Sprječavanje fizičkih napada na ATM uređaje

Razvoj učinkovitog pristupa

Prihvaćanje
Ovaj dokument je plod suradnje između Agencije Europske unije za izvršavanje zakonodavstva (Europol) i tajništva Europske mreže za sprječavanje kriminala (EUCPN). Željeli bismo zahvaliti stručnjacima na području fizičkih napada na bankomate (ATM) koji su uložili vrijeme i trud kako bi podržali stvaranje ovog dokumenta preporuke. Oni su pridonijeli svojim sudjelovanjem na konferenciji o sprječavanju fizičkih napada na ATM-ove (siječanj 2019., Bruxelles) i pružanjem ključnih informacija. Posebno se želimo zahvaliti agencijama za provedbu zakona iz zemalja EU-a i zemalja koje nisu članice EU-a ("trećih"), privatnom sektoru, uključujući Udruženje ATM industrije (ATMIA), BPost, Centrum voor Criminaliteitspreventie en Veiligheid (CCV), Diebold Nixdorf, Europsku stručnu skupinu za sigurne transakcije na bankomatima i fizičke napade na ATS [automatizirani sefovi] (EAST EGAP), Europsu udrugu za inteligentnu zaštitu gotovine (Euricpa), ING, Febelfin, NCR, Protect, SIOC bankarstvo, Spinnaker, TMD sigurnost i ministarstva unutarnjih poslova Belgije, Hrvatske, Njemačke i Španjolske.

Sadržaj

1 Kontekst

Budući da se broj fizičkih napada na bankomate (ATM) i broj europskih zemalja koje su pogođene povećavao, Europska mreža za sprječavanje kriminala (EUCPN) i Europol organizirali su konferenciju (siječanj 2019.) na kojoj se policija zajedno s javnim i privatnim partnerima zajedno bavila traženjem načina prevencije ovog zločina. Ovaj dokument preporuke obuhvaća zaključke ove konferencije kako bi se podigla svijest tijela vlasti o fizičkim napadima na bankomate i preventivnim mjerama.

Širok raspon različitih metoda (*modi operandi* (MOs)) kojima se kriminalci koriste za napade na bankomate može se podijeliti u dvije glavne kategorije: fizički napadi na bankomate i prijevare povezane s bankomatima (to uključuje ATM-logičke napade i napade zlonamjernim softverom). Ovaj dokument usmjeren je na fizičke napade na bankomate: nasilne upade fizičkim sredstvima u bankomate kako bi se ispraznio novac. Nasilni upad se može izvršiti na sljedeći način:

- uporabom eksploziva: napadači upotrebljavaju plinske ili krute eksplozive kako bi fizički probili ATM sef te došli do novca:
- napadi izbijanjem/probijanjem: napadači fizički uklanjaju bankomat iz instalacijskog okruženja, često koristeći vrlo brza vozila;
- napadi na licu mjesta: napadači velikom silom probijaju sef, često koristeći alate za rezanje ili lomljenje, poput kutnih brusilica, udarnih čekića ili oksiacetilenskih baklji.

Ograničeni, ali sve veći broj zemalja u Europskoj uniji ima problem zbog fizičkih napada na bankomate. U 2017. godini nastali financijski gubici procijenjeni su na preko 30 milijuna eura u Europi. Neke su zemlje i dalje svjedoče značajnom broju fizičkih napada na bankomate, a druge su zabilježile značajan porast broja tih incidenata u posljednje 2 godine. Ovo područje kriminala brzo se razvija. Neke zemlje su bile uspješne u svojem pristupu rješavanju fizičkih napada na ATM uređaje i nedavno su zabilježile značajan pad napada. S druge strane, zemlje koje prije nisu bile pogođene, suočile su se s iznenadnim porastom fizičkih napada na ATM uređaje u 2018. godini zbog organiziranih kriminalnih skupina (OCG) koje šire svoj teritorij. Nisu pogođene samo banke, nego se sve više napadaju bankomati neovisnih pružatelja usluga, jer se često nalaze u izloženim prostorima ili lokacijama.

2 Čimbenici koji određuju uspjeh fizičkog napada na ATM

Stopa uspjeha napada na ATM uređaje je niska; samo trećina napada uspije. Međutim, čak i kada napad ne uspije, šteta koja je nanesena (npr. eksplozivom) na građevinskim konstrukcijama jednako je važna, ostavljajući nesigurno okruženje u blizini mjesta zločina za lokalne stanovnike, spasioce i prolaznike.

Uspjeh fizičkog napada ovisi o brojnim čimbenicima, koji uključuju; karakteristike bankomata, organizaciju ATM napada te iskustvo i znanje počinitelja.

2.1 Ranjivost bankomata

Najosjetljiviji bankomati su oni koji se nalaze vani (kroz zid (TTW)) ili oni postavljeni unutar zgrada. Kada napadaju unutarnji ATM uređaj (samostojeći), organiziranje kriminalne skupine (OCG) preferiraju ATM uređaje koji se nalaze u prostorima trgovačkih centara više nego ATM uređaje u prostorima banaka, u kojima je nadzor obično jači. Banke uglavnom posluju s bankomatima koji se nalaze unutar ili izvan zgrade banke. Udaljene lokacije banke ("banke na udaljenosti") na ulici ili u trgovačkim centrima, poput benzinskih postaja, supermarketa, hotela, kockarnica, zračnih luka itd., postaju sve važnije kada se poslovnice banaka zatvore. Nezavisni pružatelji usluga posluju s ATM uređajima kao samostalnom uslugom. Njihovi bankomati često se nalaze na lokacijama maloprodajnih trgovina, ugostiteljskim i rekreativnim lokacijama, lokacijama za prijevoz (željezničke stanice, zračne luke itd.), javnim zgradama i na ulici.

Zbog sve veće popularnosti internetskog bankarstva, vjerojatno će se mnoge poslovnice banaka narednih godina zatvoriti, što će dovesti do općenitog smanjenja broja bankomata. ([1]) Međutim, to bi moglo dovesti do povećanja broja bankomata koji su udaljeni od banaka i bankomata nezavisnih pružatelja usluga, koji se nalaze na osjetljivijim lokacijama.

([1]) Willem Pieter de Groen, Zachary Kilhoffer i Roberto Musmeci, *Budućnost tržišta bankomata u EU-u: utjecaji digitalizacije i politika cijena na poslovne modele*, izvješće CEPS-a, 2018.

