

Предотвратяване на физически нападения срещу банкомати

РАЗРАБОТВАНЕ НА ЕФЕКТИВЕН ПОДХОД



“

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

”

БЛАГОДАРНОСТИ

Настоящият документ е резултат от сътрудничеството между Агенцията на Европейския съюз за сътрудничество в областта на правоприлагането (Европол) и секретариата на Европейската мрежа за превенция на престъпността (EUCPN). Благодарим на специалистите в областта на физическите нападения срещу банкови автомати (АТМ), които вложиха време и усилия в подкрепа на създаването на настоящия документ с препоръки. Те допринесоха чрез участието си в конференцията на тема предотвратяване на физически нападения над банкомати (януари 2019 г., Брюксел), като предоставиха изключително важна информация. Благодарим по-специално на правоприлагащите органи от държави членки на ЕС и от държави извън ЕС („трети страни“), на частния сектор, включително Асоциацията на АТМ бранша (АТМIA), BPost, Centrum voor Criminaliteitspreventie en Veiligheid (CCV), Diebold Nixdorf, експертната група по физически нападения над банкомати и [автоматични сейфове] АТS към Европейската асоциация за сигурни транзакции (EAST EGAP), Европейската асоциация за интелигентна защита на парични средства (Euricpa), ING, Febelfin, NCR, Protect, SIOC Banking, Spinnaker, TMD Security и министерствата на вътрешните работи на Белгия, Хърватия, Германия и Испания.

Citation

© Агенция на Европейския съюз за сътрудничество в областта на правоприлагането 2019
© Европейска мрежа за предотвратяване на престъпността 2019

Правна информация

Съдържанието на настоящата публикация не отразява непременно официалното становище на която и да е държава членка на ЕС или на която и да е агенция или институция на Европейския съюз или на Европейските общности.

Възпроизвеждането е разрешено, при условие че е посочен източникът. За всяко ползване или възпроизвеждане на отделни снимки трябва да се иска директно съгласието на притежателите на авторските права. Тази публикация и повече информация за Европол са налични в Интернет.



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

СЪДЪРЖАНИЕ

	<u>Благодарности</u>	3
	<u>Съдържание</u>	4
	<u>Контекст</u>	5
01	<u>Фактори, определящи успеха на физическите нападения над банкомати</u>	6
	1. Уязвимост на банкоматите	6
	2. Организация на нападението над банкомат	7
	3. Опитът и познанията на извършителите	7
02	<u>Необходимост от превантивен подход</u>	8
03	<u>Предотвратяване</u>	10
	1. Оценка на ситуацията	10
	2. Разработване на подход за предотвратяване	11
	3. Изпълнение на превантивните мерки	12
	3.1 Намалете изгодата	12
	3.2 Увеличете риска	13
	3.3 Увеличете усилието	15
	3.4 Паралелни мерки	16
04	<u>Заклучения</u>	18
	Factsheet	20
	<u>Endnotes</u>	22

КОНТЕКСТ

Тъй като броят на физическите нападения над банкови автомати (АТМ) и броят на засегнатите европейски държави нараства, Европейската мрежа за превенция на престъпността (EUCPN) и Европол организираха конференция (януари 2019 г.), на която правоприлагащите органи се събраха с публични и частни партньори, за да разгледат предотвратяването на тези престъпления. В този документ с препоръки са обобщени заключенията на тази конференция за повишаване на осведомеността на властите относно физическите нападения над АТМ и мерките за предотвратяването им.

Ограничен, но нарастващ брой държави в Европейския съюз имат опасения от физически нападения на АТМ. През 2017 г. причинените финансови загуби са оценени на повече от EUR 30 милиона Евро в Европа. Някои държави продължават да стават свидетели на значителен брой нападения над банкомати, докато в други има значително увеличаване на броя на тези инциденти през последните 2 години. Този вид престъпления се развива бързо. Някои държави постигнаха успех в подхода си към справяне с физическите нападения над банкомати и напоследък отбелязват значително намаляване на нападенията. От друга страна, незасегнати досега държави са изправени пред внезапно повишаване на броя на физическите нападения през 2018 г., тъй като организирани престъпни групи (ОПГ) разширяват територията си. Засегнати са не само банки – все повече банкомати на независими доставчици са обект на нападения, тъй като често са разположени в по-уязвими помещения или места.

Множеството различни методи (modi operandi (MO)), които престъпниците използват за нападения над АТМ, могат да бъдат разделени на две основни категории: физически нападения над АТМ и свързани с АТМ измами (това включва въздействия върху логиката на АТМ и атаки чрез зловреден софтуер). Настоящият документ е съсредоточен върху физическите нападения над АТМ: проникване с взлом в АТМ чрез физически средства с цел отнемане на парите. Проникването с взлом може да бъде осъществено чрез:

- > **употреба на експлозиви:** нападателите използват газообразни или твърди експлозиви, за да разрушат физически касетата на АТМ и да се доберат до парите;
- > **нападения с изтръгване/избиване:** нападателите изваждат физически АТМ от мястото, където е инсталиран, често с помощта на автомобил от висок клас;
- > **нападения на място:** нападателите проникват в касетата с груба сила, често пъти с помощта на режещи или пробивни инструменти, като ъглошлиф, чук вария или кислороден.

01 ФАКТОРИ, ОПРЕДЕЛЯЩИ УСПЕХА НА ФИЗИЧЕСКИТЕ НАПАДЕНИЯ НАД БАНКОМАТИ

Успеваемостта на нападенията над банкомати е ниска; само една трета от нападенията са успешни. Независимо от това, когато нападението е успешно, причинените щети (например от експлозиви) на конструкциите на сградите са също толкова големи, а средата в района на местопрестъплението остава опасна за живущите, спасителните служби и минувачите.

Успехът на физическото нападение зависи от редица фактори, сред които характеристиките на банкомата, организацията на нападението, опитът и познанията на извършителите.

