja podatkov o tem kriminalnem področju. S prepoznavo vsakega koraka, potrebnega za izvedbo fizičnega napada na bankomat, se lahko določi ovire za preprečitev kaznivega dejanja in najboljše partnerje za pripravo ovir. Model oviranja določi tudi signale za opozarjanje javnih in zasebnih partnerjev na fizične napade na bankomate ter signale, ki jih lahko sami pošljejo, da bi javnim organom sporočili svoje sume.

Potrebna je tudi dobro razvita strategija za ublažitev tveganja pri okrepitvi preventive. Preventivni ukrepi, ki so zelo učinkoviti pri odvračanju amaterjev in posnemovalcev, imajo včasih neželene učinke. Nekatere združbe se zatečejo k metodi poskusov in napak, da bi našle ranljive bankomate, kar privede do več poškodovanih bankomatov. Nevarnejše in brezobzirnejše OKZ se zatečejo k nasilnejšim MO, kot je uporaba trdnih razstreliv namesto plina pri svojih napadih.

Za pripravo učinkovitega kompleta preventivnih ukrepov je najboljša praksa ustanovitev državnega organa, ki ima pooblastila za izvajanje posebnih ukrepov za bankomate visokega tveganja na podlagi temeljite analize situacije. Ta pristop se je izkazal za učinkovitega v Franciji, predvsem ob oblikovanju pravnega okvira in če se ti ukrepi izvajajo skupaj z operativnimi ukrepi.

4.3 Izvajanje preventivnih ukrepov

Ukrepi za preprečevanje fizičnih napadov na bankomate iz tega poglavja so se izkazali za učinkovite v različnih državah. Slonijo na sklepih te konference o preventivi ter preventivnih ukrepih, ki jih aktivno promovirajo mednarodne organizacije s področja varnosti bankomatov. Mnogi ukrepi so dobro znani. Nekaj držav že uspešno izvaja številne izmed teh ukrepov. Toda predlagani ukrepi se pogosto izvajajo le delno in niso vključeni v zakonodajo.

Kot je bilo že omenjeno, se predlagajo tri osi preventivnih ukrepov: zmanjšanje izkupička, povečanje tveganja za storilca ter povečanje napora, ki ga je treba vložiti za dostop do plena.

4.3.1 Zmanjšanje izkupička

Zmanjšanje izkupička, pridobljenega s kaznivim dejanjem, je prva os za preprečevanje fizičnih napadov na bankomate. Kriminalci se bodo ukvarjali s to vrsto kriminala, dokler bodo imeli občutek, da lahko pridejo do "lahkega denarja". Zmanjšanje razpoložljivega zneska gotovine ter odstranitev ali

uničenje gotovine zmanjša možnost, da bi bil to zanimiv plen. Zmanjšano pričakovanje zmanjša željo kriminalca, da bi se ukvajal s to vrsto kriminala.

4.3.1.1 *Zmanjšanje zneska gotovine*

Eden od ukrepov je zmanjšanje izkupička z zmanjšanjem zneska gotovine v bankomatu. V idealnem primeru bi moral biti znesek omejen le na potrebe poslovanja v enem dnevu. Sodelovanje med bankami bi lahko zagotovilo stroškovno učinkovitost. Na Nizozemskem je ob sodelovanju številnih bank nastala od bank neodvisna mreža bankomatov z imenom "Geldmaat". Cilj sodelovanja je zagotovitev razpoložljivosti, cenovne dostopnosti in varnosti gotovine. To bo verjetno privedlo do zmanjšanja števila bankomatov. Toda posamezni bankomati ne bodo vsebovali več gotovine, temveč jih bodo pogosteje polnili. Število polnjenj bo prilagojeno potrebam.

Glede na to, da se napadi na bankomate večinoma zgodijo med 3.00 in 4.00, se pri prostostoječih bankomatih (večinoma se nahajajo v trgovskih in javnih prostorih, ki so ranljivejši) močno priporoča, da se jih ob koncu dneva izprazni, gotovina pa se prenese v sef. Opozorilni znak lahko javnost obvešča, da v bankomatu ponoči ni gotovine. Naslednji dan se mora bankomat napolniti ob odsotnosti strank v zaklenjenem prostoru. Ta sistem se izvaja v Franciji, kjer zakonodaja maloprodajnim trgovcem, ki imajo v trgovini bankomat, nalaga ponoči odstraniti denar iz bankomata ter ga pustiti odprtega. Pri ostalih bankomatih se lahko zneski v njih zmanjšajo z nižjo frekvence polnjenja.