2.2 Organiziranje napada na ATM

Priprema napada može trajati tjednima pa čak i mjesecima. Prijestupnici moraju prikupiti potreban **alat i sredstva** poput vozila, opreme i kontaktnih točaka. **Vozila** su bitan alat za fizičke napade na ATM uređaje; počinitelji uglavnom putuju automobilom, a nakon napada najčešće bježe brzim vozilima. Ona su često ukradena, ali ih se također može unajmiti ili kupiti (npr. putem interneta). Većina **opreme** za fizičke napade na ATM uređaje (bankomate) brzo i legalno je dostupna u običnim dućanima. Time se dodatno spušta prag za ulazak u ovo područje kriminala. Praćenje porijekla alata je teško za provoditelje zakona pa su zato rizici za počinitelje ograničeni. Organizirane kriminalne skupine (OCG-ovi) koje su aktivne u fizičkim napadima na bankomate na međunarodnoj razini gotovo uvijek imaju kontaktne točke u ciljnoj zemlji (ljudi koji tamo žive određeno vrijeme) ili, alternativno, mogu primijeniti tehniku udari-i-bježi. Ti kontakti podržavaju OCG-ove logistikom, kao što je najam smještaja, nabavka vozila ili druge opreme te izviđanje ciljeva. Neki međunarodni počinitelji prepuštaju logistiku i izviđanje u potpunosti lokalnim kontaktima i putuju cestom ili zrakom samo u svrhu izvođenja napada na bankomat.

Organizirane kriminalne skupine (OCG-ovi) često izvode sveobuhvatno **izviđanje** kako bi identificirale pogodne ciljeve; procjenjuju doba dana kada se bankomat puni, okruženje bankomata, tehničke posebnosti bankomata, rute za bijeg i sigurnosne mjere koje postoje, poput videonadzora (CCTV), senzora alarma i zasuna.

Neki OCG-ovi prije napada poduzimaju brojne radnje **kako bi obeshrabrili službe za provedbu zakona i sigurnosti**. Oni onesposobljavaju alarmne sustave i javnu rasvjetu, koriste se tehnikama preusmjeravanja, postavljaju blokade na cestama ili pokušavaju onesposobiti vozila službi za provođenje zakona.

2.3 Iskustvo i znanje počinitelja

Fizički napadi na bankomate privlačni su kriminalcima, jer je novac odmah dostupan i nema potrebe za opsežnom mrežom za prodaju ukradene robe. To je pogodna alternativa za kriminalce koji su već aktivni u organiziranom imovinskom kriminalu.

Organizirane kriminalne skupine moraju steći **potrebnu stručnost i tehničko znanje**, jer su oni odlučujući faktor uspjeha ili neuspjeha napada. Potrebna stručnost i tehničko znanje snažno ovise o **vrsti napada**. Napadi izbijanjem/probijanjem i oni *na licu mjesta* imaju jednostavan MO (uglavnom hrabrost i upotrebu grube sile), tako da uglavnom ne zahtijevaju posebne vještine. Napadi zapaljivim plinom i napadi krutim eksplozivima zahtijevaju višu razinu stručnosti.

Napadači pokazuju različite **razine stručnosti**. S jedne strane, visoko organizirane i iskusne skupine mogu izvesti uspješan fizički napad na ATM u roku od nekoliko minuta. One kontroliraju postupak i sposobne su same ograničiti rizik, čime ograničavaju i kolateralnu štetu. S druge strane, manje organizirane i oportunističke skupine često ne uspijevaju u svojim pokušajima i mogu prouzročiti značajnu štetu na objektima i zgradama u susjedstvu. Vjeruje se da će se neki od slabije organiziranih OCG-ova vratiti tradicionalnim aktivnostima organiziranog imovinskog kriminaliteta, obeshrabreni preventivnim mjerama koje nisu u stanju prevladati pri napadu na bankomate.

3 Potreba za preventivnim pristupom

Zemlje u kojima počinitelji imaju niske stope uspjeha pri fizičkim napadima na ATM uređaje ili u kojima se broj fizičkih napada na ATM uređaje smanjuje, pokazuju da se uspješan pristup suzbijanju fizičkih napada na ATM uređaje sastoji od kombinacije operativnih i preventivnih mjera. Kako je broj organiziranih kriminalnih skupina aktivnih na ovom području zločina ograničen, uhićenja i posljedično kažnjavanje članova organiziranih kriminalnih skupina značajno smanjuje broj napada. Međutim, nakon oslobađanja, mnogi napadači na bankomate ponovno pokreću svoje aktivnosti. Štoviše, skupina ponekad može brzo zamijeniti uhićenog počinitelja. Stoga postoji snažna potreba za preventivnim mjerama, po mogućnosti ugrađenima u zakonodavni okvir. Nadalje, iskustvo pokazuje da mjere prevencije u jednoj zemlji mogu organizirane kriminalne skupine usmjeriti prema ranjivijim ciljevima u drugim zemljama. Samo je pitanje vremena kada će se modi operandi koji su se pojavili u jednoj zemlji proširiti na druge zemlje. To jsno ukazuje na **potrebu usvajanja preventivnih i operativnih mjera na europskoj razini** s privatnim, javnim i partnerima za provedbu zakona koji usko surađuju.

4 Prevencija

Za sprječavanje i suzbijanje ove vrste kriminala potrebna je jasna strategija. U ovom ćemo poglavlju dati pregled triju koraka koji se obično poduzimaju kada se suočimo s fizičkim napadima na bankomate ili se pripremamo za njihovo sprječavanje.

Prije svega **procjena situacije**; treba utvrditi profil rizika ATM uređaja i njegove okoline uzimajući u obzir količinu raspoloživog novca (moguću pljačku), rizik kolateralne štete i rizik od osobnih ozljeda. Kao drugo, na temelju procjene rizika trebalo bi razviti **preventivnu strategiju**. Na kraju treba provesti **preventivne mjere**.

4.1 Procjena situacije

Organizirane kriminalne skupine uglavnom ciljaju na posebne vrste bankomata ili bankomate određenih pružatelja usluga čije značajke olakšavaju napad na bankomat. Zato je potrebno provesti temeljitu procjenu rizika od fizičkih napada na bankomate, po mogućnosti uključujući cijeli lanac sigurnosti novca od tranzita do isporuke za pohranu u bankomat. Kako bi se uspostavio profil rizika za svaki od ATM uređaja, potrebno je analizirati brojne elemente uključujući sljedeće.

