Předcházení fyzickým útokům na bankomaty

Vyvíjení efektivního přístupu

Poděkování
Tento dokument je výsledkem spolupráce mezi agenturou Evropské unie pro spolupráci v oblasti vymáhání práva (Europol) a sekretariátem Evropské sítě pro předcházení trestné činnosti (EUCPN). Rádi bychom poděkovali odborníkům na fyzické útoky na bankomaty , kteří investovali čas a úsilí do vytvoření tohoto dokumentu obsahujícího doporučení. Přispěli tím, že se zúčastnili konference o prevenci fyzických útoků na bankomaty (leden 2019, Brusel) a poskytli zásadní informace. Zejména bychom rádi poděkovali trestněprávním orgánům ze zemí EU i z jiných zemí mimo EU, soukromému sektoru včetně organizací ATM Industry Association (ATMIA), BPost, Centrum voor Criminaliteitspreventie en Veiligheid (CCV), Diebold Nixdorf, the European Association for Secure Transactions Expert Group on ATM and ATS [„automatic teller safes“] Physical Attacks (EAST EGAP), European Intelligent Cash Protection Association (Euricpa), ING, Febelfin, NCR, Protect, SIOC Banking, Spinnaker a TMD Security, a dále ministerstvům vnitra Belgie, Chorvatska, Německa a Španělska.

Právní upozornění
Obsah této publikace nemusí nutně odrážet oficiální stanovisko kteréhokoli členského státu EU nebo jakéhokoli orgánu nebo instituce Evropské unie nebo Evropských společenství.

Obsah

1 Kontext

Vzhledem k rostoucímu počtu fyzických útoků na bankomaty a počtu postižených evropských zemí uspořádala Evropská síť pro předcházení trestné činnosti (EUCPN) a Europol v lednu 2019 konferenci, na níž se orgány činné v trestním řízení spojily s veřejnými a soukromými partnery s cílem věnovat se podrobněji předcházení této trestné činnosti. Tento dokument je charakteru doporučení a shrnuje závěry této konference s cílem zvýšit povědomí orgánů o fyzických útocích na bankomaty a preventivních opatřeních.

Širokou škálu různých metod (*modus operandi* neboli MO) používaných kriminálními živly k útokům na bankomaty lze dělit na dvě hlavní kategorie: fyzické útoky na bankomat a podvody související s bankomaty, kam patří útoky na logiku bankomatu a útoky s využitím škodlivého softwaru. Tato práce se zaměřuje na fyzické útoky na bankomaty, tj. násilné vniknutí do bankomatu pomocí fyzických prostředků za účelem odebrání hotovosti z přístroje. Násilné vniknutí lze provést pomocí:

- výbušných látek: útočníci použijí výbušniny v plynném nebo pevném stavu k fyzickému narušení trezoru bankomatu a k získání přístupu k hotovosti,
- násilná demontáž: útočníci bankomat fyzicky odeberou z prostředí, kde je přístroj instalován, často s použitím vysoce kvalitního a robustního vozidla,
- útoky poničením přístroje na místě: útočníci do trezoru proniknou hrubou silou, často pomocí řezného nebo bouracího nářadí (např. úhlové brusky, bourací kladiva nebo kyslíkoacetylénové hořáky).

Obavy z fyzických útoků na bankomaty má sice omezený, ale neustále rostoucí počet zemí v Evropské unii. V roce 2017 byla finanční ztráta v Evropě odhadnuta na více než 30 milionů EUR. Některé země jsou i nadále svědky značného počtu fyzických útoků na bankomaty, jiné významný nárůst počtu těchto incidentů zaznamenaly během posledních 2 let. Tato oblast kriminální činnosti se vyvíjí rychle. Některé země byly úspěšné v přístupu k řešení fyzických útoků na bankomaty a v poslední době zde došlo k výraznému snížení počtu útoků. Na druhé straně země, které předtím dotčeny nebyly, byly v roce 2018 konfrontovány s náhlým nárůstem fyzických útoků na bankomaty v důsledku rozšíření skupin organizovaného zločinu (SOZ) na svá území. Postiženy jsou přitom nejen banky – stále častěji se útočí na bankomaty jiných než bankovních provozovatelů, protože se často nacházejí ve zranitelnějších prostorách nebo lokalitách.

2 Faktory určující úspěch fyzického útoku na bankomat

Míra úspěšnosti útoků na bankomaty je nízká; úspěšná je pouze jedna třetina útoků. I když je však útok neúspěšný, stejně důležité jsou škody způsobené (např. výbušninami) konstrukcím staveb, kdy po útoku zůstává prostředí v blízkosti místa činu nebezpečné pro místní obyvatele, osoby zasahující na místě činu jako první a kolemjdoucí nebo projíždějící.

Úspěch fyzického útoku závisí na řadě faktorů, včetně vlastností bankomatu, technické přípravy provedení útoku i zkušeností a know-how pachatelů.

2.1 Zranitelnost bankomatů

Nejzranitelnějšími bankomaty jsou bankomaty umístěné venku a propojené s vnitřkem skrze zdivo, nebo přístroje stojící uvnitř budov. Při útoku na vnitřní (volně stojící) bankomat upřednostňují SOZ bankomaty umístěné v komerčních prostorách před bankomaty umístěnými v prostorách bank, kde je dohled obvykle silnější. Banky provozují zejména bankomaty umístěné uvnitř nebo vně budovy banky. Vzhledem k uzavírací době bankovních poboček postupně nabývají na významu bankomaty umístěné mimo lokalitu bank, např. na ulici nebo v komerčních prostorách, jako jsou čerpací stanice, supermarkety, hotely, kasina, letiště atd. Jiní než bankovní provozovatelé bankomaty provozují jako samostatné objekty. Jejich bankomaty se často nacházejí v maloobchodních prodejnách, v pohostinských a rekreačních zařízeních, v dopravních lokalitách(železniční stanice, letiště aj.), ve veřejných budovách a na ulici.

Vzhledem k rostoucí oblibě internetového bankovnictví bude v nadcházejících letech pravděpodobně mnoho bankovních poboček uzavřeno, což povede k celkovému snížení počtu bankomatů. ([1]) To by však mohlo vést ke zvýšení počtu bankomatů bank i nebankovních provozovatelů umístěných na daleko ohroženějších místech.

