Prevenire gli attacchi fisici agli ATM

SVILUPPARE UN APPROCCIO EFFICACE

EUCPN
EUROPEAN CRIME PREVENTION NETWORK
EMPACT
EUROPOL

“

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

”

RINGRAZIAMENTI

Questo documento è frutto di una collaborazione tra l'Agenzia dell'Unione europea per la cooperazione tra le forze dell'ordine (Europol) e il segretariato della Rete europea di prevenzione della criminalità (EUCPN). Ringraziamo gli esperti di attacchi fisici agli sportelli automatici (bancomat ATM) che hanno investito tempo e sforzi a sostegno della creazione di questo documento di raccomandazione. Tali attori hanno contribuito partecipando alla conferenza sulla prevenzione degli attacchi fisici agli ATM (gennaio 2019, Bruxelles) e fornendo informazioni cruciali. In particolare, desideriamo ringraziare le forze dell'ordine dei paesi dell'UE e non appartenenti all'UE ("paesi terzi"), il settore privato, tra cui l'Associazione dell'industria ATM (ATMIA), BPost, Centrum voor Criminaliteitspreventie en Veiligheid (CCV), Diebold Nixdorf, il gruppo di esperti il gruppo di esperti dell'Associazione europea per la sicurezza delle transazioni su ATM e casseforti per sportelli automatici ATS Attacchi fisici (EAST EGAP), la European Intelligent Cash Protection Association (Euricpa), ING, Febelfin, NCR, Protect, SIOC Banking, Spinnaker, TMD Security e i ministeri dell'Interno di Belgio, Croazia, Germania e Spagna.

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

CONTENTS

CONTESTO

Con l'aumento del numero di attacchi fisici agli sportelli automatici (ATM) e del numero di paesi europei interessati, la Rete europea di prevenzione della criminalità (EUCPN) ed Europol hanno organizzato una conferenza (gennaio 2019) che ha riunito le forze dell'ordine con partner pubblici e privati per esaminare la prevenzione di questo reato. Il presente documento di raccomandazione riassume le conclusioni di tale conferenza per sensibilizzare le autorità in merito agli attacchi fisici agli ATM e alle misure preventive.

Un numero limitato, ma crescente, di paesi dell'Unione europea è preoccupato dagli attacchi fisici agli sportelli automatici. Nel 2017, in Europa, si è stimata una perdita finanziaria causata da tale fenomeno pari a oltre 30 milioni di euro. Se è vero che alcuni paesi continuano ad assistere a un numero significativo e costante di attacchi fisici ai danni dei bancomat, altri hanno registrato un considerevole aumento del numero di questi reati negli ultimi 2 anni. Si tratta di un settore criminale in rapida evoluzione. Alcuni paesi si sono dimostrati efficaci nel contrasto agli attacchi fisici agli ATM e di recente hanno assistito a una notevole diminuzione di tali effrazioni. D'altro canto, i paesi precedentemente non interessati dal fenomeno hanno dovuto far fronte a un'improvvisa ondata di attacchi fisici agli sportelli automatici nel 2018 a causa dell'espansione del territorio da parte di gruppi criminali organizzati. A essere colpite non sono solo le banche, ma sempre più spesso anche gli sportelli automatici di fornitori indipendenti che spesso si trovano in locali o luoghi più vulnerabili.

L'ampia gamma di diversi metodi (modi operandi (MO)) utilizzati dai criminali per attaccare gli sportelli automatici può essere suddivisa in due macrocategorie: gli attacchi fisici e quelli fraudolenti legati agli ATM (tra cui gli attacchi logici agli ATM e gli attacchi malware). Il presente documento si concentra sugli attacchi fisici agli ATM: l'effrazione con mezzi fisici negli sportelli automatici per prelevare il contante. L'effrazione può essere effettuata mediante:

> **l'uso di esplosivi:** gli aggressori utilizzano gas o esplosivi solidi per scassinare fisicamente la cassaforte del bancomat e accedere al contante;

> **attacchi di sfondamento con auto-ariete:** gli aggressori rimuovono fisicamente l'ATM dall'ambiente di installazione, spesso utilizzando un veicolo di fascia alta;

> **attacchi in situ:** gli aggressori estraggono la cassaforte con la forza bruta, spesso utilizzando utensili da taglio o da rottura come smerigliatrici angolari, mazze o torce ossiacetileniche.