- Karakteristike lokacije postavljanja i okruženja bankomata; značajke poput gradskog ili ruralnog područja, gustoća naseljenosti, blizina policijskih postaja, kamere za automatsko prepoznavanje registarskih tablica (ANPR) u susjedstvu, videonadzor u blizini itd.
- Lokacija ATM-a:
    - unutar ili izvan zgrade, u poslovnici banke ili u udaljenim (npr. komercijalnim) prostorijama, ugrađeni ili pričvršćeni na zgradu,
    - za samostalni ATM: bilo da je učvršćen ili ne.
    - kod bankomata ugrađenih ili pričvršćenih na zgradu: postoje li arhitektonske slabosti, kako je organizirano spremanje novca itd.
- Vrsta ATM-a.
- Sigurnosne funkcionalnosti uključene u ATM.
- Količina gotovine u ATM uređaju.
- Vrsta fizičkih napada na ATM uređaje i MO-i koje treba očekivati kako bi se najprije usvojile najprikladnije mjere prevencije.
- Već poduzete sigurnosne i preventivne mjere (inteligentni sustavi neutralizacije novčanica (IBNS), videonadzor (CCTV), sustav sigurnosne magle (smanjenje vidljivosti) itd.).

Ostali elementi koje treba ocijeniti su stanje suradnje s partnerima i dionicima te zakonodavstvo. Suradnja između tijela za provođenje zakona, privatnih i javnih partnera trebala bi se ocijeniti u svrhu stvaranja saveza za borbu protiv kriminala. Moguće je da svaki partner posjeduje zanimljive informacije koje mogu pridonijeti procjeni situacije. Lokalna policija ili lokalne vlasti osobito su važne unutar tog okvira. Zakonodavstvo se mora vrednovati u smislu uspostavljanja pravnog okvira za prevenciju, poduzimanja obaveznih mjera prevencije, izricanja kazni za napade na ATM uređaje itd.

4.2 Razvoj preventivnog pristupa

Nakon što se procijeni situacija i utvrde glavna područja rizika te snaga i slabosti u sigurnosti bankomata, može se izraditi strategija (koja se često nadograđuje na suradnju između javnog i privatnog sektora) i mogu se uspostaviti preventivne i operativne mjere suzbijanja. Mjere prevencije trebale bi biti usmjerene na smanjenje namjere i sposobnosti počinitelja. Da bi se to postiglo, predložene su tri okosnice preventivnih akcija temeljene na tri od pet strategija prevencije situacijskog kriminala po Clarkeu ([2]); smanjenje nagrada, povećanje rizika za počinitelje i povećanje napora za pristup plijenu.

Kriminalci uspostavljaju ravnotežu povrata koja se očekuje i pridruženi rizik (npr. s napadom na ATM). Smanjenje šansi za ostvarivanje nagrade na lak način i povećanje rizika za počinitelje smanjuje njihova očekivanja i želju da se uključe u fizički napad na ATM. Daljnje mjere koje povećavaju napor potreban za pristup bankomatu utječu na sposobnosti počinitelja. Oportunistički počinitelji, koji često ne uspijevaju u svojim pokušajima, prestaju se baviti napadima na ATM uređaje. Za profesionalne napadače na ATM uređaje stopa uspješnosti se smanjuje, što opet utječe na ravnotežu povratka/rizika.

Nadalje, paralelne mjere kao što su učinkovita medijska strategija, rana socijalna prevencija i mjere za smanjenje rizika od kolateralnih šteta na zgradama i za osiguranje sigurnosti lokalnog stanovništva, osoba iz službi za pružanje pomoći i prolaznika, upotpunjuju strategiju prevencije.

([2]) Derek Cornish i Ronald V. Clarke, 'Prilike, prijestupnici i kaznene odluke: odgovor na Wortleyevu kritiku situacijskog sprječavanja kriminala', *Studije o prevenciji kriminala 16* (2003), 41-96.

Mogući su i drugi načini strukturiranja pristupa. U Nizozemskoj vlasti primjenjuju takozvani model prepreka ([3]). Taj model identificira korake koje zločinac mora poduzeti da bi počinio zločin. Također identificira partnere i mogućnosti koje omogućuju zločin te je koristan instrument kojim se može organizirati postupak prikupljanja informacija na području zločina. Identificiranjem svakog koraka potrebnog za izvršenje fizičkog napada na ATM mogu se utvrditi prepreke za opstrukciju zločina i najbolji partneri za postavljanje prepreka. Model prepreka također identificira signale koji upozoravaju javne i privatne partnere na fizičke napade na ATM uređaje i signale koje oni mogu poslati sami kako bi obavijestili vlasti o svojim sumnjama.

Potrebna je dobro razvijena strategija za ublažavanje rizika koji idu u kombinaciji s jačanjem prevencije. Preventivne mjere koje su vrlo učinkovite u obeshrabrivanju amatera i oponašatelja, ponekad imaju neželjene učinke. Neke se skupine okreću metodama pokušaja i pogreške kako bi pronašle ranjive bankomate, ostavljajući trag oštećenih ATM uređaja. Opasnije i nemilosrdnije organizirane kriminalne skupine počinju primjenjivati nasilnije MO-e, poput prelaska s plina na kruti eksploziv u svojim napadima.

Kako bi se uspostavio učinkovit skup preventivnih mjera, najbolja je praksa postavljanje nacionalnog tijela koje je ovlašteno nametati specifične mjere za visokorizične ATM uređaje na osnovi temeljite analize situacije. Ovaj se pristup pokazao učinkovitim u Francuskoj, posebno ako je uspostavljen pravni okvir i mjere se provode zajedno s operativnim mjerama.

4.3 Implementacija preventivnih mjera

Mjere uvedene u ovom poglavlju za sprječavanje fizičkih napada na ATM uređaje pokazale su svoju iskoristivost u različitim zemljama. Oni se temelje na zaključcima konferencije o prevenciji i na preventivnim mjerama koje aktivno promiču međunarodne organizacije koje djeluju na području sigurnosti ATM uređaja. Mnoge mjere su dobro poznate. Nekoliko je zemalja već uspješno uvelo niz mjera. Međutim, često se predložene mjere uvode samo djelomično i nisu ugrađene u zakonodavstvo.

Kao što je gore spomenuto, predložene su tri okosnice preventivnih djelovanja: smanjenje nagrade, povećanje rizika za počinitelje i povećanje napora potrebnog za pristup plijenu.

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

4.3.1 Smanjenje nagrade

Smanjenje nagrade od kaznenih djela prva je okosnica u sprječavanju fizičkih napada na bankomate. Sve dok postoji percepcija o 'lakom novcu', kriminalci će se baviti ovom vrstom kriminala. Smanjivanje količine raspoloživog novca i uklanjanje ili uništavanje gotovine, smanjuje mogućnosti za postojanje zanimljivog plijena. Smanjena očekivanja smanjuju želju kriminalca da se uključi u ovu vrstu kriminala.