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

2.2 Technická příprava na útok na bankomat

Příprava útoku může trvat až několik týdnů nebo dokonce měsíců. Pachatelé musí shromáždit potřebné **nástroje a zdroje** –vozidla, vybavení, kontaktní místa aj. Základním nástrojem fyzického útoku na bankomat jsou **vozidla**– pachatelé cestují hlavně autem a po útoku nejčastěji unikají rychlým vozidlem. Tato vozidla jsou často vozidla odcizená, mohou být ale také najatá nebo zakoupená (např. přes internet). Většina **vybavení** pro fyzické útoky na bankomaty je snadno a legálně dostupná v běžných obchodech. Tím se dále snižuje práh pro vkročení do této oblasti trestné činnosti. Vysledování původu nástroje je v trestněprávním procesu obtížné, rizika pro pachatele jsou tak omezená. SOZ působící při fyzických útocích na bankomaty na mezinárodní úrovni mají téměř vždy kontaktní místa v cílové zemi (osoby, které tam po určitou dobu pobývají); případně jsou schopny rychle zasáhnout a uniknout. Tyto kontakty podporují SOZ pomocí logistiky – např. pronájem ubytování, nákup vozidla nebo jiného vybavení, a průzkum zájmové lokality. Někteří mezinárodní pachatelé logistiku i průzkum plně ponechávají na místních kontaktech a pouze dorazí na místo činu, vozem nebo letecky.

SOZ často provádějí rozsáhlý **průzkum** za účelem určení vhodných cílů útoku – posuzují denní dobu, kdy se bankomat plní hotovostí, jeho okolí, technické zvláštnosti, únikové cesty a zavedená bezpečnostní opatření, např. sledování bankomatu průmyslovou televizí , poplachové senzory a bezpečnostní uzávěry.

Některé SOZ podnikají před útokem řadu kroků, jejichž cílem je **ztížit práci trestněprávních složek a bezpečnostních služeb**. Jedná se o narušení funkčnosti poplašných systémů a veřejného osvětlení, odvádění pozornosti, zřizování překážek na silnici nebo pokusy o narušení funkčnosti zásahových vozidel.

2.3 Zkušenosti a know-how pachatelů

Fyzické útoky na bankomaty jsou pro zločince atraktivní, protože hotovost je okamžitě k dispozici a není třeba rozsáhlá síť pro prodej odcizeného zboží. Představuje vhodnou alternativu pro zločince, kteří již v oblasti organizovaného zločinu působí.

SOZ musí získat **potřebné odborné znalosti a know-how**, jelikož se jedná o rozhodující faktory úspěšnosti nebo neúspěšnosti útoku. Potřebné odborné znalosti a know-how výrazně závisejí na **typu útoku**. V případě útoku formou násilné demontáže nebo poničení přístroje *na místě* je metoda jednoduchá (hlavně smělost a použití hrubé síly), takže obecně se zde specifické dovednosti nevyžadují. Útoky hořlavými plyny a útoky výbušninami v pevném stavu vyžadují vyšší úroveň odbornosti.

Útočníci vykazují různé **úrovně schopností**. Na jedné straně mohou vysoce organizované a zkušené skupiny provést úspěšný fyzický útok na bankomat během několika minut. Mají nad tímto procesem kontrolu a jsou schopny omezit riziko jim z toho plynoucí, a tím také omezit vedlejší škody. Na druhé straně méně organizované a oportunistické skupiny ve svých pokusech často selhávají a mohou způsobit značné škody na objektech a budovách v sousedství. Předpokládá se, že některé méně organizované SOZ se vrací k tradičním činnostem organizovaného zločinu v oblasti majetku, jelikož je odrazují preventivní opatření, jež při útocích na bankomaty nejsou schopny překonat.

3 Potřeba preventivního přístupu

Na zemích, kde mají pachatelé při fyzických útocích na bankomaty nízkou míru úspěšnosti nebo kde počet fyzických útoků na bankomaty klesá, se dokládá, že úspěšný přístup k boji proti fyzickým útokům na bankomaty spočívá v kombinaci operačních a preventivních opatření. Vzhledem k tomu, že počet SOZ činných v této oblasti trestné činnosti je omezený, počet útoků významně snižuje zatýkání a následné trestání členů SOZ. Po propuštění však mnoho útočníků na bankomaty svou činnost obnovuje. Navíc může někdy skupina zadrženého pachatele rychle nahradit. Proto jsou nutná preventivní opatření, pokud možno začleněná do legislativního rámce. Zkušenosti dále ukazují, že preventivní opatření v jedné zemi mohou SOZ přecházet na zranitelnější cíle v jiných zemích. Je jen otázka času, než se MO z jedné země rozšíří do jiných zemí. To jasně ukazuje, že je **třeba přijmout preventivní a operativní opatření na evropské úrovni** s partnery ze soukromého sektoru, z veřejného sektoru a s trestněprávními orgány, a to v rámci úzké spolupráce.

4 Prevence

Pro zamezení tohoto druhu trestné činnosti a boj s ní je zapotřebí jasné strategie. V této kapitole uvedeme základní informace o třech krocích, které se obecně provádějí při konfrontaci s fyzickými útoky na bankomat nebo při přípravě na prevenci těchto útoků.

Nejprve je třeba **posoudit situaci**: měl by být stanoven rizikový profil bankomatu a jeho okolí s ohledem na množství dostupné hotovosti(jako možné kořisti), riziko dalších škod a riziko zranění osob. Za druhé: na základě posouzení rizik by měla být vypracována**preventivní strategie**. A konečně je třeba realizovat **preventivní opatření**.

4.1 Zhodnocení situace

SOZ mají tendenci zaměřit se buď na konkrétní typy bankomatů, nebo na bankomaty konkrétních provozovatelů s charakteristickými vlastnostmi, které usnadňují útok na bankomat. Proto je nezbytné provést důkladné posouzení rizika fyzických útoků na bankomat, pokud možno včetně celého řetězce zabezpečení hotovosti od tranzitu po dodání do zásobníku v bankomatu. Pro stanovení rizikového profilu každého bankomatu by měla být analyzována řada prvků, a to včetně prvků, uvedených níže.