4.3.1.2 *Onemogočanje plena in sledenje denarju*

Inteligentni sistemi za nevtralizacijo bankovcev (IBNS) so prva tehnika za onemogočanje izkupička. Ti sistemi obarvajo bankovce z barvilom in jih označijo kot ukradene. V IBNS-barvilo se lahko dodajo sledila in markerji. Trenutno se ti markerji večinoma uporabljajo za forenzične namene tako, da povežejo bankovce s krajem kaznivega dejanja in povečajo možnost, da bo storilec ujet. Čeprav je IBNS učinkovit preventivni ukrep, obstaja nekaj pomislekov.

Evropska centralna banka ne nadomešča obarvanih bankovcev ([4]) (od leta 2003), številne centralne banke držav članic EU pa jih še. Obarvani bankovci se v legalni sistem vrnejo tudi preko igralnic. IBNS ustvari dodatno oviro za kriminalce, vendar bi bil precej učinkovitejši, če kriminalci obarvanih bankovcev v EU ne bi mogli uporabljati. To bi dosegli, če državne centralne banke ne bi sprejemale

([4]) Sklep Evropske centralne banke o apoenih, specifikacijah, reprodukciji, zamenjavi in jemanju evrobankovcev iz obtoka, 2003.

obarvanih bankovcev. Izjema so lahko posebne okoliščine, kot so bankovci, ki so se obarvali med slučajnim sproženjem. Hkrati je pomembno svetovati prebivalstvu, naj ne sprejemajo obarvanih bankovcev. Dolgoročno bi morali sprejemniki bankovcev odkriti obarvane bankovce, nameščeni pa bi morali biti v bankah in trgovskih prostorih, kot so igralnice, avtopralnice itd. Odkrivanje barvila je težko in drago, stroškovno učinkovita rešitev pa bi bila namestitev infrardečih sistemov za odkrivanje bankovcev, obarvanih z infrardečimi markerji. Ti sistemi so se izkazali za učinkovite ter so najboljša praksa v Belgiji in Franciji. Ko se bankovci z infrardečim markerjem vstavijo v bankomat, slednji sprejme ("požre") denar, vendar ga ne položi na račun. Obenem je treba registrirati osebo, ki vstavlja obarvan bankovec.

Glede uvedbe rešitev IBNS obstaja še nekaj drugih pomislekov. Posamezni proizvajalci zagotavljajo različne rešitve IBNS z različnimi sprožilnimi mehanizmi in tipi barvila. Prvi pomislek se nanaša na dejstvo, da vse tehnologije za sprožanje IBNS niso učinkovite pri vseh grožnjah. Nekateri IBNS delujejo dobro pri napadih z izruvanjem, napadih *in situ* ali s plinom, vendar ne delujejo pri napadih s trdnim razstrelivom in obratno. Zato je pred izbiro tehnologije potreben tehten razmislek.
Naslednji pomislek je, kateri tip barvila izbrati. V Belgiji na državni ravni veljajo minimalne zahteve za IBNS (varnost, odstotek obarvanosti, ne sme se sprati itd), neodvisni testi pa potrjujejo, da sistem ustreza državnim standardom in deluje v skladu z proizvajalčevimi trditvami. Test je treba izvesti s pravimi bankovci, saj so na trgu tudi cenejša barvila, ki dobro delujejo pri ponarejenih bankovcih, s pravimi bankovci pa ne: to pomeni, da se lahko barvilo s pristnih bankovcev odstrani s pranjem. Hkrati je priporočljivo v barvilo dodati forenzični marker, ki omogoča preiskovati povezavo med obarvanimi bankovci in določenim krajem kaznivega dejanja.

Najboljša praksa kaže, da je lahko IBNS zelo učinkovit v povezavi z drugimi preventivnimi ukrepi. Francija je leta 2015 uvedla novo zakonodajo s členi o namestitvi IBNS in uporabi barvila z izvirno DNK. Francoska vojaška policija (žandarmerija) se na podlagi ocene tveganja odloči, kje se bo uporabil IBNS in drugi ukrepi. Odkar je nova zakonodaja okrepila preventivni in operativni pristop, se je število napadov znižalo s 300 leta 2013 na 50 leta 2018.