4.3.1.1 *Smanjenje količine novca*

Jedna od mjera za smanjenje nagrade je smanjivanje količine gotovine dostupne u bankomatu. U idealnom slučaju taj iznos treba biti ograničen na iznos potreban za samo jedan dan trgovanja. Suradnja između banaka mogla bi osigurati isplativost. U Nizozemskoj je nekoliko banaka surađivalo na uspostavljanju mreže ATM uređaja neovisnih o bankama, nazvane 'Geldmaat'. Cilj suradnje je osigurati dostupnost, pristupačnost, raspoloživost i sigurnost gotovine. To će vjerojatno dovesti do smanjenja broja bankomata. Međutim, nijedan ATM uređaj neće sadržavati više gotovine, već će se češće puniti. Broj punjenja prilagodit će se potrebama.

Budući da prijestupnici bankomate uglavnom napadaju između 03.00 i 04.00, preporučuje se da se samostojeći bankomati (uglavnom smješteni u komercijalnim i javnim prostorima, koji su ranjiviji) isprazne i da se gotovina prebaci u sef na kraju dana. Znakom upozorenja može se obavijestiti javnost da u bankomatu noću nema novca. Sljedećeg dana bankomat treba napuniti izvan vidokruga klijenata i u zaključanom objektu. Ovaj se sustav primjenjuje u Francuskoj gdje zakonodavstvo obvezuje trgovce da iz samostojećih ATM uređaja koje imaju u dućanu noću vade novac i ATM uređaj ostavljaju otvorenim. Kod ostalih bankomata zadržane količine mogu se smanjiti povećanjem učestalosti punjenja.

4.3.1.2 *Upropaštavnje plijenja i činjenje novca sljedivim*

Sustavi inteligentne neutralizacije novčanica (IBNS) prva su tehnika za upropaštavanje nagrade. Ovi sustavi mrljaju novčanice tintom kako bi ih označili kao ukradene. U IBNS tintu mogu se dodati obilježivači i markeri. U ovom trenutku ovi se markeri uglavnom upotrebljavaju u forenzičke svrhe, povezujući novčanicu s mjestom zločina i povećavajući rizik počinitelja da bude uhvaćen. Iako je IBNS učinkovita preventivna mjera, postoje određeni problemi.

Europska središnja banka ne nadoknađuje zamrljane novčanice ([4]) (od 2003.), ali neke od nacionalnih središnjih banaka zemalja članica EU-a i dalje to čine. Zamrljane novčanice ponovno uvode u legalni sustav putem kockarnica. IBNS stvara dodatnu prepreku za kriminalce, ali bio bi mnogo učinkovitiji kad bi kriminalcima bilo nemoguće upotrebljavati zamrljane novčanice u EU-u. Kako bi se to postiglo, nacionalne središnje banke ne bi trebale prihvaćati zamrljane novčanice. Iznimke se mogu napraviti za posebne okolnosti, poput zamrljanja novčanica prilikom lažne aktivacije. Također je važno savjetovati stanovništvu da ne prihvaća zamrljane novčanice. Dugoročno gledano, uređaji za prihvat novčanica trebali bi otkriti obojene novčanice, a trebali bi biti instalirani u bankama i u komercijalnim prostorima kao što su kockarnice, autopraonice itd. Otkrivanje tinte je teško i skupo, no isplativo rješenje bi moglo biti instaliranje infracrvenih sustava koji otkrivaju novčanice obojene infracrvenim markerima. Ovi su sustavi dokazali svoju učinkovitost i najbolja su praksa u Belgiji i Francuskoj. Kada se u bankomat unesu novčanice s infracrvenim markerima, bankomat će prihvatiti ('progutati') novac, ali neće ga uplatiti na račun. Osoba koja je unijela obojene novčanice također bi trebala biti registrirana.

Postoje i neki drugi aspekti pri instaliranju IBNS rješenja. Razni proizvođači pružaju niz IBNS rješenja s različitim mehanizmima aktivacije i različitim vrstama tinte. Prvo razmatranje odnosi se na činjenicu da se ne mogu sve vrste aktivacijskih tehnologija za IBNS suprotstaviti svim prijetnjama. Neki IBNS-ovi funkcioniraju vrlo dobro kod napada probijanjem/razbijanjem, napadima *na licu mjesta* i napade plinom, ali ne funkcioniraju u slučaju napada krutim eksplozivnim sredstvima ili obrnuto. Stoga se izabrana tehnologija treba dobro razmotriti.
Razmatra se i vrsta tinte koju treba odabrati. U Belgiji su postavljeni nacionalni minimalni zahtjevi za IBNS (sigurnosni, postotak obojenih, koji se ne mogu prati itd.), a neovisna ispitivanja potvrđuju da sustav ispunjava nacionalne standarde i da djeluje u skladu s tvrdnjama proizvođača. Važno je testirati na stvarnim novčanicama, jer na tržištu postoje jeftinije tinte koje dobro funkcioniraju s krivotvorenim/lažnim novčanicama, ali ne i s pravim novčanicama: što znači da se tinta ispiranjem može ukloniti s pravih novčanica. Uz sve to, preporučuje se da se tinti dodaje forenzički marker kako bi se omogućila istraga povezanosti između obojenih novčanica i određenog mjesta zločina.

Najbolja praksa pokazuje da IBNS može biti vrlo učinkovit, posebno u kombinaciji s drugim preventivnim mjerama. Godine 2015. Francuska je uvela novo zakonodavstvo, uključujući članke o instaliranju IBNS-a i uporabi tinte s jedinstvenom DNK. Francuska vojna policija (žandarmerija) na

([4]) Odluka Europske središnje banke, denominacije, specifikacije, umnožavanje, razmjena i povlačenje novčanica eura, 2003.

temelju procjene rizika odlučuje gdje se mora primijeniti IBNS i druge mjere. Budući da je novo zakonodavstvo ojačalo preventivni i operativni pristup, broj napada smanjio se s 300 u 2013. na 50 u 2018. godini.

Još jedna od tehnika koje se razvijaju kako bi upropastila plijen je **ljepilo**. Učinkovitost ljepila dokazana je u Nizozemskoj, ali trenutačno su visoki troškovi implementacije te tekući troškovi. Štoviše, ljepilo može predstavljati opasnost od požara ako se sustav ne aktivira prije napada, jer bi raspršivanje čestica ljepila u zraku moglo stvoriti zapaljivu smjesu. Ova metoda još nije spremna za tržište, ali mogla bi predstavljati rješenje za budućnost.