01 FATTORI CONCORRENTI AL SUCCESSO DI UN ATTACCO FISICO A UNO SPORTELLO ATM

Il tasso di successo degli attacchi agli ATM è basso: solo un terzo va a buon fine. Tuttavia, anche quando l'attacco non ha successo, il danno causato (ad esempio da esplosivi) alle strutture edilizie è comunque ingente e genera un ambiente non sicuro in prossimità della scena del crimine per i residenti locali, i primi soccorritori e i passanti.

Il successo di un attacco fisico dipende da una serie di fattori, tra cui: le caratteristiche di un ATM, l'impostazione dell'attacco allo sportello e l'esperienza e il know-how degli autori del reato.

1. Vulnerabilità degli sportelli ATM

Gli ATM più vulnerabili sono quelli situati all'esterno (attraverso il muro (TTW)) o quelli che si trovano all'interno degli edifici. Quando attaccano un bancomat interno (a se stante), i gruppi criminali organizzati preferiscono gli ATM situati in locali commerciali rispetto a sportelli automatici situati in locali bancari dove la sorveglianza è solitamente più forte. Le banche gestiscono principalmente ATM situati all'interno o all'esterno di un edificio bancario. Le sedi remote delle banche su strada o nei locali commerciali di commercianti

come stazioni di servizio, supermercati, alberghi, casinò, aeroporti, ecc. stanno diventando poco a poco sempre più importanti con la chiusura delle filiali bancarie. I fornitori indipendenti gestiscono gli ATM come servizio autonomo. I loro sportelli bancomat sono spesso situati in esercizi di vendita al dettaglio, strutture ricettive e di svago, luoghi di trasporto (stazioni ferroviarie, aeroporti, ecc.), edifici pubblici e in strada.

Con la crescente popolarità dell'online banking, nei prossimi anni molte filiali bancarie probabilmente andranno incontro a chiusure, con una conseguente diminuzione complessiva del numero di sportelli ATM[1] Tuttavia, ciò potrebbe comportare un aumento del numero di sportelli bancomat a distanza e di distributori automatici indipendenti situati in punti più vulnerabili.

2. Preparazione di un attacco a uno sportello ATM

La preparazione di un attacco può richiedere fino a diverse settimane o addirittura mesi. Gli autori del reato devono raccogliere gli **strumenti e le risorse** necessari, quali veicoli, attrezzature e punti di contatto. I **veicoli** sono uno strumento essenziale per gli attacchi fisici agli ATM: i criminali si muovono, infatti, principalmente in auto e dopo l'attacco si spostano spesso con veicoli veloci, che spesso vengono rubati, ma che possono anche essere noleggiati o acquistati (ad es. via Internet). La maggior parte delle **attrezzature** per gli attacchi fisici agli ATM è facilmente e legalmente disponibile in comuni negozi: Ciò abbassa ulteriormente la soglia che consente di affacciarsi a questo settore criminale. Poiché le forze dell'ordine hanno difficoltà a rintracciare l'origine di un dato strumento, i rischi per gli autori del reato sono limitati. I gruppi criminali organizzati attivi negli attacchi fisici agli ATM a livello internazionale dispongono quasi sempre di punti di contatto nel paese interessato (persone che vi risiedono per un certo periodo) o, in alternativa, possono avvalersi di una tecnica "mordi e fuggi". Questi contatti supportano i gruppi criminali organizzati sul piano logistico, come l'affitto di alloggi, l'acquisto di veicoli o di altre attrezzature e la ricerca di obiettivi. Alcuni criminali internazionali lasciano la logistica e la ricerca degli obiettivi in toto ai contatti locali e si limitano a viaggiare su strada o in aereo per l'esecuzione degli attacchi agli ATM.