Še ena razvijajoča se tehnika za onemogočanje plena je **lepilo**. Učinkovitost lepila je bila dokazana na Nizozemskem, toda izvedbeni in tekoči stroški so trenutno visoki. Poleg tega lahko lepilo povzroči požar, če sistem pred napadom ni aktiviran, saj lahko zaradi razpršenih delcev lepila v zraku nastane vnetljiva mešanica. Te metoda še ni pripravljena za prodajo na trgu, vendar bi lahko bila ena izmed rešitev v prihodnosti.

4.3.2 Povečanje tveganja

Druga os za preprečevanje fizičnih napadov na bankomate je odvrnitev potencialnih storilcev od izvajanja kaznivih dejanj. Poleg tveganja fizične poškodbe pri uporabi razstreliva za napade na bankomate je glavno tveganje za kriminalca zaporna kazen, če ga ujamejo med samim napadom ali po preiskavi. Željo potencialnega storilca se zmanjša tako, da se poveča tveganje za odkritje in kazen. Za družbo je prijetje in obsodba kriminalca zelo učinkovita preventivna metoda, če temu sledi tudi kazen, kot smo videli v nekaterih državah.

4.3.2.1 *Izmenjava podatkov*

Ključno pri odkritju in kaznovanju napadalcev na bankomate je izmenjava podatkov med vsemi zainteresiranimi stranmi v boju proti fizičnim napadom na bankomate, vključno s ponudniki bankomatov, organi pregona (policija, tožilec itd.), javnimi organi, proizvajalci tako bankomatov kot varnostnih in zaščitnih naprav, poklicnimi združenji, ponudniki bankomatov (banke in neodvisni ponudniki), varnostnimi podjetji in alarmnimi centri. V idealnem primeru bi to potekalo tako na državni kot mednarodni ravni.

Težko je zgodaj odkriti bližajoči se fizični napad na bankomat. Zgodnje odkritje je možno le pri skoraj brezhibni izmenjavi podatkov na mednarodni ravni med organi pregona in zasebnimi partnerji (varnostna podjetja in ponudniki bankomatov). Spremljati je treba širok krog kazalnikov, zlasti zgodnja opozorila med organi pregona o dejavnih OKZ, podatke o ("vročih") vozilih, uporabljenih v napadih na bankomate, podatke varnostnih podjetij ali sosedskih straž o sumljivem obnašanju v okolici bankomata, sumljive transakcije, ki jih zaznajo ponudniki bankomatov in druge metode zaznavanja. Drugi možni policijski ukrepi za zgodnje odkritje so spremljanje ukradenih avtov, proizvajalcev in distributerjev razstreliv in podjetij, pooblaščenih za uporabo razstreliv. Zgodnje odkritje zahteva veliko truda, ki hkrati ne zagotavlja uspeha, zato so posredovanja organov pregona pred samimi napadi redka.

Če zgodnje odkritje ni možno, lahko alarmni centri hitro izdajo opozorilo v primeru fizičnega napada na bankomat. Posredovanje se omogoči z dogovorom in vzpostavitvijo državnih predpisov in protokolov za hitro komunikacijo med alarmnimi centri in organi pregona. V primeru zgodnjega odkritja ali informacij v realnem času morajo organi pregona vedno izbrati najustreznejši čas in

možnost za posredovanje. Zelo težko je kriminalca zalotiti med samim dejanjem, hkrati pa lahko pride do nevarne situacije, saj so nekatere OKZ zelo nasilne in uporabljajo težko orožje.

Za uspešno preiskavo po fizičnem napadu na bankomat morajo predstavniki organov pregona komunicirati z zainteresiranimi stranmi, saj lahko vsak izmed njih razpolaga s podatki, ki lahko pripomorejo k uspešnosti preiskave. Seveda sta potrebna komunikacija in sodelovanje s primarnimi žrtvami, bankami in ponudniki bankomatov, ki imajo dostop do podatkov, pomembnih za preiskavo. Ponudniku bankomata podatki organov pregona pomagajo izboljšati preventivne ukrepe. Tudi stik s poklicnimi združenji in proizvajalci se je izkazal za koristnega, saj pogosto pošiljajo sporočila z varnostnimi opozorili, na katera se lahko naročijo zainteresirane strani. Proizvajalci bankomatov imajo dober pregled nad različnimi tipi napadov na bankomate ter slabostmi in prednostmi posameznih preventivnih ukrepov. Policiji so pripravljeni sporočati podatke o tehničnih vidikih bankomatov in uporabljenih MO.