4.3.2 Povećanje rizika

Druga okosnica za sprječavanje fizičkih napada na ATM uređaje jest odvraćanje potencijalnih počinitelja od počinjenja kaznenih djela povećanjem rizika od otkrivanja i kažnjavanja. Osim rizika od tjelesnih ozljeda tijekom upotrebe eksploziva pri napadu na ATM uređaje, glavni rizik za kriminalca je zatvorska kazna ako je uhvaćen na djelu ('uprljanih ruku') ili uslijed istrage. Kako bi se smanjila želja potencijalnih počinitelja, treba povećati rizik otkrivanja i kažnjavanja. Naravno, za društvo je hvatanje i osuđivanje zločinaca također vrlo učinkovita metoda prevencije ako postoji posljedična kazna, kao što smo vidjeli u nekoliko država.

4.3.2.1 *Djeljenje informacija*

Ključno u otkrivanju i kažnjavanju napadača na ATM uređaje je razmjena informacija između svih dionika u borbi protiv fizičkih napada na ATM uređaje, uključujući pružatelje usluga bankomata, tijela za provedbu zakona (policija, tužilaštvo itd.), tijela javne vlasti, proizvođače bankomata i uređaja za sigurnost i zaštitu, profesionalna udruženja, pružatelje usluga bankomata (banke i neovisni isporučitelji), zaštitarske tvrtke i alarmni centri. Idealno bi bilo da je to i na nacionalnoj, i na međunarodnoj razini.

Rano otkrivanje nadolazećeg fizičkog napada na ATM je teško. Rano otkrivanje moguće je samo u slučajevima s gotovo besprijekornom razmjenom informacija na međunarodnoj razini između partnera u provođenju zakona i privatnih partnera (zaštitarske tvrtke i pružatelji usluga bankomata). Potrebno je pratiti širok spektar pokazatelja, uključujući rane poruke upozorenja između tijela za

provedbu zakona o OCG-u u pokretu, informacije o ('vrućim') vozilima koja su korištena u napadima na bankomate, informacije sigurnosnih tvrtki ili susjednih stražara o otkrivenom sumnjivom ponašanju na području oko bankomata, sumnjive transakcije koje su otkrili pružatelji usluga bankomata te druge metode ispitivanja. Ostale moguće policijske mjere za rano otkrivanje su praćenje ukradenih automobila, proizvođača i distributera eksploziva te tvrtki ovlaštenih za upotrebu eksploziva. Napori potrebni za postizanje ranog otkrivanja zahtjevni su i ne jamče uspjeh, stoga su intervencije u smislu provođenja zakona prije napada rijetke.

Ako rano otkrivanje nije moguće, alarmni centri mogu brzo izdati upozorenje u slučaju fizičkog napada na bankomat. Kako bi se omogućila intervencija, moraju se dogovarati i uspostaviti nacionalni propisi i protokoli za brzu komunikaciju između alarmnih centara i tijela za provođenje zakona. U slučaju informacija uslijed ranog otkrivanja ili informacija u stvarnom vremenu, provedba zakona uvijek će morati procijeniti vrijeme i najbolju priliku za intervenciju. Hvatanje kriminalaca na djelu vrlo je teško i može dovesti do opasnih situacija, jer su neke organizirane kriminalne skupine vrlo nasilne i koriste teško naoružanje.

Za uspješnu istragu nakon fizičkog napada na bankomat službenici za provedbu zakona moraju komunicirati sa svim sudionicima, jer bi svaki od njih mogao imati podatke koji pridonose uspjehu istrage. Naravno, potrebna je komunikacija i suradnja s primarnim žrtvama, bankama ili drugim pružateljima usluga bankomata: oni imaju pristup podacima koji su važni za istragu. Kod pružatelja usluga bankomata informacije policijske službe pomoći će poboljšati mjere prevencije. Nadalje, kontakti s profesionalnim udruženjima i proizvođačima pokazali su se korisnima: ona često šalju sigurnosno-upozoravajuće poruke na koje se drugi zainteresirani sudionici mogu predbilježiti. Proizvođači ATM uređaja imaju dobar uvid u različite vrste napada na ATM uređaje i odgovarajuće slabosti i prednosti mjera prevencije. Oni su vrlo voljni pružiti podršku policiji s informacijama o tehničkim aspektima ATM uređaja i MO-ija koji se primjenjuju.

Prekogranična suradnja je od ključne važnosti: zemlje bi trebale razmjenjivati informacije (o osumnjičenima, osuđenim napadačima na bankomate, MO-ima, sumnjivim vozilima, slikama napada itd.), ne samo kao podrška istrazi, već i zbog toga što osumnjičeni osuđenici u drugoj zemlji mogu biti kažnjeni za ponavljanje kaznenog djela/recidivizam.

U konačnici, stvaranje baze podataka na europskoj razini, dostupne službama za provedbu zakona i koje sadrže forenzičke podatke (npr. o različitim vrstama IBNS tinte, tragova i markera ili zaštitnom staklu bankomata), moglo bi snažno podržati istrage i povezati osumnjičene s određenim mjestom

zločina. Standardizacija tehnologije na međunarodnoj razini često je nedovoljna: tijekom konferencije u siječnju 2019. sudionici su spomenuli kako bi standardizacija tinta i oznaka kriminala na razini EU-a mogla uvelike olakšati istrage.

4.3.2.2 *Videonadzor (CCTV) i uređaji za slušanje*

Slikovni i zvučni podaci iz sustava videonadzora (CCTV) i uređaja za slušanje mogu podržavati otkrivanje napada u stvarnom vremenu (npr. da se spriječi fizičko ozljeđivanje prvih osoba koje stignu na mjesto zločina) i naknadne istrage (npr. radi identificiranja počinitelja i njihovih MO-ija). Slike videonadzora mogu se kombinirati sa slikama iz javnih i drugih CCTV sustava u susjedstvu ATM uređaja i prometnim radarskim snimcima kako bi se dobila cjelovitija slika počinitelja i njihovog MO-ija.

No, slika videonadzora često je loše kvalitete ili loše pohranjena. Slike bi trebale biti dovoljno kvalitetne da omoguće identifikaciju osobe. Ponovno, postavljanje europskih standarda za sigurnosni videonadzor olakšalo bi istrage. Budući da počinitelji često onemoguće CCTV kamere prije napada, također bi se mogla razmotriti instalacija nevidljivog videonadzora ili uređaja za slušanje u stvarnom vremenu.