- Vlastnosti umístění lokality a okolí bankomatu; vlastnosti, jako je poloha ve městském nebo venkov, hustota obyvatelstva, blízkost policejních stanic, kamery automatického rozpoznávání registračních značek (ANPR) v okolí, kamerový systém v blízkosti atd.
- Umístění bankomatu:
    - uvnitř budovy nebo mimo ni, v bankovní pobočce nebo mimo ni(např. v komerčních prostorách), zabudovaný nebo připevněný k budově,
    - volně stojící bankomat – bez ohledu na to, zda je ukotven k zemi či nikoli,
    - bankomaty zabudované nebo připevněné k budově: zda existují nedostatky ve stavebním řešení, jak je uspořádán úložný prostor hotovosti, aj.
- Typ bankomatu.
- Bezpečnostní funkce obsažené v bankomatu.
- Výše hotovosti v bankomatu.
- Očekávaný typ fyzických útoků na bankomat a jejich MO, aby byla nejdříve přijata nejvhodnější preventivní opatření.
- Již přijatá bezpečnostní a preventivní opatření(inteligentní systémy neutralizace bankovek – IBNS), systémy průmyslové televize, systém bezpečnostní mlhy – snížení viditelnosti) atd.).

Dalšími prvky, které je třeba vyhodnotit, jsou stav spolupráce s partnery a zúčastněnými stranami a právní předpisy. Měla být posouzena spolupráce mezi trestněprávními orgány a soukromými a veřejnými partnery s cílem vytvořit spojenectví pro boj proti trestné činnosti. Je možné, že každý partner má zajímavé informace, které k hodnocení situace přispějí. V tomto rámci je obzvláště důležitá místní policie nebo místní správní orgány. Je třeba vyhodnotit právní předpisy, pokud jde o vytvoření právního rámce pro prevenci, přijetí povinných preventivních opatření, odsouzení za útoky na bankomat atd.

4.2 Vypracování preventivního přístupu

Po posouzení situace a určení hlavních rizikových oblastí a silných stránek i nedostatků ohledně zabezpečení bankomatů lze vypracovat strategii (často vycházející ze spolupráce veřejného a soukromého sektoru) a zavést preventivní a operativní protiopatření. Preventivní opatření by měla být zaměřena na zmenšení odhodlanosti pachatelů a jejich schopností. Za tímto účelem jsou navrženy tři osy preventivních opatření na základě tří z pěti strategií prevence situačního zločinu podle Clarkea ([2]) – snížení výnosu, zvýšení rizika pro pachatele a zvýšení úsilí k získání přístupu ke kořisti.

Pachatelé trestných činů si provádí bilanci očekávaného výnosu a rizik souvisejících např. s útokem na bankomat. Snížení šance na získání snadného výnosu a zvýšení rizika pro pachatele snižuje jejich očekávání a jejich potřebu angažovat se ve fyzickém útoku na bankomat. Další opatření, která zvyšují úsilí potřebné k získání přístupu k bankomatu, mají vliv na schopnost pachatelů. Oportunističtí pachatelé, jejichž pokusy jsou často neúspěšné, se v útocích na bankomaty angažovat přestanou. U profesionálních útočníků na bankomaty se snižuje úspěšnost, což opět ovlivňuje poměr návratnosti a rizika.

Preventivní strategii dále doplňují souběžná opatření, jako je účinná mediální strategie, včasná sociální prevence a opatření ke snížení rizika vedlejších škod na budovách a k zajištění bezpečnosti místních obyvatel, osob zasahujících na místě činu jako první a kolemjdoucích nebo projíždějících.

([2]) Derek Cornish a 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.

Jsou možné i další způsoby, jak tento přístup strukturovat. V Nizozemsku používají orgány tzv. bariérový model ([3]). Tento model určuje kroky, které musí zločinec podniknout pro spáchání trestného činu. Identifikuje rovněž partnery a příležitosti, které umožňují trestnou činnost, a je užitečným nástrojem pro organizaci procesu shromažďování informací o oblasti trestné činnosti. Určením všech kroků nezbytných k provedení fyzického útoku na bankomat lze identifikovat bariéry, které brání zločinu, i nejvhodnější partnery pro jejich vytvoření. Bariérový model také identifikuje signály, které veřejné a soukromé partnery upozorní na fyzické útoky na bankomat, ale i signály, které mohou tito partneři vyslat sami pro informování orgánů o svém podezření.

Ke zmírnění rizik, která jdou v jedné ruce s posílením prevence, je zapotřebí dobře vypracovaná strategie. Preventivní opatření, která jsou velmi účinná v odrazování amatérů a napodobovatelů, mají někdy nežádoucí účinky. Některé skupiny se při hledání zranitelných bankomatů uchylují k metodě pokus-omyl a zanechaly za sebou stopu v podobě poškozených bankomatů. Nebezpečnější a tvrdší SOZ začínají při svých útocích používat násilnější MO, například přesun od plynných k tuhým výbušninám.

Pro vytvoření účinného souboru preventivních opatření je nejlepším postupem zřízení vnitrostátního orgánu s pravomocí ukládat zvláštní opatření pro vysoce rizikové bankomaty, a to na základě důkladné analýzy situace. Tento přístup se osvědčil jako účinný ve Francii, zejména pokud je vytvořen právní rámec a daná opatření jsou prováděna společně s opatřeními operativního charakteru.

4.3 Realizace preventivních opatření

Opatření představená v této kapitole s cílem zabránit fyzickým útokům na bankomaty prokázala svou užitečnost v různých zemích. Vycházejí ze závěrů konference o prevenci a z preventivních opatření aktivně podporovaných mezinárodními organizacemi působícími v oblasti zabezpečení bankomatů. Mnohá z opatření jsou dobře známá. Několik zemí již řadu opatření s úspěchem zavedlo. Navrhovaná opatření jsou však často prováděna pouze částečně a nejsou zakotvena v právních předpisech.

Jak je již zmíněno výše, navrhují se tři osy preventivních kroků: snížení výnosu, zvýšení rizika pro pachatele a zvýšení úsilí k získání přístupu ke kořisti.

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

4.3.1 Snížení výnosu

První osou prevence fyzických útoků na bankomaty je snížení výnosu z trestného činu. Dokud bude vnímání „rychlých peněz“ přetrvávat, pachatelé trestných činů se do tohoto druhu zločinnosti zapojí. Snížení množství hotovosti, která je k dispozici, a buď její odstranění nebo znehodnocení snižuje možnost zajímavé kořisti. Menší očekávání snižují potřebu zločince zapojit se do tohoto typu trestné činnosti.