Čezmejno sodelovanje je ključnega pomena: države bi si morale izmenjavati podatke (o osumljencih, obsojencih za napade na bankomate, MO, sumljivih vozilih, posnetke napadov itd.), ne le za pomoč pri preiskavi, ampak tudi zato, ker se lahko osumljencem, obsojenim v drugi državi, izreče kazen kot povratnikom (recidivizem).

Naposled bi uvedba baze podatkov na evropski ravni, ki bi jo imeli na razpolago organi pregona, vsebovala pa bi forenzične podatke (npr. o različnih tipih IBNS-barvil, sledilih in markerjih ali zaščitnih steklih na bankomatih), močno olajšala preiskavo in povezala osumljenca z določenim krajem kaznivega dejanja. Standardizacija tehnologij na mednarodni ravni je pogosto nezadostna: med konferenco januarja 2019 so udeleženci omenili, da bi standardizacija barvil in oznak kaznivih dejanj močno pripomogla k uspešnosti preiskav.

4.3.2.2 *CCTV in naprave za poslušanje*

Slikovni in zvočni podatki sistemov CCTV in naprav za poslušanje pomagajo tako pri odkritju napada v realnem času (npr. za preprečitev fizičnih poškodb prvih oseb, ki prispejo na kraj kaznivega dejanja) ter kasnejši preiskavi (npr. za prepoznavo storilcev in njihovega MO). Posnetki CCTV-kamer se lahko povežejo z drugimi sistemi v okolici bankomata in posnetki prometnih radarjev, kar omogoči popolnejšo sliko storilcev in njihovega MO.

Toda posnetki CCTV-kamer so pogosto slabe kakovosti sli slabo shranjeni. Posnetki morajo biti zadostne kakovosti za prepoznavo osebe. Tudi v tem pogledu bi evropska standardizacija varnostnih CCTV olajšala preiskave. Glede na to, da storilci pogosto onesposobijo CCTV-kamere, je vredno razmisliti o namestitvi skritih CCTV ali naprav za poslušanje v realnem času.

4.3.2.3 *Kazen in rehabilitacija prestopnikov*

Dosledna in stroga kazen ima dokazano preventiven učinek. Pridržanje OKZ ima takojšen učinek na številne napade na bankomate. Izpustitev napadalcev na bankomate iz zapora pa pogosto privede k novemu valu napadov. To pomeni, da ob kratki kazni storilci zelo hitro postanejo spet dejavni. Najnižje in najvišje kazni za kriminalce, obsojene za posamezen tip fizičnega napada na bankomat, se razlikuje glede na državo članico. Nekateri menijo, da bi višje kazni potencialne storilce odvračale od napadov. Toda znanstvene raziskave ([5]) kažejo, da strožje kazni ne izboljšajo nujno učinka odvračanja od napadov. Zato bi lahko razmislili o popravnih (in s poudarkom na prestopnikih) rehabilitacijskih programih, da bi znižali visoko stopnjo recidivizma.

4.3.3 Povečanje napora

Tretja os za preprečevanje fizičnih napadov na bankomate se nanaša na dejanja, ki prestopniku otežujejo izvesti kaznivo dejanje.

4.3.3.1 *Ustvariti na kriminal odporno okolje*

Če ocena tveganja (cf. supra) pokaže, da se bankomat nahaja v zelo tveganem okolju, je treba lokacijo demontirati in bankomat prenesti na nizko ali srednje tvegana območja. To v vsakem primeru velja, če analiza pokaže, da bi se zgradba ob napadu na bankomat z razstrelivom lahko porušila. Lahko bi se sprejela zakonodaja, ki bi zahtevala takšne ukrepe v visoko tveganih primerih. Ob zmanjšanju števila bankomatov v visoko tveganih okoljih bi morali tudi spodbujati brezgotovinska plačila, ki bi zmanjšala potrebo po bankomatih.