1. Уязвимост на банкоматите

Най-уязвимите банкомати са тези, разположени отвън (вградени в стената (TTW) или тези, които стоят вътре в сградите. Когато атакуват вътрешен (самостоятелен) банкомат, ОПГ предпочитат банкомати, разположени в търговски сгради пред банкомати, разположени в банки, където наблюдението обикновено е засилено. Банките използват основно банкомати, разположени вътре или пред сградата на банката. Изнесените банкови обекти („изнесени гишета“) на улицата или в търговски помещения на търговци, като например бензиностанции, супермаркети, хотели, казина, летища и т.н., придобиват все по-голямо значение поради закриването на банкови клонове. Независими доставчици експлоатират банкомати като самостоятелна

услуга. Техните банкомати често са разположени в търговски обекти, места за настаняване и отдих, транспортни съоръжения (железопътни гари, летища и др.), обществени сгради и на улицата.

Поради нарастващата популярност на онлайн банкирането, много банкови клонове вероятно ще бъдат затворени през идните години, а това ще доведе до общо намаляване на броя на банкоматите¹. Това обаче може да доведе до увеличаване на броя на изнесените от банките банкомати и банкомати на независими доставчици, разположени на по-уязвими места.

2. Организация на нападението над банкомат

Подготовката на нападението може да отнеме няколко седмици или дори месеци. Престъпниците трябва да съберат необходимите **средства и ресурси**, като например превозни средства, оборудване и връзки. **Превозните средства** са основно средство за физическо нападение над банкомат; извършителите се придвижват основно с автомобили, а след нападението те най-често бягат с бърз автомобил. Най-често те са крадени, но могат да бъдат наети или купени (например онлайн). По-голямата част от **оборудването** за физическо нападение над банкомат се намира лесно и законно в обикновените магазини. Това допълнително улеснява навлизането в този вид престъпления. Правоприлагащите органи трудно могат да проследят произхода на дадено средство, тъй че рискът за извършителите е малък. ОПГ, които се занимават с физически нападения над банкомати на международно равнище, почти винаги имат връзки в целевата държава (хора, които живеят там от известно време), но могат също да извършват еднократни удари. Тези връзки помагат на ОПГ с логистиката, като например наемане на жилище, предоставяне на автомобил или друго оборудване и проучване на целите. Някои международни престъпници оставят логистиката и проучването изцяло на местните връзки и отиват със сухопътен или въздушен транспорт единствено за извършване на нападението над банкомата.

ОПГ често извършват обширно **проучване**, за да определят подходящите цели; оценка на часа, в който се зарежда банкоматът, на околностите на банкомата, на техническите особености на банкомата,

маршрутите за бягство и въведените мерки за сигурност, като например видеонаблюдение (CCTV), датчици на аларми и щори.

Някои ОПГ предприемат редица действия, за да **попречат на правоприлагащите органи и службите за сигурност** преди нападението. Те манипулират алармените системи и уличното осветление, използват техники за отклоняване на вниманието, организират пътни блокади или се опитват да манипулират автомобилите на правоприлагащите органи.

3. Опитът и познанията на извършителите

Физическите нападения над банкомати привличат престъпниците, защото парите са непосредствено достъпни и няма нужда от широка мрежа за продажба на крадени стоки. Те са удобна алтернатива за престъпници, които вече се занимават с организирани престъпления срещу собствеността.

ОПГ трябва да натрупат **необходимия опит и познания**, защото те са определящ фактор за успеха или провала на нападението. Необходимият опит и познания зависят до голяма степен от **вида на нападението**. Нападенията с изтръгване/избиване и **на място** са с прост механизъм на действие (основно дързост и използване на груба сила), тъй че за тях по принцип не са необходими специални умения. За нападенията с горим газ и с твърди експлозивни е необходима висока степен на професионален опит.

Нападателите показват различни **нива на компетентност**. От една страна, добре организирани и опитни групи могат да извършат успешно физическо нападение над банкомат за минути. Те владеят процеса и могат да ограничат риска за себе си, като по този начин ограничават и косвените щети. От друга страна, по-слабо организирани групи, които разчитат на късмет, често се провалят в опитите си и могат да причинят значителни щети на помещенията и сградите наоколо. Смята се, че някои от по-слабо организирани ОПГ се връщат към традиционните организирани престъпления срещу собствеността, обезкуражени от превантивните мерки, които не са в състояние да преодолеят при нападение над банкомати.

02 НЕОБХОДИМОСТ ОТ ПРЕВАНТИВЕН ПОДХОД

Държавите, в които извършителите имат ниска успеваемост на физическите нападения над банкомати или където броят на физическите нападения над банкомати намалява, са пример за това, че успешният подход за противодействие на физическите нападения над банкомати се състои от комбинация от оперативни и превантивни мерки. Тъй като броят на ОПГ, занимаващи се с този вид престъпления, е ограничен, арестите и последващите наказания на техните членове намаляват значително броя на нападенията. Въпреки това, след като бъдат освободени, много от нападателите на банкомати възобновяват дейността си. Освен това, понякога групата може да замени арестувания престъпник бързо. Затова има остра нужда от превантивни мерки, за предпочитане включени в правна рамка. Освен това опитът показва, че превантивните мерки в една държава могат да насочат ОПГ към по-уязвими цели в други държави. Въпрос на време е механизмите на действие, възникнали в една страна, да се разпространят в други страни. Това показва ясно **необходимостта от възприемане на превантивни и оперативни мерки на европейско равнище** в тясно сътрудничество между частните, обществени и правоприлагащи партньори.



03 — ПРЕДОТВРАТЯВАНЕ

Необходима е ясна стратегия за предотвратяване и справяне с този вид престъпления. В тази глава ще направим общ преглед на трите стъпки, които обикновено се предприемат, когато сме изправени пред физическо нападение над банкомат или се подготвяме да го предотвратим.

Първо, **оценка на ситуацията**; трябва да се състави профил на риска за банкомата и околностите, като се вземат предвид наличната парична сума (вероятна плячка), риска от косвени щети и риска от телесни повреди. Второ, въз основа на оценката на риска трябва да се състави **стратегия за предотвратяване**. И накрая, трябва да се изпълнят **превантивните мерки**.