4.3.1.1 *Snížení částky hotovosti*

Jedním z opatření ke snížení výnosu je snížení částky hotovosti dostupné v bankomatu. V ideálním případě by tato částka měla být omezena na nezbytnou částku pouze na jeden obchodní den. Ekonomickou výhodnost by mohla zajistit spolupráce mezi bankami. V Nizozemsku spolupracovala celá řada bank na vytvoření sítě bankomatů nazvané „Geldmaat“, která je nezávislá na bankách. Cílem spolupráce je zajistit dostupnost, přístupnost, ekonomickou výhodnost a zabezpečení hotovosti. To pravděpodobně povede ke snížení počtu bankomatů. Každý z bankomatů však nebude obsahovat více peněz – bude častěji doplňován. Počet doplnění bude přizpůsoben dle potřeby.

Vzhledem k tomu, že pachatelé většinou na bankomaty útočí mezi 3. a 4. hodinou ranní, důrazně se doporučuje, aby byly samostatně stojící bankomaty (umístěné většinou v komerčních a veřejných prostorách, které jsou zranitelnější) prázdné a aby se hotovost na konci dne přesunovala na bezpečné místo. Veřejnost lze výstražným signálem informovat, že v bankomatu není v noci žádná hotovost. Druhý den by měl být bankomat doplněn za nepřítomnosti zákazníků a v prostorách pod uzamčením. Tento systém je zaveden ve Francii, kde právní předpisy ukládají maloobchodníkům, kteří mají v obchodě volně stojící bankomat, povinnost odebrat přes noc hotovost a nechat bankomat otevřený. U ostatních bankomatů lze přechovávané částky snížit zvýšením frekvence doplňování.

4.3.1.2 *Znehodnocení kořisti a zajištění sledovatelnosti peněz*

První technikou znehodnocení lupu jsou tzv. inteligentní systémy neutralizace bankovek (IBNS). Zde se bankovky potřísní barvou a označí se tak jako odcizené. Do barvy lze přidat i sledovací látky a markéry. V současné době se tyto markéry používají zejména pro kriminalistické účely, neboť bankovky spojují s místem činu a zvyšují riziko, že budou pachatelé dopadeni. I když je IBNS účinným preventivním opatřením, je třeba zvážit několik věcí.

Evropská centrální banka zabarvené bankovky neproplácí ([4]) (od roku 2003), řada národních centrálních bank členských států EU však tak stále činí. Zbarvené bankovky také do právního systému opětovně vstupují prostřednictvím kasin. Systém IBNS je pro zločince další překážkou, byl by ale mnohem účinnější, pokud by nebylo možné, aby pachatelé trestných činů zabarvené bankovky používali v EU. Aby toho bylo možné dosáhnout, národní centrální banky by zabarvené bankovky přijímat neměly. Výjimky lze učinit za konkrétních okolností, jako jsou bankovky zbarvené během chybné aktivace. Je také důležité informovat obyvatelstvo, aby zbarvené bankovky nepřijímalo. Z dlouhodobějšího pohledu by měla zbarvené bankovky detekovat zařízení pro kontrolu bankovek a měla by být instalována v bankách a komerčních prostorách, jako jsou kasina, myčky aut atd. Detekce barvy je obtížná a nákladná, ekonomicky úsporným řešením by však mohla být instalace infračervených systémů, které detekují bankovky zbarvené infračervenými markéry. V Belgii a Francii tyto systémy prokázaly svou efektivitu a představuje zde osvědčené postupy. Pokud jsou do bankomatu vloženy bankovky s infračervenými markéry, bankomat peníze přijme („spolkne“), nepřipíše je však na účet. Zaevidována by měla být i osoba zbarvené bankovky vkládající.

Při instalaci řešení IBNS je třeba vzít v úvahu i některé další skutečnosti. Několik výrobců nabízí řadu různých řešení IBNS s různými aktivačními mechanismy a různými typy barev. První úvaha se týká skutečnosti, že ne všechny typy aktivačních technologií IBNS mohou představovat ochranu před všemi hrozbami. Některé IBNS fungují velmi dobře pro útoky formou násilné demontáže nebo poničení přístroje *na místě* a útoky plynnou výbušninou, ale nefungují v případě útoku pomocí výbušniny v pevném stavu nebo naopak. Proto je zvolenou technologii třeba důkladně zvážit.
Dalším faktorem je typ barvy, který je na výběr. V Belgii jsou stanoveny vnitrostátní minimální požadavky na IBNS (bezpečnost, procento zbarvení, neomyvatelnost atd.) a nezávislé zkoušky potvrzují, že systém splňuje vnitrostátní normy a funguje podle tvrzení výrobce. Je důležité testování skutečných bankovek, protože na trhu jsou i barvy levnější, které dobře fungují s padělanými nebo falešnými bankovkami, nikoli však s bankovkami reálnými: to znamená, že barvu lze z pravých bankovek odstranit mytím. Kromě toho se do barvy doporučuje přidat kriminalistický markér, který umožní prošetřit vazbu mezi zbarvenými bankovkami a konkrétním místem zločinu.

Osvědčené postupy ukazují, že IBNS může být velmi účinná metoda, a to zejména v kombinaci s dalšími preventivními opatřeními. V roce 2015 zavedla Francie nové právní předpisy, včetně článků o instalaci IBNS a o používání barvy s obsahem unikátní DNA. Je to právě francouzská vojenská policie (četnictvo), která na základě posouzení rizik rozhodne, kde je třeba provést IBNS a další opatření.

([4]) Rozhodnutí Evropské centrální banky o Evropské centrální bance. Nominální hodnoty, specifikace, reprodukce, výměna a stahování eurobankovek z oběhu, 2003.

Vzhledem k tomu, že nové právní předpisy posílily preventivní a operační přístup, klesl počet útoků z 300 v roce 2013 na 50 v roce 2018.

Další technikou, která je vyvíjena s cílem znehodnotit kořist, je použití **lepidla**. Účinnost lepidla byla prokázána v Nizozemsku, ale náklady na implementaci a provoz jsou v současné době vysoké. Kromě toho může lepidlo představovat nebezpečí požáru, pokud není systém před útokem aktivován, protože rozptýlení částic lepidla ve vzduchu může způsobit vznik hořlavé směsi. Tato metoda zatím není připravena na komercializaci, ale mohla by být řešením pro budoucnost.