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

Če bankomata ni možno prenesti, je treba izvesti maksimalne preventivne ukrepe: npr. uporaba zaščitnih količkov proti vdorom z vozilom, uličnih svetilk in drugega uličnega pohištva za omejitev dostopa do zgradbe, sistemov za prisilno ustavitev vozil, namestitev ustrezne ulične razsvetljave, dodaten viden ali skrit nadzor in protiropne naprave, kot je sistem za degradacijo bankovcev. Če je bila napadena lokacija, ki ni veljala za visoko tvegano, bi se jo moralo prepoznati kot tako ter izvesti dodatne varnostne ukrepe. V orodje za oceno tveganja je treba vnesti nove dejavnike ter ga tako posodobiti. Ocenjevanje tveganja je treba redno ponavljati.

4.3.3.2 *Okrepitev bankomatov*

Proizvajalci bankomatov ponujajo standarden nabor bankomatov s številnimi varnostnimi funkcijami, ki se ocenjujejo glede na stopnje varnosti Evropskega odbora za standardizacijo (CEN). Na splošno so pri tem ocenjevanju bankomatom dodeljene varnostne stopnje od CEN1 (najnižja) do CEN4 (najvišja). Stopnja se dodeli glede na značilnosti, kot sta moč ohišja in odpornost. Odpornost na plin je večinoma ponujena kot izbira (CEN-GAS). Standardne modele je možno izboljšati z dodatnimi varnostnimi ukrepi. Običajno tretje osebe namestijo te funkcije, da bi zadostile lokalni zakonodaji in prilagodile osnovni model potrebam lokalnih strank. Dodatne varnostne funkcije vključujejo različne senzorje za sproženje sistema za nevtralizacijo plina ali IBNS za primer napada *in situ* ali napada z razstrelivom ter boljša vratca in ključavnice za preprečevanje dostopa do sefa, ko so glavna vratca onesposobljena. Pri prenosnih prostoječih bankomatih je pomembno uporabiti sistem zasidranja, ki ponuja dodatno zaščito pred izruvanjem/vdorom z vozilom. Bankomate se lahko opremi s sledilnim sistemom, ki pomaga preiskovalcem, ko je bankomat pred odprtjem prepeljan na drugo lokacijo.

4.3.3.3 *Arhitekturni ukrepi*

Priporočajo se bankomati z izdajanjem denarja zadaj. V tem primeru mora storilec vstopiti v zgradbo in imeti dostop do zadnjega dela bankomata, da bi ukradel gotovino. Najranljivejši so prenosni in prostostoječi bankomati. Zmanjšanje števila takšnih bankomatov bi povečalo varnost. Obveznost nameščanja bankomatov v protivlomnem prostoru bi avtomatsko zmanjšala uporabo prostostoječih bankomatov.

4.3.3.4 *Varnostna megla*

Top hitro napolni sobo z gosto meglo, tako da vsiljivec ne vidi ničesar. Varnostna megla pogosto onemogoči izvedbo napada na bankomat. Če nič drugega, sistem upočasni storilca, kar da policiji več časa za posredovanje. Sistem varnostne megle je povezan z alarmnim sistemom ter se lahko sproži na dva načina. Samodejno ga lahko sprožijo alarmni senzorji, kot so detektorji za zaznavo gibanja (ponoči) ali senzorji za nasilno odpiranje vratc bankomata. Sproži ga lahko tudi alarmni center, da bi se izognili preveč lažnim alarmom. Pri zunanjih bankomatih "skozi zid" se lahko varnostna megla uporabi tako, da se sproži pri zadnjem delu bankomata, od koder se razširi in zmanjša vidljivost storilcev na nič.

Z varnostno meglo se lahko zaščiti posamezne točke z bankomati, ki se nahajajo v odprtih prostorih na bencinskih črpalkah, veleblagovnicah itd. Tako megla ne zajame celotnega območja. Zaščita z meglo je najučinkovitejša, če megla prihaja iz različnih kotov ali ko napolni prostor za bankomatom v primeru
vdora z vozilom. Trenutno se še testira, ali bi topove za meglo lahko namestili v sam bankomat, in ne v prostor, kjer se nahaja bankomat. V meglo se lahko doda DNK-markerje, ki bi se znašli na storilcih in njihovih oblačilih.