1. Оценка на ситуацията

ОПГ обикновено се насочват към определени видове банкомати или банкомати на определени доставчици, които имат характеристики, улесняващи нападението. Затова е необходимо да се направи задълбочена оценка на риска от физическо нападение над банкомата, препоръчително като се включи цялата верига за сигурност на парите от превоза, през доставката до съхранението им в банкомата. За да се състави профил на риска за всеки банкомат, трябва да се анализират множество елементи, сред които са следните.

- Характеристики на местоположението на обекта и околностите на банкомата; характеристики като град или село, гъстота на населението, близост до полицейски управления, камери за автоматично разпознаване на номерата на автомобили (ANPR) в квартала, видеонаблюдение в околността и т.н.
- Местоположение на банкомата:
 - В сградата или извън нея, в банков клон или в отдалечени (например търговски) помещения, вграден или закрепен за сградата,

- за стоящи банкомати: дали са закрепени за пода или не,
- за вградени или закрепени за сградата банкомати: дали има архитектурни слабости, как е организирано съхранението на парите и т.н.
- Видът банкомат.
- Функциите за сигурност, с които е снабден банкоматът.
- Паричната сума, която е в банкомата.
- Видът на физическото нападение над банкомата и механизмът на действие, който може да се очаква, за да се предприемат първо най-подходящите превантивни мерки.
- Мерките за сигурност и превантивните мерки, които вече са въведени (интелигентни системи за неутрализация на банкноти (IBNS), видеонаблюдение, система за димна завеса (намаляване на видимостта) и др.).

Други елементи, които следва да бъдат оценени, са състоянието на сътрудничество с партньорите и участниците, както и законодателството. Сътрудничеството между правоприлагащите органи, частните и обществени партньори трябва да бъде оценено с цел създаване на съюзи за борба с престъпността. Възможно е всеки партньор да разполага с интересна информация, която да допринесе за оценката на ситуацията. Местната полиция или местните власти са особено важни в този контекст. Законодателството трябва да бъде оценено по отношение на създаването на правна рамка за предотвратяване, предприемане на задължителни превантивни мерки, присъди за нападение над банкомат и т.н.

2. Разработване на подход за предотвратяване

След като е направена оценка на ситуацията и основните рискови области и са определени силните и слабите страни в сигурността на банкомата, може да бъде разработена стратегия (често изградена на основата на публично-частно партньорство) и да бъдат въведени превантивни и оперативни мерки за противодействие. Превантивните мерки трябва да бъдат насочени към снижаване на намеренията и възможностите на извършителите. За постигане на тази цел се предлагат три направления за превантивни действия, основани на три от петте стратегии за ситуационно предотвратяване на

престъпления на Clarke²; намаляване на облагите, увеличаване на риска за извършителите и увеличаване на усилията, необходими за достигане до плячката.

Престъпниците претеглят очакваната възвръщаемост спрямо свързаните рискове (например при нападение над банкомат). Намалването на шансовете за постигане на лесна облага и увеличаването на риска за извършителите понижава техните очаквания и желанието им да участват във физическо нападение над банкомат. Допълнителните мерки, които увеличават усилията за достигане до банкомата, оказват влияние върху възможностите на извършителите. Извършителите, които разчитат на късмет и често се провалят в опитите си, спират да се занимават с нападения над банкомати. Успеваемостта на професионалните нападатели над банкомати се намалява, което също засяга съотношението между възвръщаемост и риск.

Освен това стратегията за предотвратяване се допълва от паралелни мерки като ефективна медийна стратегия, ранна обществена превантивна работа и мерки за намаляване на риска от нанасяне на косвени щети на сградите и за гарантиране на безопасността на местните жители, спасителните служби и минавачите.

Възможни са и други начини за структуриране на подхода. Властите в Нидерландия прилагат тъй наречения бариерен модел³. Този модел разкрива стъпките, които даден престъпник трябва да предприеме, за да извърши престъпление. Той разкрива също партньорите и възможностите, които дават възможност за извършване на престъплението, и е полезен инструмент, чрез който да се организира процесът на събиране на информация в областта на престъпността. Като се разкрият всички стъпки, необходими за извършване на физическо нападение над банкомат, могат да бъдат определени бариерите за възпрепятстване на престъплението и най-добрите партньори за установяване на тези бариери. Бариерният модел определя също сигналите, които трябва да предупреждават публичните и частните партньори за физическо нападение над банкомат, както и сигналите, които те самите могат да изпратят, за да уведомят властите за подозренията си.

Необходима е добре разработена стратегия за намаляване на рисковете, съгласувана с

укрепването на мерките за предотвратяване. Мерките за предотвратяване, които са много ефективни за разубеждаване на аматьорите и имитаторите, понякога имат нежелани ефекти. Някои групи започват да действат по метода проба-грешка, за да намерят уязвими банкомати, като оставят след себе си поредица от повредени банкомати. Най-опасните и безскрупулни ОПГ започват да прилагат по-жестоки механизми на действие, като например преминават от газове към твърди експлозиви при своите нападения.

За да се състави ефикасен набор от превантивни мерки, най-добрата практика е създаването на национален орган, който има правомощията да налага конкретни мерки за банкомати, изложени на висок риск, основаващи се на задълбочен анализ на ситуацията. Този подход е доказал ефективността си във Франция, особено ако се създаде правна рамка и мерките се прилагат заедно с оперативните мерки.

3. Изпълнение на превантивните мерки

Ползата от представените в тази глава мерки за предотвратяване на физически нападения над банкомати е доказана в различни държави. Те се основават на заключенията на конференцията на тема предотвратяване и на превантивните мерки, насърчавани активно от международни организации, занимаващи се със сигурността на банкоматите. Много мерки са известни. Няколко държави вече са въвели успешно редица мерки. Въпреки това, предлаганите мерки често се изпълняват само частично и не са заложили в законодателството.

Както бе споменато по-горе, предлагат се три направления за превантивни действия: намаляване на изгодата, увеличаване на риска за извършителите и увеличаване на усилията, необходими за достигане до плячката.

3.1 Намалете изгодата

Намаляването на изгодата от престъпните действия е първото направление в предотвратяването на физическите нападения над банкомати. Докато съществува усещането за „лесни пари“, престъпниците ще продължават да извършват този вид престъпления. Намаляването на наличното

количество пари и премахването или унищожаването на парите намалява възможностите да има плячка, представляваща интерес. Намалените очаквания намаляват желанието на престъпника да извърши такова престъпление.