I gruppi criminali organizzati spesso svolgono **ricognizioni** approfondite per individuare gli obiettivi più adatti; valutano l'ora del giorno in cui il bancomat viene rifornito, l'ambiente circostante, le specifiche tecniche dell'ATM, le vie di fuga e le misure di sicurezza in atto, come televisione a circuito chiuso (TVCC), sensori di allarme e serrande.

Alcuni gruppi criminali organizzati intraprendono una serie di azioni per **sventare l'intervento delle forze dell'ordine e i servizi di sicurezza** prima dell'attacco. Manomettono i sistemi di allarme e l'illuminazione pubblica, utilizzano tecniche diversive, creano blocchi stradali o tentano di sabotare i veicoli delle forze dell'ordine.

3. L'esperienza e il know-how dei criminali

Gli attacchi fisici agli sportelli ATM risultano interessanti agli occhi dei criminali perché il denaro è immediatamente disponibile e non c'è bisogno di disporre di una rete capillare per la ricettazione della refurtiva. Si tratta di un'alternativa conveniente per criminali già attivi in associazioni a delinquere.

I gruppi criminali organizzati devono raccogliere le **competenze e il know-how necessari**, poiché questi sono un fattore determinante per il successo o il fallimento di un attacco. La competenza e il know-how richiesti dipendono fortemente dal **tipo di attacco**. Gli attacchi di sfondamento con auto-ariete e *in situ* si basano su un MO semplice (che prevede principalmente l'audacia e l'uso della forza bruta) e, in genere, non richiedono competenze specifiche. Gli attacchi che ricorrono all'utilizzo di gas combustibili ed esplosivi solidi, invece, esigono un livello di competenza più elevato.

Gli autori del reato mostrano dunque diversi **livelli di competenza**. Se da un lato, gruppi altamente organizzati ed esperti riescono a commettere un attacco fisico a un bancomat in pochi minuti (hanno il controllo del processo e sono in grado di limitare il rischio per se stessi contenendo così anche i danni collaterali); dall'altro, i gruppi meno organizzati e opportunisti spesso falliscono nei loro tentativi e possono causare ingenti danni ai locali e agli edifici del quartiere. Si ritiene che alcune delle associazioni a delinquere meno organizzate siano tornate a dedicarsi alle tradizionali attività della criminalità organizzata, scoraggiate da misure preventive che non sono in grado di superare per le rapine ai bancomat.

02 NECESSITÀ DI UN APPROCCIO PREVENTIVO

I paesi in cui si registrano bassi tassi di successo sul fronte degli attacchi fisici agli ATM o in cui il numero di attacchi fisici ai bancomat è in calo dimostrano che, per contrastare efficacemente gli attacchi fisici agli sportelli automatici, è necessario adottare un approccio consistente in una combinazione di misure operative e preventive. Poiché il numero di gruppi criminali organizzati attivi in questo settore criminale è limitato, gli arresti e le conseguenti punizioni dei membri dei gruppi criminali organizzati riducono notevolmente il numero di attacchi. Tuttavia, una volta rilasciati, molti rapinatori di ATM riprendono le loro attività. Inoltre, un gruppo può talvolta sostituire rapidamente il criminale arrestato. Vi è quindi una forte necessità di misure preventive, preferibilmente inserite in un quadro legislativo. Inoltre, l'esperienza dimostra che le misure di prevenzione in uno Stato possono spingere i gruppi criminali organizzati verso obiettivi più vulnerabili in altri paesi. È solo questione di tempo prima che i MO che emergono in un paese si diffondano altrove. Ciò indica chiaramente il **bisogno di adottare misure preventive e operative a livello europeo** con partner privati, pubblici e delle forze dell'ordine che lavorano in stretta collaborazione.

03 PREVENZIONE

Per prevenire e affrontare questo tipo di criminalità è necessaria una strategia chiara. In questo capitolo vedremo una panoramica delle tre misure che vengono generalmente adottate quando ci si trova dinnanzi ad attacchi fisici agli ATM o quando ci si prepara a prevenirli.