4.3.4 Vzporedni ukrepi

Za zagotovitev učinkovitega izvajanja omenjenih preventivnih ukrepov je treba razmisliti še o vzporednih ukrepih. To so nujni ukrepi za vzpostavitev ali okrepitev celostnega preventivnega in operativnega pristopa za soočanje s fizičnimi napadi na bankomate.

4.3.4.1 *Zakonodaja*

V številnih državah zakonodaja obvezuje ponudnike bankomatov izvajati preventivne ukrepe. V drugih državah sklenjeni sporazumi in dogovori med bankami in organi pregona omogočajo dobro voden pristop za soočanje s fizičnimi napadi na bankomate. Med področja, kjer bi lahko razmislili o regulativnih ukrepih, sodijo:

- vključevanje preventivnih ukrepov;
- pravni okviri, ki bi omogočili sodelovanje med organi pregona ter javnimi in zasebnimi partnerji;

- preoblikovanje kaznovalne politike, če so kazni za storilce pri fizičnih napadih na bankomate prenizke.

Toda pogosto morajo te obveznosti izpolnjevati le bančne ustanove, medtem ko za neodvisne ponudnike bankomatov ti zakoni in dogovori ne veljajo. To je pogosta šibka točka regulativne zakonodaje.

Nekatere države ne izvajajo nikakršnih predpisov, ampak poskušajo ponudnike bankomatov prepričati v izvajanje preventivnih ukrepov tako, da jih opozarjajo na to kriminalno področje in trende: v državah z velikim številom neodvisnih bank se je to izkazalo za še posebej težko.

Poskrbeti se mora, da bi učinkovito izvajanje preventivnih ukrepov vključevalo spremembe zakonodaje in predpisov tako na državni kot mednarodni ravni, kar bi veljalo za vse vrste ponudnikov bankomatov. V idealnem primeru bi morali zakonodajo poenotiti na ravni EU, da bi se izognili temu, da bi se zaradi strogih preventivnih ukrepov v zakonodaji ene države OKZ preusmerile v države z manj strogimi predpisi.

4.3.4.2 *Medijska strategija*

Še ena pomembna os preventivne strategije je dobra medijska strategija, katere namen je zmanjšanje pričakovanj in želje napadalcev na bankomate po ukvarjanju s to vrsto kriminala. Izpostaviti bi se morala nizka stopnja uspešnosti in visoko tveganje za storilce, izogibati pa se je treba omembam izkupička (plena) ali podrobnosti napadov na bankomat, kot sta tip napadenega bankomata ali MO. Po drugi strani pa bi se moralo obsežno poročati o pridržanju osumljencev in kaznih, ki so jih prejeli po obsodbi.

4.3.4.3 *Boljše sodelovanje*

Boljše sodelovanje in izmenjava podatkov sta že bila izpostavljena, vendar ju zaradi izredne pomembnosti velja omeniti večkrat. Ključna dejavnost Europola je izmenjava operativnih podatkov na mednarodni ravni. Ob izmenjavi podatkov se je na konferenci o preventivi izpostavila potreba po izrazitejši večdisciplinarnosti in sodelovanju na več ravneh ter izmenjavi podatkov med vsemi pomembnimi zainteresiranimi stranmi, vključno z organi pregona, javnimi organi, proizvajalci bankomatov ter varnostnih in zaščitnih naprav, poklicnimi združenji, ponudniki bankomatov (banke

in neodvisni ponudniki), varnostnimi podjetji in alarmnimi centri. To mora veljati za lokalno, državno in mednarodno raven.

4.3.4.4 *Zmanjšanje tveganja za postransko škodo*

Ob napadu s trdnimi razstrelivi bodo nekatere OKZ pustile material na kraju kaznivega dejanja. To je lahko nevarno za osebe, ki se prve odzovejo na dogodek, ali civiliste (živeče v soseski ali mimoidoče). Poskrbeti je treba za njihovo varnost. Kot to velja v Belgiji, je treba protokole in postopke, ki jih morajo upoštevati osebe, ki se prve odzovejo na dogodek (tako iz vrst organov pregona kot ponudnikov bankomatov), razviti in medsebojno poenotiti. Še ena najboljša praksa v tem pogledu je nizozemska, kjer za oceno situacije uporabljajo posnetke napada na bankomat, ki jih ujamejo CCTV-kamere. Lahko se sklenejo dogovori z alarmnimi centri, ki bi nemudoma posredovali te posnetke.