Намаляване на количеството пари

Една от мерките за намаляване на изгодата е намаляването на наличното количество пари в банкомата. В идеалния случай тази сума трябва да бъде ограничена до необходимата сума само за един работен ден. Сътрудничеството между банките може да осигури ефективност на разходите. В Нидерландия редица банки си сътрудничиха за създаването на независима от банка мрежа от банкомати, наречена „Geldmaat“. Целта на сътрудничеството е да се осигури наличност, достижимост, достъпност и сигурност на паричните средства. Това вероятно ще доведе до намаляване на броя на банкоматите. Всеки банкомат обаче няма да съдържа повече пари, но ще се зарежда по-често. Броят на зарежданията ще бъде адаптиран към потребностите.

Тъй като престъпниците нападат банкомати предимно между 03:00 и 04:00 часа, настоятелно се препоръчва стоящите банкомати (разположени най-често в търговски и обществени помещения, които са по-уязвими), да бъдат изпразвани, а парите да се преместят в сейф в края на деня. Може да се постави табела, предупреждаваща хората, че в банкомата няма пари през нощта. На следващия ден банкоматът трябва да бъде зареден, без това да се вижда от клиентите, докато помещенията са заключени. Тази система се прилага във Франция, където законодателството задължава търговците на дребно със самостоятелен банкомат в магазина да вадят парите през нощта и да оставят банкомата отворен. При други банкомати държаните суми могат да бъдат намалени, като се увеличи честотата на зареждане.

Повреждане на плячката и осигуряване на възможност за проследяване на парите

Интелигентните системи за неутрализация на банкноти (IBNS) представляват първия начин за повреждане на изгодата. Тези системи оцветяват банкнотите с мастило, за да ги бележат като крадени. В мастилото на IBNS могат да бъдат

добавени вещества за проследяване и маркери. В момента тези маркери се използват главно за криминалистични цели, като свързват банкнотата с местопрестъплението и увеличават риска за извършителите да бъдат заловени. Макар че IBNS е ефективна превантивна мярка, има някои съображения.

Европейската централна банка не възстановява оцветените банкноти⁴ (от 2003 г. насам), но редица национални централни банки в държавите членки на ЕС все още го правят. Оцветени банкноти се връщат в законно обращение и чрез казината. IBNS създава допълнителна пречка за престъпниците, но би била много по-ефективна, ако престъпниците не можеха да използват оцветени банкноти в ЕС. За да се постигне това, националните централни банки не трябва да приемат оцветени банкноти. Изключения могат да се правят в особени случаи, като например банкноти, оцветени при фалшиво задействане. Важно е също да се уведоми населението да не приема оцветени банкноти. В по-дългосрочен план акцепторите на банкноти трябва да откриват оцветени банкноти и да бъдат инсталирани в банки и в търговски помещения като казина, автомивки и др. Откриването на мастилото е трудно и скъпо, но рентабилно решение би могло да бъде инсталирането на инфрачервени системи, които откриват банкноти, оцветени с инфрачервени маркери. Тези системи са доказали ефективността си и са част от най-добрите практики в Белгия и Франция. Когато в банкомата се поставят банкноти с инфрачервени маркери, той приема („поглъща“) парите, но не ги кредитира по сметка. Лицето, което поставя оцветените банкноти, също трябва да се регистрира.

Има и някои други съображения при инсталирането на IBNS решения. Няколко производители предоставят редица различни IBNS решения с различни механизми на задействане и различни видове мастило. Първото съображение се отнася до това, че не всички видове технологии за задействане на IBNS могат да противодействат на всички заплахи. Някои IBNS действат много добре при нападения изтръгване/избиване, нападения **на място** и нападения с газ, но не функционират при нападения с твърди експлозивни или обратно. Затова избраната технология трябва да се обмисли добре.

Друго съображение е видът на мастилото, което се използва. В Белгия са определени национални минимални изисквания за IBNS (безопасност,

процент оцветяване, да не се отмива и т.н.) и независими тестове потвърждават, че системата отговаря на държавните стандарти и работи в съответствие с твърденията на производителя. Важно е тестът да се извършва с истински банкноти, тъй като на пазара има по-евтини мастила, които работят добре с подправени/фалшиви банкноти, но не и с истински банкноти: което означава, че мастилото може да бъде отстранено от истинските банкноти чрез измиване. В допълнение към това се препоръчва към мастилото да се добави криминалистичен маркер, което прави възможно разследването на връзка между оцветени банкноти и конкретно местопрестъпление.

Най-добрата практика показва, че IBNS може да бъде много ефективна, особено в комбинация с други превантивни мерки. През 2015 г. Франция въведе ново законодателство, в което има членове относно инсталирането на IBNS и използването на мастило с уникална ДНК. Френската военна полиция (жандармерия) въз основа на оценка на риска решава къде трябва да се прилагат IBNS и други мерки. Тъй като новото законодателство засили превантивния и оперативен подход, броят на нападенията спадна от 300 през 2013 г. на 50 през 2018 г.

Друга техника за повреждане на плячката, която се разработва в момента, е използването на **лепило**. Ефективността на лепилото е доказана в Нидерландия, но засега разходите за внедряване и текущите разходи са високи. Освен това лепилото може да породи опасност от пожар, ако системата не се задейства преди нападението, тъй като разпръскването на частиците лепило във въздуха може да доведе до запалителна смес. Методът не е готов за пазара, но би могъл да бъде решение в бъдеще.

3.2 Увеличете риска

Второ направление в предотвратяването на физически нападения над банкомати е да се възпират потенциалните извършители от извършване на престъпления чрез увеличаване на риска от разкриване и наказание. Освен опасността от телесни повреди при използване на експлозивни за нападения над банкомати, основният риск за престъпника е да бъде осъден на затвор, ако бъде заловен по време на деянието („на местопрестъплението“) или след разследване.

За да се намали желанието на потенциалните извършители, рискът от разкриване и наказание трябва да се увеличи. За обществото залавянето и осъждането на престъпниците е, разбира се, също много ефективен метод за предотвратяване, ако има последващи наказания, както видяхме в някои държави.