Prima di tutto la **valutazione della situazione**: sarebbe opportuno stabilire un profilo di rischio degli sportelli automatici e dell'ambiente circostante considerando la quantità di contante disponibile (il possibile bottino), il rischio di danni collaterali e il rischio di lesioni personali. In secondo luogo, sulla base della valutazione del rischio, si dovrebbe sviluppare una **strategia preventiva.** Infine, dovrebbero essere attuate **misure preventive.**

1. Valutare la situazione

I gruppi criminali organizzati tendono a colpire sia determinati tipi di sportelli automatici o ATM di specifici fornitori con caratteristiche che facilitano l'attacco agli sportelli stessi. È pertanto necessario eseguire una valutazione approfondita del rischio di attacchi fisici agli ATM, includendo preferibilmente l'intera catena di sicurezza del contante, dal transito alla consegna fino allo stoccaggio nel bancomat. Per stabilire il profilo di rischio di ogni ATM occorre analizzare una serie di elementi, tra cui i seguenti.

- Le caratteristiche dell'ubicazione del sito e dei dintorni del bancomat; caratteristiche come la posizione della città o della campagna, la densità di popolazione, la vicinanza delle stazioni di polizia, le telecamere per il riconoscimento automatico della targa (ANPR) nel quartiere, la presenza di sistemi TVCC nei dintorni, ecc.
- L'ubicazione dell'ATM:
  - all'interno o all'esterno di un edificio, in una filiale di una banca o in un locale remoto (ad es. commerciale), integrato o annesso a un edificio;
  - per ATM autonomi: che siano integrati o meno,
  - per ATM integrati o annessi a un edificio: se ci sono punti deboli architettonici, come è organizzato il deposito del contante, ecc.
- Il tipo di ATM.
- Le funzionalità di sicurezza incluse nell'ATM.
- La quantità di contanti nell'ATM.
- Il tipo di attacchi fisici agli ATM e il MO prevedibile per adottare anticipatamente le misure preventive più adeguate.
- Le misure di sicurezza e di prevenzione già adottate (sistemi intelligenti di neutralizzazione delle banconote (IBNS), TVCC, sistemi di sicurezza nebbiogeni (riduzione della visibilità) ecc.).

Altri elementi da considerare sono lo stato della cooperazione con i partner e i soggetti interessati e la legislazione. Sarebbe opportuno valutare la collaborazione tra forze dell'ordine, partner privati e pubblici in modo da stringere alleanze volte a combattere la criminalità. È possibile che ogni partner possieda informazioni interessanti per contribuire alla valutazione della situazione. La polizia locale o le autorità locali sono particolarmente importanti in questo contesto. Peraltro occorre studiare la legislazione in termini di definizione di un quadro giuridico per la prevenzione, di adozione di misure preventive obbligatorie, di condanne emesse per attacchi agli ATM, ecc.

2. Sviluppare un approccio preventivo

Una volta valutata la situazione e stabilite le principali aree di rischio e i punti di forza e di debolezza della sicurezza di uno sportello ATM, è possibile sviluppare una strategia (spesso basata sulla collaborazione tra settore pubblico e privato) e mettere in atto contromisure preventive e operative. Le misure di prevenzione dovrebbero mirare a ridurre le intenzioni e le capacità dei criminali. Per raggiungere questo obiettivo, vengono proposti tre assi di azioni preventive fondate su tre delle cinque strategie di prevenzione della criminalità situazionale di Clarke[2]; ridurre le ricompense, aumentare il rischio per gli esecutori e aumentare lo sforzo per accedere al bottino.

I criminali fanno un bilancio del rendimento previsto e dei rischi associati (ad es. in caso di attacco a un bancomat). Riducendo le possibilità di una facile ricompensa e accrescendo i rischi, si riducono le aspettative e il desiderio dei criminali di perpetrare un attacco fisico a un bancomat. Ulteriori misure che aumentano lo sforzo necessario per accedere allo sportello ATM influiscono sulle capacità degli autori del reato. Gli esecutori opportunisti, che spesso falliscono nei loro tentativi, smettono di attaccare gli ATM. Per i rapinatori professionisti di ATM il tasso di successo si riduce, influenzando di nuovo il rapporto rischio/rendimento.