4.3.2 Zvýšení rizika

Druhou osou prevence fyzických útoků na bankomaty je odradit potenciální pachatele od páchání trestných činů zvýšením rizika odhalení a potrestání. Kromě rizika fyzické újmy při použití výbušnin při útocích na bankomat je hlavním rizikem trestného činu trest odnětí svobody v případě dopadení při činu nebo po vyšetřování. Aby se snížila žádostivost potenciálních pachatelů, je třeba zvýšit riziko odhalení a potrestání. Pro společnost je samozřejmě velmi účinným preventivním způsobem i dopadání pachatelů trestných činů a jejich odsouzení, pokud existuje následné odsouzení, jak jsme se přesvědčili v několika zemích.

4.3.2.1 *Sdílení informací*

Klíčové je při odhalování a trestání útočníků na bankomaty sdílení informací mezi všemi zúčastněnými stranami v boji proti fyzickým útokům na bankomaty, a to včetně provozovatelů bankomatů, trestněprávních orgánů (policie, státní zastupitel atd.), orgánů veřejné správy, výrobců bankomatů a bezpečnostních či ochranných zařízení, profesních sdružení, provozovatelů bankomatů (banky a nebankovní provozovatelé) a firem provádějících ostrahu nebo provozujících pulty centrální ochrany. V ideálním případě by to bylo jak na vnitrostátní, tak na mezinárodní úrovni.

Včasné odhalení chystaného fyzického útoku na bankomat je obtížné. Včasné odhalení je možné pouze v případech, kdy na mezinárodní úrovni probíhá téměř bezproblémová výměna informací mezi trestněprávními a soukromými partnery (firmy provádějící ostrahu a provozovatelé bankomatů). Je třeba sledovat širokou škálu ukazatelů, včetně zpráv o včasném varování mezi trestněprávními orgány ohledně pohybu SOZ, informací o vozidlech, která byla použita při útocích na bankomaty,

informací od firem provádějících ostrahu nebo subjektů v sousedství sledujících podezřelé chování zjištěné v okolí bankomatu a podezřelých transakcí detekovaných provozovateli bankomatů a dalšími metodami snímání. Dalšími možnými policejními opatřeními pro včasnou detekci jsou sledování odcizených automobilů, výrobců a distributorů výbušnin a firem s oprávněním používat výbušniny. Úsilí nezbytné k dosažení včasného odhalení je náročné a nemá žádnou záruku na úspěch, a proto jsou zásahy trestněprávních orgánů ještě před útokem ojedinělé.

Pokud není včasná detekce možná, mohou v případě fyzického útoku na bankomat vydat rychlou výstrahu pulty centrální ochrany. Aby bylo možné zasáhnout, musí být dohodnuty a stanoveny vnitrostátní předpisy a protokoly pro rychlou komunikaci mezi pulty centrální ochrany a trestněprávními orgány. V případě včasného odhalení nebo předání informací v reálném čase bude vždy nutné, aby trestněprávní orgány vyhodnotily načasování a nejvhodnější příležitost k zásahu. Přistižení zločinců při činu je velmi obtížné a může vést k nebezpečným situacím, protože některé SOZ jsou velmi násilnické a používají těžké zbraně.

Pro úspěšné vyšetřování po fyzickém útoku na bankomat musí pracovníci trestněprávních orgánů komunikovat se všemi zúčastněnými stranami, protože kterýkoli z nich by mohl mít informace přispívající k úspěchu vyšetřování. Nezbytná je samozřejmě komunikace a spolupráce s hlavními oběťmi, tj. bankami nebo jinými provozovateli bankomatů: tyto subjekty mají přístup k údajům, které jsou pro vyšetřování důležité. Pro provozovatele bankomatů pomohou informace od trestněprávních orgánů zlepšit preventivní opatření. Kromě toho se jako užitečné ukazují kontakty s profesními sdruženími a výrobci: vydávají často výstražné zprávy ohledně bezpečnosti, k jejichž odběru se mohou přihlásit další zainteresované strany. Výrobci bankomatů mají dobrý přehled o různých typech útoků na bankomaty a o odpovídajících nedostatcích a silných stránkách preventivních opatření. Jsou také velmi ochotni poskytnout policii pomoc pomocí informací o technických aspektech bankomatů a o používaných MO zločinců.

Přeshraniční spolupráce je nezbytná: státy by měly sdílet informace (o podezřelých, odsouzených útočnících na bankomaty, jejich MO, podezřelých vozidlech, snímky z útoků atd.), a to nejen na pomoc při vyšetřování, ale také proto, že podezřelé odsouzené v jiné zemi lze odsoudit za opětovné spáchání/recidivu.

Vyšetřování by mohlo výrazně podpořit vytvoření databáze na celoevropské úrovni, která bude k dispozici pro trestněprávní orgány a bude obsahovat kriminalistické údaje (např. o různých typech barev IBNS, sledovacích látkách a markérech nebo ochranných sklech bankomatů), a propojit

podezřelé s konkrétním dějištěm trestného činu. Nedostatečná je často normalizace technologií na mezinárodní úrovni: během konference v lednu 2019 účastníci uvedli, že normalizace barev a označení na úrovni EU by mohla vyšetřování značně usnadnit.

4.3.2.2 *Průmyslová televize a odposlouchávací zařízení*

Obrazová a zvuková data ze systémů průmyslové televize a odposlouchávacích zařízení mohou pomoci jak při odhalení útoku v reálném čase(např. za účelem zabránění tělesné újmě osob, které na místě činu zasahují jako první), tak při následném vyšetřování (např. za účelem identifikace pachatelů a jejich MO). Snímky z průmyslové televize lze kombinovat se obrazy z veřejných a jiných systémů průmyslové televize v sousedství záznamu z bankomatu a dopravního radaru, aby bylo možné získat úplnější obraz pachatelů a jejich MO.

Snímky z kamerových systémů jsou však často nekvalitní nebo špatně uložená. Snímky by měly být dostatečně kvalitní, aby umožnily identifikaci osoby. Stanovení evropských norem pro bezpečnostní systémy průmyslové televize by opět bylo usnadněním vyšetřování. Vzhledem k tomu, že pachatelé často před útokem kamerové systémy průmyslové televize nebo zařízení pro odposlech v reálném čase deaktivují, je také možné zvážit instalaci neviditelných systémů průmyslové televize nebo zařízení pro odposlech v reálném čase.