Споделяне на информация

От основно значение за разкриването и наказването на нападатели на банкомати е споделянето на информация между всички заинтересовани страни в борбата срещу физическите нападения над банкомати, сред които са производителите на банкомати, правоприлагащите органи (полиция, прокуратура и т.н.), държавните органи, производителите на банкомати и устройства за сигурност и защита, професионалните сдружения, доставчиците на услуги от банкомати (банки и независими доставчици), охранителните фирми и алармените центрове. В идеалния случай това важи както на национално, така и на международно равнище.

Ранното разкриване на предстоящо физическо нападение над банкомат е трудно. Ранно откриване е възможно само в случаите с почти безупречен обмен на информация на международно равнище между правоприлагащи партньори и частни партньори (охранителни фирми и доставчици на банкомати). Трябва да се следи широк спектър от индикатори, включително съобщения за ранно предупреждение между правоприлагащите органи относно раздвижване на ОПГ, информация за („горещи“) превозни средства, използвани при нападения над банкомати, информация от охранителни фирми или наблюдателни съседи за засечено подозрително поведение в района около банкомата, засечени подозрителни транзакции от доставчици на банкомати и други методи за отчитане. Други възможни полицейски мерки за ранно откриване са наблюдение на откраднати автомобили, производители и дистрибутори на експлозивни и фирми с лиценз за употреба на взривни вещества. За ранно откриване са необходими големи усилия, които не дават гаранция за успех, поради което правоприлагащите органи рядко успяват да се намесят преди нападение.

В случай че не е възможно ранно откриване, алармените центрове са в състояние бързо

да издадат предупреждение в случай на физическо нападение над банкомат. За да се даде възможност за намеса, трябва да бъдат съгласувани и създадени национални разпоредби и протоколи за бърза комуникация между алармените центрове и правоприлагащите органи. В случай на ранно откриване или информация в реално време, правоприлагащите органи винаги трябва да преценяват точния момент и най-добрата възможност за намеса. Залавянето на престъпниците на местопрестъплението е много трудно и може да доведе до опасни ситуации, защото някои ОПГ са много жестоки и използват тежко въоръжение.

За успешното разследване след физическо нападение над банкомат, правоприлагащите органи трябва да общуват с всички заинтересовани страни, тъй като всеки един от тях може да разполага с информация, допринасяща за успеха на разследването. Разбира се, комуникацията и сътрудничеството с основните жертви, банките или други доставчици на банкомати са необходими: те имат достъп до важни за разследването данни. На доставчика на банкомати информацията от правоприлагащите органи ще помогне за подобряване на превантивните мерки. Освен това връзките с професионални сдружения и производители се оказват полезни: те често изпращат предупредителни съобщения за сигурност, за които могат да се абонират други заинтересовани страни. Производителите на банкомати имат добър поглед върху различните видове нападения над банкомати и съответните слабости и силни страни на превантивните мерки. Те са готови да окажат подкрепа на полицията с информация за техническите аспекти на банкоматите и за използваните механизми на действие.

Трансграничното сътрудничество е от съществено значение: държавите трябва да споделят информация (за заподозрени, осъдени нападатели на банкомати, механизми на действие, подозрителни превозни средства, снимки от нападения и т.н.) не само в подкрепа на разследването, но и защото заподозрените, осъдени в друга държава, могат да бъдат осъдени за извършване на друго престъпление/рецидив.

И накрая, създаването на база данни на европейско равнище, достъпна за правоприлагащите органи и съдържаща криминалистични данни (например за различни видове мастила, вещества за

проследяване и маркери от IBNS или защитни стъкла за банкомати) може да подпомогне много разследванията и да свърже заподозрените лица с конкретно местопрестъпление. Стандартизацията на технологиите на международно ниво често е недостатъчна: по време на конференцията през януари 2019 г. участниците посочиха, че стандартизацията на мастило и маркери на престъпления на ниво ЕС може значително да улесни разследванията.

Видеонаблюдение и подслушвателни устройства

Картината и звукът от системите за видеонаблюдение и подслушвателните устройства могат да спомогнат както за откриване на нападение в реално време (например за предотвратяване на телесни повреди на спасителите, пристигнали на местопрестъплението), така и за последващи разследвания (например за идентифициране на извършителите и техните механизми на действие). Картината от системата за видеонаблюдение може да се комбинира с картина от обществени и други системи за видеонаблюдение в съседство с банкомата и с кадри от пътни радари, за да се предостави по-пълна картина на извършителите и техния механизъм на действие.

Картината от системата за видеонаблюдение обаче често е с лошо качество или не се съхранява добре. Изображенията трябва да бъдат достатъчно качествени, за да дадат възможност за идентификация на дадено лице. И тук създаването на европейски стандарти за охранително видеонаблюдение би улеснило разследванията. Освен това, тъй като извършителите често изключват камерите за видеонаблюдение преди нападението, може да се обмисли и инсталирането на скрита система за видеонаблюдение или на устройства за подслушване в реално време.

Наказание и реабилитация на престъпници

Доказано е, че последователните и тежки наказания имат превантивен ефект. Арестът на дадена ОПГ оказва непосредствено въздействие върху броя на нападенията над банкомати. Освобождаването от затвора на нападатели на банкомати обаче също толкова често води до ново внезапно нарастване на броя на нападенията. Това означава, че

малките присъди водят до това, че извършителите подновяват дейността си много бързо. Минималните и максималните наказания за престъпници, осъдени за всеки вид физическо нападение над банкомат, се различават в отделните държави членки. Някои хора смятат, че по-големите наказания ще възпират потенциалните извършители. Научните изследвания⁵ обаче сочат, че увеличаването на строгостта на присъдите не оказва непременно възпиращо въздействие. Ето защо може да представлява интерес да се разгледат поправителните програми за реабилитация (и тези на база конкретен престъпник), за да се намали високата степен на рецидивизъм.

3.3 Увеличете усилиято

Третото направление в предотвратяването на физическите нападения над банкомати съдържа действия, които затрудняват извършването на криминалното деяние от престъпника.