4.3.2.3 *Kazna i rehabilitacija prekršitelja*

Pokazalo se da dosljedna i stroga kazna ima preventivni učinak. Uhićenje organizirane kriminalne skupine neposredno utječe na broj napada na ATM uređaje. Međutim, puštanje napadača na bankomate iz zatvora također često dovodi do novog porasta napada. To znači da male kazne dovode do toga da počinitelji ponovno budu vrlo aktivni. Minimalne i maksimalne kazne za zločince osuđene za pojedinu vrstu fizičkog napada na ATM razlikuju se među državama članicama. Neki vjeruju da će veće kazne odvratiti potencijalne počinitelje. Međutim, znanstvena istraživanja ([5]) pokazuju da povećanje strogosti kazni ne mora nužno pojačati učinak odvraćanja od počinjenja. Zato bi moglo biti zanimljivo pogledati popravne programe (i one bazirane na prijestupnicima) rehabilitacije kako bi se smanjila visoka stopa recidivizma.

([5]) David Weisburd, David P. Farrington i Charlotte Gill, 'Zaključak: Što funkcionira u prevenciji kriminala, revidirano', David Weisburd, David P. Farrington i Charlotte Gill, *Što funkcionira u prevenciji zločina i rehabilitaciji*. Cambridge: Springer, 2016, 311.

4.3.3 Povećanje napora

Treća okosnica za sprječavanje fizičkih napada na ATM uređaje sadrži radnje koje počinitelju počinjenje kriviČnog djela čine zahtjevnijim.

4.3.3.1 *Osiguranje okruženja otpornog na kriminal*

Ako procjena rizika (vidjeti prethodni tekst) pokaže da se ATM uređaj nalazi u okruženju visokog rizika, lokaciju treba rastaviti i bankomat prenijeti u područje niskog ili srednjeg rizika. Takav slučaj je sigurno ako analiza pokazuje da bi se zgrada mogla srušiti ako se na ATM uređaj izvrši napad eksplozivom. Za podršku takvim mjerama u visokorizičnim slučajevima moglo bi se uključiti zakonodavstvo. Osim smanjenja broja ATM uređaja u okruženjima visokog rizika, potrebno je poticati bezgotovinsko plaćanje kako bi se smanjila potreba za bankomatima.

Ako ATM nije moguće premjestiti, treba poduzeti maksimalne mjere sigurnosti: npr. uporaba protuprovalnih zaslona, rasvjetnih stupova i druge ulične opreme za ograničavanje pristupa zgradi, sustava za zaustavljanje vozila, instalacija odgovarajuće ulične rasvjete, pojačani neskriveni ili prikriveni nadzor i uređaji protiv krađe, poput sustava degradacije novčanica. Kada je napadnuta lokacija koja nije identificirana kao lokacija visokog rizika, trebala bi se prepoznati kao takva i dodati joj se dodatne sigurnosne mjere. U alatu za procjenu rizika treba uzeti u obzir nove čimbenike kako bismo ga ažurirali. Ponovna procjena ovog rizika trebala bi se sustavno ponavljati.

4.3.3.2 *Ojačavanje ATM uređaja*

Proizvođači ATM uređaja nude standardni asortiman ATM uređaja s nizom sigurnosnih značajki koje se ocjenjuju prema stupnju sigurnosti Europskog odbora za normizaciju (CEN). ATM uređaji obično imaju oznaku CEN u rasponu od nižeg stupnja CEN1 do najvišeg, CEN4. Značajke poput snage tijela i otpornosti na napade određuju stupanj. Otpornost na plin uglavnom se nudi kao opcija (CEN-GAS). Standardni modeli se mogu poboljšati dodatnim mjerama zaštite. Obično treće strane instaliraju ove značajke kako bi osigurale usklađenost s lokalnim zakonodavstvom i prilagođavanje osnovnog modela potrebama lokalnih klijenata. Dodatne sigurnosne značajke uključuju razne senzore za aktiviranje sustava za neutralizaciju plina ili IBNS-a u slučaju napada *in situ* ili napada eksplozivima te poboljšane zasune i brave na trezorima kako bi se spriječio neovlašteni pristup sefu tamo gdje je

glavni zatvarač oštećen. Kod prijenosnih, samostojećih bankomata važno je upotrebljavati sustave sidrenja koji nude dodatnu zaštitu od provale/probijanja. Sustavi praćenja mogu biti uključeni u ATM uređaj kako bi se pružila podrška istražiteljima kada se ATM uređaj transportira na drugo mjesto prije otvaranja.

4.3.3.3 *Arhitektonske mjere*

Prilikom instaliranja ATM uređaja preporučuje se uporaba uređaja sa stražnjim pristupom. U tom slučaju počinitelj mora ući u zgradu i dobiti pristup stražnjem dijelu uređaja kako bi ukrao novac. Prijenosni, samostojeći bankomati najviše su ranjivi. Smanjenje broja tih bankomata povećalo bi sigurnost. Obveza postavljanja ATM uređaja u sobu osiguranu protiv provale automatski bi smanjila upotrebu samostojećih bankomata.

4.3.3.4 *Sustav zamagljivanja*

Topovi za maglu brzo ispunjavaju prostoriju gustom maglom, tako da uljez ništa ne vidi. Ova sigurnosna magla često onemogućuje izvršenje napada na ATM. U najmanju ruku, sustav usporava počinitelja, ostavljajući policiji vrijeme za intervenciju. Sustav sigurnosne magle povezan je s alarmnim sustavom i može se aktivirati na dva načina. Može se aktivirati automatski senzorima alarma, poput detektora kretanja (noću) ili senzorima za manipulaciju zasunom na ATM-u. Također ga može aktivirati alarmni centar kako bi se izbjeglo previše lažnih alarma. Kod vanjskih bankomata ugrađenih kroz zid, sustav zamagljivanja može se primijeniti na stražnjem dijelu bankomata kako bi se prostorija iza ispunila maglom, a vidljivost počinitelja smanjila do ništice.

Sustavi zamagljivanja mogu pružiti točku zaštite bankomata koji se nalaze na otvorenim prostorima na benzinskim stanicama, supermarketima itd. Tako se izbjegava da magla ispuni cijelo područje. Zaštita zamagljivanjem najuspješnija je kada magla dolazi iz različitih uglova ili kada ispunjava prostor iza bankomata u slučaju
probijanja. U tijeku su ispitivanja mogu li se topovi s maglom postaviti unutar samog ATM uređaja, umjesto u prostoriji u kojoj se ATM uređaj nalazi. U maglu se mogu dodati DNK markeri koji oboje počinitelje i njihovu odjeću.