4.3.4.5 *Socialna preventiva*

OKZ pogosto novačijo mlade osebe. Lahko bi se pripravili projekti, ki bi ovirali procese novačenja v zgodnji fazi. Policija in socialni delavci bi morali biti pozorni na te procese, da bi lahko ukrepali preko osebnega stika s potencialnimi storilci.

5 Sklepi

V zadnjih 2 letih se je število napadov na bankomate v evropskih državah povečalo. V zvezi s tem sta Europol in EUCPN združila sile ter zbrala najboljše ukrepe za boj proti tej vrsti kriminala.

Uspešen pristop za preprečevanje fizičnih napadov na bankomate je kombinacija operativnih in preventivnih ukrepov, po možnosti vključenih v zakonodajo. Te ukrepe je priporočljivo uvesti na evropski ravni, da bi se izognili temu, da bi se zaradi strogih ukrepov v eni državi OKZ preusmerile v ranljivejše države.

Za preprečevanje in spopadanje s to vrsto kriminala je treba oblikovati jasno strategijo v treh korakih: ocena situacije, razvoj preventivnega pristopa na podlagi ocene tveganja in izvajanje preventivnih ukrepov.

Ocena tveganja za fizične napade na bankomate bi morala vključevati značilnosti bankomata in njegove okolice, sodelovanje s partnerji in zainteresiranimi stranmi za oblikovanje zavezništev za boj proti tej vrsti kriminala ter ovrednotenje preventivnega in pravnega okvira. Po oceni situacije je treba oblikovati strategijo na podlagi javno-zasebnega sodelovanja ter preventivnih in operativnih protiukrepov. Cilj preventivnih ukrepov je zmanjšanje stopnje namena in zmožnosti storilcev za izvedbo fizičnega napada na bankomat. Za dosego tega cilja se predlagajo tri osi preventivnih dejanj: zmanjšanje izkupička, povečanje tveganja in povečanje napora. Preventivno strategijo bi morali dopolniti vzporedni ukrepi. Najboljša praksa je oblikovanje državnega organa s pooblastili, da lahko naloži izvajanje potrebnih ukrepov.

Ob **zmanjšanju izkupička** se zmanjša tudi želja kriminalca po ukvarjanju s to vrsto kriminala. Eden izmed ukrepov za zmanjšanje pričakovanja kriminalca je znižanje zneska gotovine v bankomatu tako, da se dnevna polnitev gotovine omeji na potrebe poslovanja le za 1 dan, ali tako, da se (najranljivejše) bankomate ponoči izprazni. Naslednja metoda je onemogočanje uporabe plena in sledenje denarju. Pri tem se lahko uporabi IBNS, ki obarva bankovce in jih označijo kot ukradene. Ta metoda je najučinkovitejša, ko kriminalci ne morejo porabiti denarja ali vrniti bankovcev v zakoniti denarni sistem. To se doseže tako, da banke in javnost ne sprejemata plačil z obarvanimi bankovci, oziroma z namestitvijo sprejemnikov bankovcev, ki odkrijejo in zavrnejo obarvane bankovce. V tem pogledu so se v Belgiji in Franciji za stroškovno učinkovito rešitev izkazali infrardeči sistemi, ki odkrivajo obarvane bankovce z infrardečimi markerji. Pri namestitvi IBNS bi morale države temeljito razmisliti o izbiri sprožilnega mehanizma, minimalnih zahtevah za nevtralizacijo bankovcev ter dodajanju forenzičnih markerjev v barvilo.

Druga os za preprečevanje fizičnih napadov na bankomate je odvračanje potencialnih storilcev od izvedbe napada tako, da se **poveča tveganje** za njihovo odkritje in kazen. Ključno pri odkrivanju in kaznovanju napadalcev na bankomate je zbiranje in izmenjava podatkov med zainteresiranimi stranmi tako na državni kot mednarodni ravni. Izmenjava visokokakovostnih posnetkov CCTV-kamer in zvočnih podatkov lahko poveča možnosti za zgodnje odkritje in uspešnost preiskave. Onesposobitev CCTV ali naprav za poslušanje pred napadom se lahko prepreči z namestitvijo skrite CCTV ali naprave za poslušanje v realnem času. Priprava forenzične baze podatkov in standardizacija tehnologij na evropski ravni bi lahko močno olajšala mednarodno sodelovanje in preiskovanje. Lahko bi razmislili tudi o popravnih (in s poudarkom na prestopnikih) rehabilitacijskih programih za ujete in obsojene prestopnike, da bi znižali visoko stopnjo recidivizma.