Осигуряване на устойчива на престъпления среда

В случай че оценката на риска (вижте по-горе) сочи, че банкоматът е разположен в среда с висок риск, обектът трябва да се премахне, а банкоматът да бъде преместен в район с нисък или средно висок риск. Със сигурност такъв е случаят, ако анализът покаже, че сградата може да се срути, ако банкоматът бъде атакуван с експлозиви. Може да се въведе законодателство за налагане на такива мерки в случаи с висок риск. Освен намаляване на броя на банкоматите в среда с висок риск, безкасовите плащания трябва да бъдат насърчавани, за да се намали нуждата от банкомати.

В случай че не е възможно да се премести банкоматът, трябва да се вземат максимални мерки за сигурност: например използване на колони против таран, стълбове за осветление и друго улично оборудване за ограничаване на достъпа до сградата, системи за спиране на автомобили, монтаж на подходящо улично осветление, увеличаване на явната или скритата охрана и устройства против кражба, като система за повреждане на банкнотите. Когато бъде нападат обект на място, което не е било определено с висок риск, то трябва да бъде определено като такова и да се предприемат допълнителни мерки за сигурност.

Новите фактори трябва да бъдат взети предвид в приложението за оценка на риска, за да бъде актуализирано. Повторната оценка на този риск трябва да бъде повтарящо се действие.

Усилване на банкоматите

Производителите на банкомати предлагат стандартна гама от банкомати, които разполагат с редица функции за сигурност, класирани според определените от Европейския комитет за стандартизация (CEN) степени на сигурност. Обикновено банкоматите имат маркировка CEN, от най-ниския клас CEN1 до най-високия - CEN4. Характеристики като здравина на корпуса и устойчивост на нападение определят класа. Устойчивостта на газ най-често се предлага като опция (CEN-GAS). Стандартните модели могат да бъдат подобрени с допълнителни защитни мерки. Обикновено тези функции се инсталират от трети страни, за да се гарантира съответствие с местното законодателство и да се пригоди базовият модел към изискванията на местните клиенти. Допълнителните характеристики за сигурност включват различни сензори за включване на система за неутрализиране на газове или IBNS в случай на нападение **на място** или с експлозивни и усиленни щори и ключалки на трезори за предотвратяване на неправомерно проникване в сейфа, когато основната решетка е компрометирана. За преносими, стоящи банкомати е важно да се използват анкерирани системи, които предлагат допълнителна защита срещу нападения с изтръгване/избиване. В банкомата могат да бъдат заложили устройства за проследяване в помощ на разследващите, в случай че банкоматът бъде пренесен на друго място, преди да бъде отворен.

Архитектурни мерки

Предлага се, когато се инсталира банкомат, той да бъде с достъп отзад. В такъв случай извършителят ще трябва да влезе в сградата и да стигне до задната част на машината, за да открадне парите. Най-силно уязвими са преносимите стоящи банкомати. Намалването на броя на този вид банкомати би повишило сигурността. Задължението за инсталиране на банкомати в помещения, защитени срещу проникване с взлом, автоматично ще намали ползването на стоящия банкомат.

Система за димна завеса

Димно оръдие изпълва бързо помещението с плътна мъгла, така че нападателят да не може да види нищо. Такава димна завеса често прави невъзможно извършването на нападение над банкомата. Най-малкото системата забавя извършителя, оставяйки време за намеса на полицейските служби. Охранителната система за димна завеса е свързана с алармената система и може да се задейства по два начина. Може да се задейства автоматично от алармени сензори, като детектори за движение (през нощта) или от сензори за задвижване на щорите. Тя може да се задейства също от алармен център, за да се избегнат прекалено много фалшиви аларми. За външни банкомати, вградени в стената, системата за димна завеса може да се сложи в задната част на банкомата, за да изпълни помещението отзад с дим и да сведе видимостта на извършителите до нула.

Системите за дим могат да осигурят защита в една точка на банкомати, разположени на открити пространства в бензиностанции, супермаркети и т.н. По този начин се избягва изпълването на целия район с дим. Защитата с дим има най-голям успех, когато димът идва от различни ъгли, или когато изпълва пространството зад банкомата с дим в случай

на таран. Продължават да се провеждат тестове, за да се установи дали оръдията за дим могат да бъдат инсталирани в самия банкомат, вместо в помещението, където се намира банкоматът. Към дима могат да бъдат добавени ДНК маркери, които оцветяват извършителите и дрехите им.

3.4 Паралелни мерки

За да се осигури ефикасното и ефективно изпълнение на горепосочените превантивни мерки, трябва да се разгледат редица паралелни мерки. Тези мерки са необходими, за да се даде възможност или да се засили цялостен превантивен и оперативен подход за справяне с физическите нападения над банкомати.

Законодателство

В редица държави законодателството задължава доставчиците на банкомати да предприемат превантивни мерки. В други държави сключването

на споразумения и договори между банки и правоприлагащи органи осигурява работещ подход за справяне с физическите нападения над банкомати. Областите, в които могат да бъдат разгледани регулаторни мерки, включват:

- включване на превантивни мерки;
- правни рамки, позволяващи сътрудничество между правоприлагащите органи и публичните и частни партньори;
- изменение на присъдите, ако наказанията за извършителите на физически нападения над банкомат са твърде малки.

Често обаче само банкови институции са длъжни да се съобразяват и независимите доставчици на банкомати не са обвързани от тези закони или споразумения. Това е често срещана слабост на нормативната уредба.

В някои държави не се налагат никакви правила, а се опитват да убедят доставчиците на банкомати да предприемат превантивни мерки чрез повишаване на осведомеността им за видовете престъпления и тенденциите: в държави с голям брой независими банки това се оказва особено трудно.

Задължително е да се гарантира, че ефективното прилагане на превантивните мерки включва промени в законодателството и нормативната уредба както на национално, така и на международно равнище, задължителни за доставчиците на всички видове банкомати. В идеалния случай законодателството трябва да бъде приведено в съответствие на равнище ЕС, за да не стане така, че строгите превантивни мерки, залегнали в законодателството на една държава да насочат ОПГ към други държави с по-малко строга нормативна уредба.