4.3.2.3 *Trest a rehabilitace pachatelů*

Je prokázáno, že důsledný a přísný trest má preventivní účinek. Zatčení celé SOZ má okamžitý vliv na počet útoků na bankomaty. Propuštění útočníků na bankomat z vězení však často vede k novému přílivu útoků. To znamená, že krátké tresty vedou k tomu, že pachatelé jsou opět velmi rychle aktivní. Minimální a maximální sankce pro pachatele trestných činů odsouzené za každý typ fyzického útoku na bankomat se v jednotlivých členských státech liší. Někteří lidé věří, že vyšší tresty potenciální pachatele odradí. Z vědeckého výzkumu ([5]) však vyplývá, že zvýšení přísnosti trestů nemusí nutně vést k odrazujícímu účinku. Proto by mohlo být zajímavé zabývat se nápravnými rehabilitačními programy zaměřenými na pachatele s cílem snížit vysokou míru recidivy.

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

4.3.3 Zvýšení úsilí

Třetí osa, která má zabránit fyzickým útokům na bankomaty, obsahuje opatření, která pachateli realizaci trestného činu ztěžuje.

4.3.3.1 *Zajištění prostředí odolného proti trestné činnosti*

Pokud z posouzení rizik (viz výše) vyplývá, že se bankomat nachází ve vysoce rizikovém prostředí, mělo by být toto umístění demontováno a bankomat přesunut do oblasti s nízkým nebo středním rizikem. To se každopádně týká případů, kdy se analýzou prokáže, že by se objekt mohl zbortit, pokud by byl bankomat napaden s použitím výbušnin. V případech s vysokým rizikem by mohly být zavedeny právní předpisy k vymáhání těchto opatření. Kromě snížení počtu bankomatů ve vysoce rizikových prostředích by měly být podporovány bezhotovostní platby, aby se snížila potřeba bankomatů.

Není-li přesun bankomatu možný, měla by být přijata maximální bezpečnostní opatření: např. používání prvků bránících přístupu vozidla, sloupů pouličních svítidel a dalšího mobiliáře k omezení přístupu k budově a systémů zablokování vozidla, instalace vhodného pouličního osvětlení, zvýšený dohled nad vozy nebo skryté sledování a zařízení proti krádeži, jako je systém znehodnocování bankovek. Pokud je místo napadeno v místě, které nebylo označeno za vysoce rizikové, mělo by být jako takové označeno a přidána další bezpečnostní opatření. Tyto nové faktory by měly být zohledněny v nástroji pro posuzování rizik, aby byl aktualizován. Opětovné posuzování tohoto rizika by se mělo stát opakující se operací.

4.3.3.2 *Zvýšení odolnosti bankomatů proti útoku*

Výrobci bankomatů nabízejí standardní řadu těchto přístrojů, které mají řadu bezpečnostních prvků hodnocených podle stupňů bezpečnosti Evropského výboru pro normalizaci (CEN). Bankomaty mají obecně označení CEN v rozsahu od nižší třídy(CEN1) až po nejvyšší úroveň (CEN4). Třídu určuje například síla konstrukce a odolnost proti útokům. Odolnost vůči plynům je většinou nabízena doplňkově (CEN-GAS). Standardní modely lze rozšířit o další ochranná opatření. Tyto funkce obvykle instalují jiné subjekty, aby bylo zajištěno dodržování místní legislativy a přizpůsobení základního modelu požadavkům místních zákazníků. Mezi další bezpečnostní funkce patří různé snímače pro

aktivaci systému neutralizace plynu nebo systému IBNS v případě poničení přístroje *na místě* nebo útoku pomocí výbušnin, a dále kvalitnější bezpečnostní uzávěry a trezorové zámky zabraňující neoprávněnému přístupu k trezoru v místech, kde je narušen hlavní uzávěr. U volně stojících bankomatů je důležité používat kotvicí systémy, které nabízejí mimořádnou ochranu proti útokům typu násilné demontáže a odvozu. V bankomatu mohou být i sledovací systémy na pomoc vyšetřovatelům v případě, že je bankomat před jeho otevřením přesunut na jiné místo.

4.3.3.3 *Opatření z pohledu stavebního řešení*

Při instalaci bankomatu se doporučuje používat přístroje s přístupem zezadu. V takovém případě musí pachatel pro odcizení hotovosti vstoupit do budovy a získat přístup k zadní části přístroje. Nejvíce ohroženy jsou přenosné, volně stojící bankomaty. Snížení jejich počtu by bezpečnost zvýšilo. Povinnost instalovat bankomaty do místností odolných proti vloupání by používání volně stojících bankomatů automaticky snížila.

4.3.3.4 *Mlhový systém*

Mlhovým dělem se místnost rychle naplní hustou mlhou, takže narušitel nic nevidí. Tato bezpečnostní mlha provedení útoku na bankomat často znemožňuje. Systém pachatele přinejmenším zpomalí a ponechá čas na zásah policejních služeb. Bezpečnostní mlhový systém je připojen k poplašné soustavě a lze jej aktivovat dvěma způsoby. Může být spouštěn automaticky pomocí poplachových senzorů, jako jsou např. detektory pohybu (v noci) nebo snímačů manipulace s ochranným uzávěrem bankomatu. Lze jej aktivovat i pultem centrální ochrany, aby se zabránilo příliš velkému počtu falešných poplachů. U venkovních bankomatů spojených s budovou pomocí zdiva lze mlhový systém použít na zadní straně bankomatu, aby se prostor za bankomatem zaplnil mlhou a pachatelé neviděli nic.

Mlhové systémy mohou zajistit bodovou ochranu u bankomatu umístěného v otevřených prostorách čerpacích stanic, v supermarketech atd. Tím se zabrání zamlžení celého prostoru. Ochrana před mlhou je nejúspěšnější, když mlha přichází z různých úhlů nebo když vyplňuje prostor za bankomatem, a to v případě násilného přesunu
bankomatu odtažením. Probíhají zkoušky, aby bylo možné zjistit, zda lze mlhová děla instalovat v samotném bankomatu, nikoli v místnosti, kde se bankomat nachází. Do mlhy lze přidávat DNA markéry, které potřísní pachatele a jejich oblečení.

4.3.4 Souběžná opatření

Aby bylo zajištěno účinné a účinné provádění výše uvedených preventivních opatření, je třeba zvážit řadu souběžných opatření. Tato opatření jsou nezbytná pro umožnění nebo posílení komplexního preventivního a operačního přístupu k řešení fyzických útoků na bankomaty.