Inoltre, la strategia di prevenzione è completata da misure parallele, come un'efficace strategia mediatica, la prevenzione sociale precoce e misure per ridurre il rischio di danni collaterali agli edifici e atte a garantire la sicurezza dei residenti locali, dei primi soccorritori e dei passanti.

Tale approccio può ad ogni modo essere strutturato in altri modi. Nei Paesi Bassi le autorità applicano il cosiddetto modello a barriere[3]. Tale modello identifica i passi che un criminale deve compiere per commettere un reato. Individua inoltre i partner e le opportunità che consentono il reato ed è un utile strumento per organizzare il processo di raccolta di informazioni in un dato ambito criminale. Individuando ogni passo necessario per eseguire un attacco fisico a un ATM, si possono individuare le barriere per ostacolare il reato e i partner migliori per erigerle. Il modello a barriere identifica anche segnali per avvertire i partner pubblici e privati di attacchi fisici agli sportelli automatici e segnali che essi stessi possono inviare per comunicare alle autorità i loro sospetti.

È necessaria una strategia ben sviluppata per mitigare i rischi che vanno di pari passo con il rafforzamento della prevenzione. Le misure preventive, che sono molto efficaci nello scoraggiare dilettanti ed emulatori, a volte hanno effetti indesiderati. Alcuni gruppi si avvalgono di metodi per tentativi ed errori per trovare gli ATM più vulnerabili, lasciando una scia di sportelli automatici danneggiati dietro di sé. I gruppi criminali organizzati più pericolosi e spietati cominciano a utilizzare MO più violenti, passando dall'impiego di gas agli esplosivi solidi nei loro attacchi.

Per definire un insieme efficiente di misure preventive, la migliore prassi consiste nell'istituzione di un'autorità nazionale che abbia il potere di imporre misure specifiche per gli ATM ad alto rischio, sulla base di un'analisi approfondita della situazione. Questo approccio si è dimostrato efficace in Francia, soprattutto laddove venga stabilito un quadro giuridico e si attuino le misure preventive unitamente a quelle operative.

3. Attuare misure preventive

Le misure introdotte in questo capitolo per prevenire gli attacchi fisici agli ATM hanno dimostrato la loro utilità in diversi paesi. Esse si basano sulle conclusioni della conferenza sulla prevenzione e sulle misure preventive promosse attivamente dalle organizzazioni internazionali attive nel campo della sicurezza degli sportelli ATM. Molte misure sono ben note e diversi paesi le hanno già attuate con successo. Tuttavia, spesso i provvedimenti proposti sono eseguiti solo parzialmente e non sono inclusi nella legislazione.

Come già detto, vengono proposti tre assi di azioni preventive: ridurre le ricompense, aumentare il rischio per gli esecutori e intensificare lo sforzo necessario per accedere al bottino.

3.1 Ridurre le ricompense

La riduzione delle ricompense derivanti da atti criminali è il primo asse nella prevenzione degli attacchi fisici agli ATM. Finché persisterà la percezione del "denaro facile", i criminali saranno dediti a questo tipo di reato. Riducendo la quantità di denaro disponibile e rimuovendo o distruggendo il contante, le possibilità di procurarsi un bottino interessante diminuiscono. L'aspettativa di un bottino più esiguo riduce il desiderio del criminale di commettere questo tipo di reato.

Ridurre la quantità di contante

Una misura per ridurre le ricompense è quella di diminuire la quantità di contante disponibile in uno sportello ATM. Idealmente, tale quantità dovrebbe essere limitata all'importo necessario per un solo giorno di trading. La collaborazione tra banche potrebbe garantire l'efficacia dei costi. Nei Paesi Bassi, alcune banche hanno collaborato alla creazione di una rete di sportelli bancomat indipendenti dalle banche, denominata "Geldmaat". L'obiettivo della collaborazione è quello di garantire la disponibilità, l'accessibilità, l'economicità e la sicurezza del contante. Ciò porterà probabilmente a una riduzione del numero di sportelli automatici. Tuttavia, ogni bancomat non conterrà più contante, ma sarà rifornito più spesso. Il numero di rifornimenti sarà adattato alle esigenze.