Медийна стратегия

Друго важно направление в превантивната стратегия е утвърдена медийна стратегия, която има за цел да намали очакванията и желанието на нападателите на банкомати да извършват това престъпление. Трябва да се подчертае ниската успеваемост и високият риск за извършителите; съобщения за изгода („пљачка“) или подробности за нападението, като например вида на засегнатия банкомат или механизма на действие, да се избягват. От друга страна, обширните съобщения за ареста на заподозрените и последвалото наказание след осъждането им са необходими.

Подобрено сътрудничество

Подобреното сътрудничество и обменът на информация бяха споменати подробно, но не могат да бъдат подчертани достатъчно. Обменът на оперативна информация на международно равнище е основна дейност на Европол. Освен обмен на информация, конференцията на тема предотвратяване показва ясно необходимостта от разширяване на сътрудничеството в различни области и на различни нива и от обмен на информация между всички заинтересовани страни, включително правоприлагащи органи, държавни власти, производители на банкомати и устройства за сигурност и защита, професионални сдружения, доставчици на банкомати (банки и независими доставчици), охранителни фирми и алармени центрове. Това трябва да се прави на местно, национално и международно равнище.

Намаляване на риска от косвени щети

В случай на нападение с твърди експлозиви, някои ОПГ оставят материали след себе си. Това може да породи опасности за спасителите или за цивилни лица (живеещи в съседство или преминаващи през района). Тяхната безопасност трябва да бъде гарантирана. Както е в Белгия, протоколите и процедурите, които следва да бъдат спазвани от спасителите (както от правоприлагащите органи, така и от доставчиците на банкомати), трябва да бъдат разработени и съгласувани помежду си. Друга най-добра практика в този контекст е примерът с Нидерландия, където за оценка на ситуацията се използват кадри от видеонаблюдение на нападението на банкомата. Могат да бъдат сключени договори с алармените центрове, за да могат тези образи да бъдат достъпни незабавно.

Обществена превантивна дейност

Често ОПГ се опитват да привлекат млади хора. Могат да бъдат създадени проекти, които да осуетят тези процеси за привличане на ранен етап. Полицията или социалните работници трябва да бъдат внимателни към тези процеси и могат да се намесят, като се обърнат лично към потенциалните извършители.

04 — ЗАКЛЮЧЕНИЯ

През последните 2 години броят на европейските държави, засегнати от физически нападения над банкомати, се е увеличил. В тази връзка Европол и EUCPN работиха заедно, за да съберат най-добрите мерки за борба и предотвратяване на този вид престъпления.

Успешният подход за противодействие на физическите нападения над банкомати се състои от комбинация от оперативни и превантивни мерки, за предпочитане включени в законодателна рамка. За да се избегне пренасочването на ОПГ от една държава със строги мерки към други, по-силно уязвими държави, препоръчва се мерките да бъдат приети на европейско равнище.

За предотвратяване и справяне с този вид престъпление следва да се създаде ясна стратегия в три стъпки: оценка на ситуацията, разработване на превантивен подход въз основа на оценката на риска и прилагане на превантивните мерки.

Оценката на риска от физически нападения над банкомати трябва да включва характеристиките на банкомата и околностите му, сътрудничеството с партньори и заинтересовани страни с цел изграждане на съюзи за борба с това престъпление и оценката на превантивната и правна рамка. След като е направена оценка на ситуацията може да бъде съставена стратегия, изградена на основата на публично-частно партньорство и превантивни и оперативни мерки за противодействие. Целта на превантивните мерки е да се намалят намерението и възможностите на престъпника да извърши физическо нападение над банкомат. За постигането на тази цел се предлагат три

направления за превантивни мерки: намаляване на изгодата, увеличаване на риска и увеличаване на усилията. Превантивната стратегия трябва да бъде допълнена от паралелни мерки. Най-добра практика е създаването на национален орган, който има правомощия да наложи необходимите мерки.

Като **намали изгодата**, се намалява желанието на престъпника да извърши такова престъпление. Намаляването на паричната сума в банкомата като се намали зареждането му с пари до сума, достатъчна за 1 работен ден, или изпразването на (най-уязвимите) банкомати през нощта е една от мерките за намаляване на очакванията на престъпниците. Друг начин е да се повреди плячката и да се осигури проследяване на парите. В този контекст може да се използва IBNS, която оцветява банкнотите и ги маркира като крадени. Този метод е най-ефективен, когато престъпниците не могат да харчат тези пари или да върнат тези банкноти в законно обращение. Това може да се постигне като банките и обществото не приемат оцветени банкноти за разплащане и се инсталират акцептори за банкноти, които могат да открият и откажат оцветените банкноти. В тази връзка инвестицията в инфрачервени системи, които откриват оцветени банкноти с инфрачервени маркери, се оказва рентабилно решение в Белгия и Франция. Когато инсталират IBNS, държавите трябва да обмислят подробно избраните механизми за задействане, минималните изисквания за неутрализиране на банкнотите и добавянето на криминалистичен маркер към мастилото.

Мерки, възпиращи потенциалните престъпници от извършване на престъпления, чрез **увеличаване**

на риска от разкриване и наказание, представляват второто направление в предотвратяването на физическите нападения над банкомати. От основно значение за разкриването и наказването на нападателите на банкомати е събирането и споделянето на информация между всички заинтересовани страни, както на национално, така и на международно равнище. Информационният обмен на висококачествени кадри от видеонаблюдение и звукозаписи може да увеличи шансовете за ранно откриване и успешно разследване. За да се избегне изключването на видеонаблюдението или подслушвателните устройства преди нападението, може да се обмисли инсталирането на скрити устройства за видеонаблюдение или подслушване в реално време. Създаването на криминалистична база данни и стандартизацията на технологиите на европейско равнище може да улесни значително международното сътрудничество и разследванията. В случай че престъпниците са заловени и осъдени може да представлява интерес да се разгледат поправителните програми за реабилитация (и тези на база конкретен престъпник), за да се намали високата степен на рецидивизъм.

Третото направление в предотвратяването на физическите нападения над банкомати включва мерки за **увеличаване на усилието**, необходимо за извършване на криминалното деяние от престъпника. Инсталирането на банкомат в устойчива на престъпления среда с максимални мерки за сигурност ще затрудни нападението над банкомат от страна на престъпниците. Освен това стандартната защита на банкомата може да бъде подобрена с редица допълнителни функции

за сигурност. В допълнение към тези мерки, инсталирането на система за дим може да възпре извършителя или поне да забави нападението.