4.3.4 Paralelne mjere

Kako bi se osigurala učinkovita i djelotvorna provedba prethodno spomenutih mjera prevencije, potrebno je uzeti u obzir niz paralelnih mjera. Ove su mjere neophodne za omogućavanje ili jačanje holističkog preventivnog i operativnog pristupa u borbi protiv fizičkih napada na ATM uređaje.

4.3.4.1 *Zaknodavstvo*

U velikom broju zemalja zakonodavstvo obvezuje pružatelje usluga bankomata na poduzimanje preventivnih mjera. U drugim zemljama uspostava dogovora i sporazuma između banaka i agencija za provođenje zakona osigurava dobro vođen pristup u rješavanju fizičkih napada na bankomate. Područja u kojima se mogu uzeti u obzir regulatorne mjere obuhvaćaju:

- ugradnja preventivnih mjera;
- pravni okviri koji omogućuju suradnju između tijela za provedbu zakona i javnih i privatnih partnera;
- prepravljanje odmjeravanja kazni ako su kazne za počinitelje fizičkih napada na ATM uređaje preniske.

Međutim, često su samo bankarske institucije to dužne poštivati, a neovisni pružatelji ATM uređaja nisu vezani ovim zakonima ili sporazumima. To je obično slaba točka regulatornog okvira.

Neke zemlje ne provode nikakvu regulativu, ali pokušavaju uvjeriti pružatelje usluga bankomata da poduzmu preventivne mjere podižući svoju svijest o područjima kriminala i trendovima: u zemljama s velikim brojem neovisnih banaka ovo se pokazuje osobito teškim.

Nužno je osigurati da učinkovita provedba preventivnih mjera obuhvati promjene u zakonodavstvu i regulativi, kako na nacionalnoj, tako i na međunarodnoj razini, koja obvezuje sve vrste pružatelja usluga bankomata. Idealno bi bilo zakonodavstvo uskladiti na razini EU-a kako bi se izbjeglo da snažne preventivne mjere ugrađene u zakonodavstvo jedne zemlje dovode skupine organiziranog kriminala u druge zemlje, one s manje strogim propisima.

4.3.4.2 *Medijska strategija*

Druga važna osovina u preventivnoj strategiji je dobro utvrđena medijska strategija, koja ima za cilj smanjiti očekivanja i želju napadača na ATM uređaj da sudjeluju u ovom kriminalnom djelu. Treba

naglasiti niske stope uspjeha i velike rizike za počinitelje; komunikacija o nagradama ('plijenu') ili pojedinostima o napadu na ATM uređaj, kao što su vrsta napadnutog ATM-a ili izbjegnutog MO-a. S druge strane, potrebna je opsežna komunikacija o uhićenjima osumnjičenih i posljedičnim kaznama nakon presude.

4.3.4.3 *Poboljšana suradnja*

Poboljšana suradnja i razmjena informacija često se spominju, ali ne može se dovoljno naglasiti. Operativna razmjena informacija na međunarodnoj razini temeljna je djelatnost Europola. Osim ove razmjene informacija, konferencija o prevenciji pokazala je jasnu potrebu za povećanjem multidisciplinarne i višerazinske suradnje i razmjene informacija između svih relevantnih dionika, uključujući agencije za provođenje zakona, javna tijela, proizvođače ATM uređaja i sigurnosnih i zaštitnih uređaja, profesionalna udruženja, pružatelje usluga bankomata (banke i nezavisni davatelji usluga), zaštitarske tvrtke i alarmni centri. To mora uključivati lokalnu, nacionalnu i međunarodnu razinu.

4.3.4.4 *Smanjenje rizika od kolateralnih šteta*

U slučaju napada krutim eksplozivom, neke organizirane kriminalne skupine (OCG) ostavit će materijal iza sebe. Ovo može stvoriti opasne situacije za osobe iz službi za pomoć ili civile (koji žive u susjedstvu ili prolaze pored). Potrebno je osigurati njihovu sigurnost. Kao što je to slučaj u Belgiji, protokoli i postupci kojih se trebaju pridržavati osobe koje prve stižu na poprište (kako one iz tijela za provedbu zakona, tako i one koje pružaju uslugu bankomata) moraju biti razvijeni i međusobno usklađeni. Druga najbolja praksa u tom kontekstu je primjer Nizozemske, gdje se snimka napada na ATM iz videonadzora upotrebljava za procjenu situacije. Mogu se sklopiti sporazumi s alarmnim centrima kako bi te slike bile odmah dostupne.

4.3.4.5 *Društvena prevencija*

Organizirane kriminalne skupine (OCG-ovi) često traže mlade ljude kako bi ih unovačili u svoje redove. Projekti bi se mogli uspostaviti tako da bi u početnoj fazi obeshrabrivali ove procese novačenja. Policija ili socijalni radnici trebali bi paziti u tim procesima i mogli bi intervenirati osobnim pristupom prema potencijalnim počiniteljima.

5 Zaključci

U posljednje 2 godine povećao se broj europskih zemalja pogođenih fizičkim napadima na bankomate. U tom smislu, Europol i EUCPN zajedno su radili na prikupljanju najboljih mjera za suzbijanje i sprječavanje ove vrste zločina.

Uspješan pristup suzbijanju fizičkih napada na ATM uređaje sastoji se od kombinacije operativnih i preventivnih mjera, po mogućnosti ugrađenih u zakonodavni okvir. Kako bi se izbjeglo da snažne mjere u jednoj zemlji usmjere organizirane kriminalne skupine (OCG) prema ranjivijim zemljama, preporučuje se usvajanje tih mjera na europskoj razini.

Za sprječavanje i suzbijanje ove vrste kriminala potrebno je uspostaviti jasnu strategiju u tri koraka: procjena stanja, razvoj preventivnog pristupa na temelju procjene rizika i provedba preventivnih mjera.

Procjena rizika za fizičke napade na ATM uređaje trebala bi sadržavati karakteristike ATM uređaja i njegove okoline, suradnju s partnerima i dionicima na izgradnji saveza za borbu protiv ovog kriminala i procjenu preventivnog i pravnog okvira. Nakon procjene situacije trebalo bi uspostaviti strategiju koja se temelji na suradnji javnog i privatnog sektora i preventivnim i operativnim protumjerama. Cilj preventivnih mjera je smanjenje namjere i sposobnosti počinitelja za anagažiranje u fizičkom napadu na ATM. Kako bi se to postiglo, predlažu se tri okosnice preventivnih aktivnosti: smanjenje nagrade, povećanje rizika i povećanje napora. Paralelne mjere trebaju upotpuniti strategiju prevencije. Najbolja praksa je uspostava nacionalnog tijela koje je ovlašteno nametati potrebne mjere.