4.3.4.1 *Právní předpisy*

V řadě zemí legislativa ukládá provozovatelům bankomatů povinnost přijmout preventivní opatření. V jiných zemích je zavedení smluvních ujednání a dohod mezi bankami a trestněprávními orgány zárukou správného přístupu k řešení fyzických útoků na bankomaty. Oblasti, v nichž lze uvažovat o regulačních opatřeních, zahrnují:

- zakotvení preventivních opatření,
- právní rámce umožňující spolupráci mezi trestněprávními orgány a partnery z veřejného a soukromého sektoru,
- reklasifikace rozsudku, pokud jsou sankce pro pachatele fyzických útoků na bankomaty příliš nízké.

Často jsou to však jen bankovní instituce, které jsou povinny dodržovat předpisy a nebankovní provozovatelé bankomatů nejsou těmito zákony nebo dohodami vázáni. V regulačním rámci je to často slabé místo.

Některé země žádná omezení nezavádějí, ale snaží se přesvědčit provozovatele bankomatů, aby přijali preventivní opatření, a to zvyšováním jejich povědomí o oblastech trestné činnosti a jejich trendech: v zemích s vysokým počtem nezávislých bank se to však ukazuje jako obzvláště obtížné.

Je nezbytné zajistit, aby účinné provádění preventivních opatření zahrnovalo i změny právních předpisů a předpisů (jak na vnitrostátní, tak na mezinárodní úrovni), které budou závazné pro všechny typy provozovatelů bankomatů. V ideálním případě by právní předpisy měly být sladěny na úrovni EU, aby se zabránilo tomu, že díky důrazným preventivním opatřením zakotveným v právních předpisech jedné země se SOZ přesunou do jiných zemí s méně přísnou regulací.

4.3.4.2 *Mediální strategie*

Další důležitou osou preventivní strategie je dobře zavedená strategie mediální, jejímž cílem je snížit očekávání a potřebu útočníků na bankomaty se v této trestné činnosti angažovat. Je třeba zdůraznit nízkou míru úspěšnosti a vysoká rizika pro pachatele a vyhýbat se sdělení o výnosech (lupu) nebo podrobnostech o útoku na bankomaty – např. typ dotyčného bankomatu nebo metody, které bylo zabráněno. Na druhé straně je nezbytná rozsáhlá komunikace ohledně zatýkání podezřelých a následných trestu po odsouzení.

4.3.4.3 *Zlepšení spolupráce*

Lepší spolupráce a výměna informací již byly zmíněny v hojné míře, nelze je však zdůraznit dostatečně. Operativní výměna informací na mezinárodní úrovni je hlavní činností Europolu. Kromě této výměny informací konference o prevenci ukázala, že je jednoznačně nutné zvýšit mezioborovou a víceúrovňovou spolupráci a sdílení informací mezi všemi zúčastněnými stranami v boji proti fyzickým útokům na bankomaty, zahrnující i trestněprávní orgány, orgány veřejné správy, výrobce bankomatů a bezpečnostních či ochranných zařízení, profesní sdružení, provozovatele bankomatů (banky a nebankovní provozovatelé) a firmy provádějících ostrahu nebo provozující pulty centrální ochrany. Toto musí zahrnovat místní, vnitrostátní i mezinárodní úroveň.

4.3.4.4 *Snížení rizika vzniku vedlejších škod*

V případě útoků pevnými výbušninami za sebou některé SOZ zanechávají materiál. To může vést k nebezpečným situacím pro osoby zasahující namístě činu jako první nebo civilisty (žijící v sousedství či procházející/projíždějící kolem). Je nutné zajistit jejich bezpečnost. Stejně jako v případě Belgie musí být vypracovány a sladěny protokoly a postupy, které musí dodržovat osoby zasahující na místě činu jako první(jak subjekty z oblasti vymáhání práva, tak provozovatelé bankomatů). Dalším osvědčeným postupem v této souvislosti je příklad Nizozemska, kde se k posouzení situace používá záznam z útoku na bankomat pořízený průmyslovou televizí. Aby byly tyto snímky okamžitě dostupné, lze uzavřít dohodu s pultem centrální ochrany.

4.3.4.5 *Sociální prevence*

SOZ často hledají nové zájemce mezi mladými lidmi. Bylo by možné vypracovat projekty, které by tyto náborové procesy v rané fázi mařily. Na tyto procesy by se měla zaměřit pozornost policie nebo sociálních pracovníků, kteří by mohli zasáhnout osobním kontaktem s těmito potenciálními pachateli.

5 Závěry

V posledních 2 letech se zvýšil počet evropských zemí postižených fyzickými útoky na bankomaty. V tomto ohledu spolupracovaly Europol a EUCPN na shromáždění osvědčených opatření pro boj proti této trestné činnosti a pro její prevenci.

Úspěšný přístup k boji proti fyzickým útokům na bankomaty spočívá v kombinaci operativních a preventivních opatření, začleněných nejlépe do legislativního rámce. Aby se zamezilo tomu, že důrazná opatření v jedné zemi přesměrují SOZ do zemí zranitelnějších, doporučuje se přijmout tato opatření na celoevropské úrovni.

Pro zamezení tohoto druhu trestné činnosti je zapotřebí stanovit jednoznačnou strategii ve třech krocích: posouzení situace, vyvinutí preventivního přístupu založeného na posouzení rizik a realizace preventivních opatření.

Posouzení rizik fyzických útoků na bankomaty by mělo zahrnovat charakteristiky bankomatu a jeho okolí, spolupráci s partnery a zúčastněnými stranami při vytváření aliancí pro boj proti této trestné činnosti a hodnocení preventivního a právního rámce. Po posouzení situace by měla být vytvořena strategie vycházející ze spolupráce veřejného a soukromého sektoru a preventivních i operativních protiopatření. Cílem preventivních opatření je zmenšit odhodlání a schopnost pachatele angažovat se ve fyzickém útoku na bankomaty. K dosažení tohoto cíle se navrhují tři osy preventivních kroků: snížení výnosu, zvýšení rizika pro pachatele a zvýšení úsilí k získání přístupu ke kořisti. Preventivní strategii by měla doplňovat souběžná opatření. Osvědčeným postupem je zřízení vnitrostátního orgánu, který má pravomoc tato nezbytná opatření zavést.