Редица **паралелни мерки** биха засилили горепосочените мерки, като например създаването на правна рамка, която задължава всички доставчици на банкомати да прилагат превантивните мерки, разработването на утвърдена медийна стратегия, подобреното сътрудничество на местно, национално и международно равнище, указания към спасителите, за да се намали риска от косвени щети, и инвестирането в обществена превантивна дейност с цел затрудняване на процесите на привличане на нови членове на престъпните групи.

Разработване на ефективна реакция за предотвратяване на физически нападения над банкомати

Оценка на ситуацията

- > Създаване на профил на риска за банкоматите в държавата/ региона
- > Откриване на партньори и заинтересовани страни в борбата срещу физическите нападения над банкомати и оценка на сътрудничеството
- > Оценка на правната рамка за справяне с физическите нападения над банкомати на национално и международно равнище

Разработване на подход за предотвратяване

- > Определяне на (основните) рискове, които следва да бъдат обхванати, и на приоритетите
- > Определяне на най-добрите превантивни мерки за обхващане на тези рискове, като се имат предвид трите основни направления.
- > Определяне на паралелните превантивни мерки, необходими за подсилване на предприетите



Превантивни мерки, които могат да бъдат предприети, за

01

Намаляване на изгодата

- > Намаляване на количеството пари.
 - Изпразване на банкомата за през нощта.
 - Увеличаване на броя/честотата на зарежданията.
- > Повреждане на плячката.
 - Интелигентни системи за неутрализация на банкноти (IBNS).
 - Инфрачервени маркери в мастилото на IBNS с цел откриване на оцветените банкноти от акцептори на банкноти.
 - В процес на разработване: лепило.

02

Увеличаване на риска

- > Трансгранично споделяне на информация за:
 - ранно откриване или откриване в реално време на вероятно нападение над банкомат,
 - укрепване на оперативния подход,
 - осъждане на рецидивистите,
 - обмен на криминалистични данни на европейско равнище.
- > Видеонаблюдение и подслушвателни устройства.
- > Последователно наказание и реабилитация на престъпници.

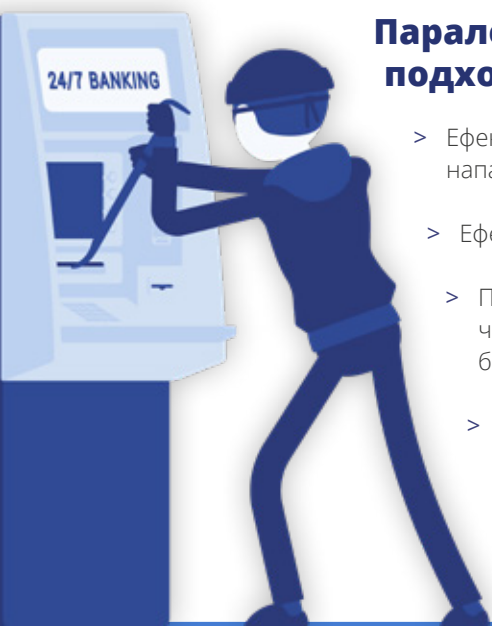
03

Увеличаване на усилието

- > Осигуряване на устойчива на престъпления среда.
 - Промяна на местоположението на банкомати във висок риск.
 - Мерки за сигурност: физически препятствия, наблюдение и т.н.
- > Усилване на банкоматите с щори, устойчиви на газове и твърди експлозиви и т.н.
- > Архитектурни мерки, като например машини с достъп от задната страна
- > Охранителни системи за дим.

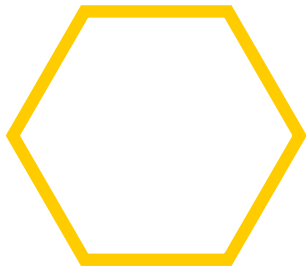
Паралелни мерки за укрепване на превантивния подход

- > Ефективно законодателство, включващо превантивни мерки срещу физическите нападения над банкомати, последващо осъждане и т.н.
- > Ефективна медийна стратегия, възпираща извършителите.
- > Подобро сътрудничество между всички заинтересовани страни (публични, частни, правоприлагащи органи) в борбата срещу физическите нападения над банкомати.
- > Намаляване на риска от косвени щети за спасителите или гражданите (например живеещите в квартала или минувачите).
- > Обществена превантивна дейност, която предотвратява наемането на млади хора за извършване на (този вид) престъпления.



ENDNOTES

- 1 Willem Pieter de Groen, Zachary Kilhoffer и Roberto Musmeci, Бъдещето на банкоматите в ЕС: *въздействие на цифровизацията и политиките за ценообразуване върху бизнес моделите*, Доклад на CEPS, 2018 г.
- 2 Derek Cornish and Ronald V. Clarke, 'Opportunities, precipitators and criminal decisions: a reply to Wortley's critique of situational crime prevention', *Crime prevention Studies* 16 (2003), стр. 41-96.
- 3 Centrum voor Criminaliteitspreventie, barrieremodellen, www.barrieremodellen.nl
- 4 Решение на Европейската централна банка относно купюрите, спецификациите, възпроизвеждането, замяната и изтеглянето на Евро банкноти от 2003 г.
- 5 David Weisburd, David P. Farrington and Charlotte Gill, 'Conclusion: *What Works in Crime Prevention Revisited*', David Weisburd, David P. Farrington and Charlotte Gill, *What works in Crime Prevention and Rehabilitation*. Cambridge: Springer, 2016, 311.



CONTACT DETAILS

EUCPN Secretariat

Phone: +32 2 557 33 30

Email: eucpn@ibz.eu

Website: www.eucpn.org, www.europol.europa.eu



[TWITTER.COM/EUCPN](https://twitter.com/EUCPN)



[FACEBOOK.COM/EUCPN](https://facebook.com/EUCPN)



[LINKEDIN.COM/COMPANY/EUCPN](https://linkedin.com/company/eucpn)