Poiché i criminali assaltano per lo più gli sportelli automatici tra le 03.00 e le 04.00, si raccomanda vivamente ai gestori degli sportelli automatici autonomi (per lo più situati in locali commerciali e pubblici, che sono più vulnerabili) di svuotare il bancomat e di spostare il contante in una cassaforte a fine giornata. Un cartello di avvertimento può informare il pubblico che l'ATM non contiene contante durante le ore notturne. Il giorno successivo il bancomat dovrebbe essere rifornito lontano dalla vista dei clienti e con i locali chiusi a chiave. Questo sistema è stato attuato in Francia, dove la legislazione obbliga i rivenditori con un bancomat autonomo all'interno del proprio negozio a rimuovere il contante di notte e a lasciare aperto lo sportello ATM. Per gli altri sportelli automatici, le quantità conservate possono essere ridotte aumentando la frequenza di ricarica.

Rovinare il bottino e rendere tracciabile il denaro

I sistemi intelligenti di neutralizzazione delle banconote (IBNS) sono una prima tecnica per rovinare le ricompense. Questi sistemi macchiano le banconote con inchiostro per contrassegnarle come rubate. Inoltre, all'inchiostro di un IBNS possono essere aggiunti traccianti e marcatori. Attualmente questi marcatori sono utilizzati principalmente per scopi forensi, collegando la banconota alla scena del crimine e aumentando il rischio di essere scoperti. Anche se l'IBNS è una misura preventiva efficace, ci sono alcune considerazioni da fare.

La Banca centrale europea non rimborsa banconote macchiate[4] (dal 2003), ma alcune banche centrali nazionali degli Stati membri dell'UE ancora procedono

in tal senso e i biglietti macchiati vengono rimessi in circolazione nel sistema legale anche attraverso i casinò. Un IBNS crea dunque un ulteriore ostacolo per i criminali, ma sarebbe molto più efficace se per gli esecutori del reato fosse impossibile utilizzare banconote macchiate sul territorio dell'Unione europea. A tal fine, sarebbe opportuno che le banche centrali nazionali non accettassero questo tipo di biglietti. In determinate circostanze, possono essere fatte delle eccezioni come, ad esempio, nel caso di banconote macchiatesi durante una falsa attivazione. È inoltre importante consigliare alla popolazione di non accettare banconote macchiate. In una prospettiva più a lungo termine, si dovrebbero installare dispositivi di accettazione del contante in grado di rilevare eventuali biglietti macchiati all'interno di banche ed esercizi commerciali come casinò, autolavaggi, ecc. Il rilevamento dell'inchiostro è difficile e costoso, tuttavia una soluzione economica potrebbe essere quella di installare sistemi a infrarossi capaci di individuare le banconote macchiate con marcatori a infrarossi. Questi sistemi hanno dimostrato la loro efficacia e sono una buona pratica in Belgio e in Francia. Quando le banconote con i marcatori a infrarossi vengono introdotte nell'ATM, quest'ultimo accetta ("ingoia") il denaro ma non lo accredita su un conto. Inoltre, è necessario anche tenere traccia della persona che immette le banconote macchiate.

Riportiamo qui altre considerazioni inerenti all'installazione di soluzioni IBNS. Diversi produttori forniscono una serie di diverse soluzioni IBNS con svariati meccanismi di attivazione e vari tipi di inchiostro. Una prima considerazione riguarda il fatto che non tutti i tipi di tecnologie di attivazione IBNS sono in grdo di contrastare tutte le minacce. Alcuni IBNS sono particolarmente efficaci in caso di attacchi di sfondamento con auto-ariete, *in situ* e con gas, ma non funzionano in caso di rapine con esplosivi solidi o viceversa. Pertanto la tecnologia scelta deve essere ben considerata.