Snížením výnosu se snižuje potřeba zločince angažovat se v tomto typu trestné činnosti. Jedním z opatření ke snížení očekávání pachatele trestné činnosti je snížení objemu hotovosti v bankomatu, a to omezením objemu doplněné hotovosti na objem dostatečný pouze pro 1 obchodní den, případně vyprázdnění(nejzranitelnějších) bankomatů v noci. Další metodou je kořist znehodnotit a zajistit vysledovatelnost peněz. V tomto kontextu lze použít systém IBNS, který bankovky zbarví a označí je jako odcizené. Tato metoda je nejúčinnější, když pachatelé tyto peníze nemohou utratit nebo je vrátit do legálního oběhu. Toho lze dosáhnout tím, že banky a veřejnost nebudou zbarvené bankovky přijímat za účelem platby a instalací zařízení pro kontrolu bankovek, která mohou zbarvené bankovky detekovat a odmítnout. V tomto ohledu se ekonomicky výhodným řešením v Belgii a Francii ukázala investice do infračervených systémů detekujících zbarvené bankovky pomocí infračervených markérů. Při instalaci IBNS by státy měly důkladně zvážit zvolené aktivační mechanismy, minimální požadavky na neutralizaci bankovek a přidání kriminalistického markéru do barvy.

Druhou osou, která má zabránit fyzickým útokům na bankomat, jsou opatření odrazující potenciální pachatele od páchání trestné činnosti tím, že **zvýší riziko** odhalení a potrestání. Klíčové pro odhalování a trestání útočníků na bankomaty je shromažďování informací a sdílení informací mezi všemi zúčastněnými stranami, a to jak na vnitrostátní, tak na mezinárodní úrovni. Šance na včasné odhalení a úspěšné vyšetřování může zvýšit výměna informací obnášejících vysoce kvalitní snímky z průmyslové televize a zvuková data. Aby se zabránilo deaktivaci systémů průmyslové televize nebo odposlouchávacích zařízení před útokem, je možné zvážit instalaci neviditelných systémů průmyslové televize nebo zařízení pro odposlech v reálném čase. Mezinárodní spolupráci a vyšetřování by mohlo značně usnadnit vytvoření kriminalistické databáze, a také normalizace technologií na evropské úrovni. Pokud jsou pachatelé dopadeni a odsouzeni, může být zajímavé zabývat se nápravnými rehabilitačními programy zaměřenými na pachatele s cílem snížit vysokou míru recidivy.

Třetí osa, která má zabránit fyzickým útokům na bankomaty, zahrnuje opatření ke **zvýšení úsilí**, které pachatel k provedení trestného činu potřebuje. Při instalaci bankomatu v prostředí odolném proti kriminální činnosti s maximálním počtem bezpečnostních opatření bude pro pachatele útok na bankomat náročnější. Standardní ochranu bankomatu lze dále rozšířit řadou dalších bezpečnostních funkcí. Kromě těchto opatření může pachatele odrazovat nebo přinejmenším útok zpomalit instalace mlhového systému.

Výše uvedená opatření se posílí celou řadou **souběžných** opatření, např. vytvoření právního rámce, který všechny provozovatele bankomatů zavazuje k provádění preventivních opatření, vypracování dobře zavedené mediální strategie, intenzivnější spolupráce na místní, vnitrostátní a mezinárodní úrovni, metodika pro osoby zasahující na místě činu jako první s cílem snížit riziko vedlejších škoda investice do sociální prevence s cílem podrýt procesy náboru nových pracovníků pro trestnou činnost.

6 Doporučení pro preventivní přístup: přehled

Vyvinout účinnou reakci pro zabránění fyzickým útokům na bankomat

Zhodnocení situace

Vytvořit rizikový profil bankomatů ve vaší zemi/regionu
Určit partnery a zúčastněné strany v boji proti fyzickým útokům na bankomaty a vyhodnotit tuto spolupráci
Vyhodnotit právní rámec pro boj s fyzickými útoky na bankomaty na vnitrostátní a mezinárodní úrovni.

Vypracování preventivního přístupu

Určit (hlavní) rizika, která mají být zahrnuta, a také priority
Určit nejvhodnější preventivní opatření k pokrytí těchto rizik s přihlédnutím ke třem hlavním osám.
Určit souběžná preventivní opatření potřebná k posílení přijatých preventivních opatření.

Možná preventivní opatření		
Snížení výnosu	Zvýšení rizika	Zvýšení úsilí
– Snížení částky hotovosti. ○ Vyprazdňování bankomatu v noci. ○ Zvýšení počtu nebo frekvence doplňování. – Znehodnocení kořisti. ○ Inteligentní systémy neutralizace bankovek (IBNS) ○ Infračervené markéry v IBNS barvě pro detekci zbarvených bankovek pomocí zařízení pro kontrolu bankovek. ○ Ve fázi vývoje: lepidlo	– Přeshraniční sdílení informací v zájmu: ○ včasné detekce možného útoku na bankomat, případně detekce v reálném čase, ○ posílení operativního přístupu, ○ odsouzení za opakovaně spáchané trestné činy, ○ výměna forenzních údajů na evropské úrovni. – průmyslová televize a odposlouchávací zařízení. – Následné potrestání a rehabilitace pachatelů.	– Zajištění prostředí odolného proti trestné činnosti. ○ Změna umístění vysoce rizikových bankomatů. ○ Zabezpečovací opatření: fyzické překážky, sledování atd. – Posílení výbavy bankomatů pomocí uzávěrů s odolností vůči plynným nebo tuhým výbušninám atd. – Stavebně-technická opatření, jako jsou přístroje s přístupem zezadu – Bezpečnostní mlhové systémy.

Souběžná opatření k posílení preventivního přístupu

- Účinné právní předpisy včetně preventivních opatření proti fyzickým útokům na bankomaty, následné odsouzení atd.
- Účinná mediální strategie odrazující pachatele.
- Intenzivnější spolupráce mezi všemi zúčastněnými stranami(veřejnými, soukromými, trestněprávními orgány) v boji proti fyzickým útokům na bankomaty.
- Snížení rizika vedlejších škod u osob zasahujících na místě činu jako první nebo civilistů (žijících v sousedství nebo procházejících).
- Sociální prevence bránící náboru mladých lidí pro trestnou činnost (tohoto typu).