Tretja os za preprečevanje fizičnih napadov na bankomate se nanaša na **povečanje napora**, ki ga mora prestopnik vložiti v izvedbo kaznivega dejanja. Namestitev bankomata v okolje, ki je odporno na kriminal, in izvajanje maksimalnih varnostnih ukrepov bo prestopniku otežilo napad na bankomat. Obenem se lahko standardna zaščita bankomata izboljša s številnimi dodatnimi varnostnimi funkcijami. Poleg teh ukrepov lahko storilca od napada odvrne ali vsaj upočasni še sistem varnostne megle.

Številni **vzporedni ukrepi** bodo okrepili navedene ukrepe, denimo priprava pravnega okvira, ki ponudnike bankomatov obvezuje izvajati preventivne ukrepe, razvoj dobre medijske strategije, boljše sodelovanje na lokalni, državni in mednarodni ravni, smernice za osebe, ki se prve odzovejo na dogodek, ki bi pomagale zmanjšati tveganje za postransko škodo, ter socialna preventiva, ki bi ovirala procese novačenja kriminalcev.

6 Priporočila za preventivni pristop: pregled

Razvijte učinkovit odgovor za preprečevanje fizičnih napadov na bankomate

Ocenite situacijo

Določite profil tveganja za bankomate v vaši državi/regiji
Ugotovite, kdo so partnerji in zainteresirane strani v boju proti fizičnim napadom na bankomate in ovrednotite sodelovanje
Ovrednotite pravni okvir za preprečevanje fizičnih napadov na bankomate na državni in mednarodni ravni.

Razvijte preventivni pristop

Izpostavite (glavna) tveganja, ki jih je treba nasloviti, ter prednostne naloge
Določite najboljše preventivne ukrepe za naslovitev teh tveganj ob upoštevanju treh glavnih osi.
Določite vzporedne preventivne ukrepe za okrepitev že sprejetih preventivnih ukrepov.

Preventivni ukrepi, ki se jih lahko sprejme za		
Zmanjšanje izkupička	Povečanje tveganja	Povečanje napora
– Zmanjšanje zneska gotovine. ○ Izpraznitev bankomata ponoči. ○ Povečanje števila/frekvence polnjenj. – Onemogočanje plena. ○ inteligentni sistemi za nevtralizacijo bankovcev (IBNS). ○ Infrardeči markerji in barvilo za odkrivanje obarvanih bankovcev s sprejemniki bankovcev. ○ V razvoju: lepilo.	– Čezmejna izmenjava podatkov za: ○ odkrivanje napadov zgodaj ali v realnem času, ○ okrepitev operativnega pristopa, ○ obsodbe povratnikov, ○ izmenjava forenzičnih podatkov na evropski ravni. – CCTV in naprave za poslušanje. – Kaznovanje in rehabilitacija prestopnikov.	– Ustvarjanje na kriminal odpornega okolja. ○ Sprememba lokacije visoko tveganih bankomatov. ○ Varnostni ukrepi: fizične ovire, nadzor itd. – Okrepitev vratc bankomata, odpornost na plin ali trdna razstreliva itd. – Arhitekturni ukrepi, kot so bankomati z izdajanjem denarja zadaj – Varnostna megla.

Vzporedni ukrepi za okrepitev preventivnega pristopa

– Učinkovita zakonodaja, zlasti s preventivnimi ukrepi proti fizičnim napadom na bankomate, doslednim kaznovanjem itd.

- Učinkovita medijska strategija za jemanje poguma storilcem.
- Boljše sodelovanje med zainteresiranimi stranmi (javnimi, zasebnimi, organi pregona) v boju proti fizičnim napadom na bankomate.
- Zmanjšanje tveganja za postransko škodo za osebe, ki se prve odzovejo na dogodek, ter civiliste (npr. živeči v soseski ali mimoidoči).
- Socialna preventiva, da mladih ne bi novačili za (takšna) kazniva dejanja.