Smanjenjem **nagrade,** smanjuje se želja kriminalca da sudjeluje u ovoj vrsti zločina. Smanjivanje količine novca u bankomatu ograničavanjem punjenja novca na onoliko koliko je dovoljno za samo 1 dan trgovanja ili pražnjenjem (najugroženijih) bankomata noću jedna je od mjera za smanjenje očekivanja počinitelja. Druga metoda je upropastiti plijen i novac učiniti sljedivim. U tom se kontekstu može primijeniti IBNS, koji zamrljava novčanice i označava ih kao ukradene. Ova je metoda najučinkovitija kada kriminalci ne mogu potrošiti taj novac ili te novčanice ponovno unijeti u legalni novčani sustav. To mogu postići banke i javnost svojim neprihvaćanjem zamrljanih novčanica pri plaćanju i instaliranjem uređaja za prihvat novčanica koji mogu otkriti i odbiti zamrljane novčanice. U tom smislu, ulaganje u infracrvene sustave koji otkrivaju zamrljane novčanice infracrvenim markerima pokazalo se kao isplativo rješenje u Belgiji i Francuskoj. Prilikom instaliranja IBNS-a zemlje trebaju temeljito razmotriti odabrane mehanizme aktiviranja, minimalne zahtjeve za neutralizaciju novčanica i dodavanje forenzičkog markera tinti.

Mjere koje odvraćaju potencijalne počinitelje od počinjenja kaznenih djela **povečavajući rizik** od otkrivanja i kažnjavanja, druga su okosnica za sprječavanje fizičkih napada na ATM uređaje. U otkrivanju i kažnjavanju napadača na ATM uređaje ključni su prikupljanje i razmjena informacija između svih dionika, kako na nacionalnoj, tako i na međunarodnoj razini. Razmjena informacija s visokokvalitetnih slika s videonadzora i zvučnim podacima može povećati šanse za rano otkrivanje i uspješnu istragu. Kako bi se izbjeglo da se uređaji videonadzora (CCTV) ili uređaji za slušanje onemoguće prije napada, može se razmotriti instalacija nevidljivog videonadzora ili uređaja za slušanje u stvarnom vremenu. Stvaranje forenzičke baze podataka i standardizacija tehnologija na europskoj razini mogli bi u velikoj mjeri olakšati međunarodnu suradnju i istrage. Ako se počinitelji uhvate i osude, moglo biti zanimljivo pogledati popravne programe (i one bazirane na prijestupnicima) rehabilitacije kako bi se smanjila visoka stopa recidivizma.

Treća okosnica za sprječavanje fizičkih napada na ATM uređaje obuhvaća mjere za **povećanje napora** koji je počinitelju potreban za izvršenje kaznenog djela. Postavljanje ATM uređaja u okruženju otpornom na kriminal s maksimalnim sigurnosnim mjerama učinit će napade na ATM uređaje zahtjevnijima za počinitelje. Nadalje, standardna zaštita ATM uređaja može se poboljšati nizom dodatnih sigurnosnih značajki. Povrh ovih mjera, postavljanje sustava za zamagljivanje može počinitelja odvratiti ili barem usporiti napad.

Brojne **paralelne mjere** ojačat će gore navedene mjere, kao što su stvaranje pravnog okvira koji obvezuje sve pružatelje usluga bankomata na provedbu preventivnih mjera, razvijanje dobro utvrđene medijske strategije, pojačana suradnja na lokalnoj, nacionalnoj i međunarodnoj razini, smjernice za osobe iz službi za pomoć, kako bi se smanjio rizik od kolateralne štete te ulaganja u socijalnu prevenciju kako bi se potkopali procesi novačenja u kriminalne skupine.

6 Preporuke za preventivni pristup: pregled

Razvoj učinkovitog odgovora kako spriječiti fizičke napade na ATM uređaje

Procjena situacije

Određivanje profila rizika ATM uređaja u svojoj zemlji/regiji
Identificiranje partnera i dionika u borbi protiv fizičkih napada na ATM uređaje i evaluacija suradnje
Evaluacija pravnog okvira za borbu protiv fizičkih napada na ATM uređaje na nacionalnoj i međunarodnoj razini.

Razvoj preventivnog pristupa

Određivanje (glavnih) rizika koje treba pokriti i prioriteta
Određivanje najboljih preventivnih mjera za obuhvaćanje tih rizika razmatrajući tri glavne okosnice.
Određivanje paralelnih mjera prevencije potrebnih za jačanje poduzetih mjera prevencije.

Mjere prevencije koje se mogu poduzeti		
Smanjenje nagrade	Povećanje rizika	Povećanje napora
– Smanjenje količine novca. ○ Pražnjenje ATM uređaja noću. ○ Povećanje broja/učestlosti ponovnih punjenja. – Upropaštavanje plijena. ○ Inteligentni sustav za neutralizaciju novčanica (IBNS). ○ Infracrveni markeri u IBNS tinti za otkrivanje znakova obojenja od strane primatelja novčanica. ○ U razvoju: ljepilo.	– Prekogranična razmjena informacija za: ○ rano otkrivanje ili otkrivanje u stvarnom vremenu mogućeg napada na ATM uređaj, ○ ačanje operativnog pristupa, ○ osuđivanje recidivista, ○ razmjena forenzičkih podataka na europskoj razini. – videonadzor (CCTV) i uređaji za slušanje. – Posljednja kazna i rehabilitacija prekršitelja	– Osiguranje okruženja otpornog na kriminal. ○ Promjena lokacije visokorizičnih ATM uređaja. ○ Sigurnosne mjere: fizičke zapreke, nadzor itd. – Ojačavanje bankomata zasunima, otpornim na plin ili krute eksplozive itd. – Arhitektonske mjere poput stražnjih strojeva za pristup – Sustavi sigurnosne magle.

Paralelne mjere za jačanje preventivnog pristupa

- Učinkovito zakonodavstvo, uključujući preventivne mjere protiv fizičkih napada na ATM uređaje, posljedične presude itd.
- Učinkovita medijska strategija koja obeshrabruje počinitelje.
- Pojačana suradnja između svih dionika (javnih, privatnih, tijela za provedbu zakona) u borbi protiv fizičkih napada na ATM uređaje.
- Smanjenje rizika od kolateralnih šteta za osobe iz službi koje pružaju pomoć ili civila (npr. onih koji žive u susjedstvu ili prolaze pored).
- Društvena prevencija kojom se izbjegavaju novačenja djece zbog (ove vrste) zločina.