Un'altra considerazione attiene al tipo di inchiostro da scegliere. In Belgio vengono stabiliti dei requisiti minimi nazionali per l'IBNS (sicurezza, percentuale di superficie macchiata, non lavabilità, ecc.) e dei test indipendenti certificano che il sistema soddisfi gli standard nazionali e funzioni secondo quanto dichiarato dal produttore. È importante effettuare test su banconote vere perché sul mercato esistono inchiostri più economici che funzionano bene con i biglietti contraffatti/falsi ma non con quelli veri e che possono quindi essere rimossi da questi ultimi tramite lavaggio. Oltre a ciò, si raccomanda di aggiungere all'inchiostro un marcatore forense che consenta di stabilire un possibile collegamento tra le banconote macchiate e una data scena del crimine durante le indagini.

Le migliori pratiche dimostrano che l'IBNS può essere molto efficace soprattutto in combinazione con altre misure preventive. Nel 2015 la Francia ha introdotto una nuova legislazione comprendente articoli inerenti all'installazione di IBNS e all'uso di inchiostro con DNA unico. È la polizia militare francese (gendarmerie) che, sulla base di una valutazione del rischio, decide dove implementare sistemi IBNS e attuare altre misure. Poiché la nuova legislazione ha rafforzato l'approccio preventivo e operativo, il numero di attacchi è sceso da 300 nel 2013 a 50 nel 2018.

Un'altra tecnica atta a rovinare il bottino prevede l'uso della **colla**. L'efficacia della colla è stata dimostrata nei Paesi Bassi, ma al momento i costi di implementazione e di gestione risultano elevati. Inoltre, la colla può costituire un pericolo di incendio se il sistema non viene attivato prima di un attacco, poiché la dispersione di particelle di colla nell'aria potrebbe produrre una miscela combustibile. Questo metodo non è ancora pronto per il mercato, ma potrebbe costituire una soluzione per il futuro.

3.2 Aumentare il rischio

Un secondo asse per la prevenzione degli attacchi fisici agli ATM è quello di dissuadere i potenziali autori dal commettere reati aumentando il rischio di essere scoperti e puniti. Oltre al pericolo di lesioni fisiche in caso di uso di esplosivi per gli attacchi ai bancomat, il rischio principale per un criminale è rappresentato da una pena detentiva quando colto in flagranza di reato o a seguito di un'indagine. Pertanto, per ridurre ogni intento criminale, è necessario aumentare il rischio di essere scoperti e puniti. Per la società, catturare e condannare i criminali è, naturalmente, anche un metodo di prevenzione molto efficace qualora sia prevista una punizione successiva, come abbiamo visto in diversi paesi.

Condivisione delle informazioni

Il segreto per l'individuazione e la punizione degli aggressori degli ATM è costituito dalla condivisione di informazioni tra tutti i soggetti interessati nella lotta contro gli attacchi fisici agli sportelli automatici, compresi i fornitori di ATM, le autorità delle forze dell'ordine (polizia, procura ecc.), le autorità pubbliche, i produttori sia di

bancomat che di dispositivi di sicurezza e protezione, le associazioni professionali, i fornitori di ATM (banche e fornitori indipendenti), le società di sicurezza e le centrali di allarme. Idealmente, questo dovrebbe avvenire sia a livello nazionale che internazionale.

L'individuazione precoce di un imminente attacco fisico a un ATM è tuttavia difficile. Solo nei casi in cui lo scambio di informazioni a livello internazionale tra i partner delle forze dell'ordine e i partner privati (società di sicurezza e fornitori di distributori automatici di banconote) è pressoché perfetto, è possibile procedere a un'individuazione precoce. È necessario monitorare un'ampia gamma di indicatori, tra cui messaggi di allerta precoce tra le agenzie delle forze dell'ordine sui gruppi criminali organizzati in movimento, informazioni su veicoli ("caldi") utilizzati negli attacchi ai bancomat, informazioni provenienti da società di sicurezza o da servizi di vigilanza di quartiere sui comportamenti sospetti riscontrati nell'area circostante lo sportello automatico, transazioni sospette individuate dai fornitori di ATM e altri metodi di rilevamento. Altre possibili misure di polizia per un'individuazione precoce sono il monitoraggio delle auto rubate, dei produttori e dei distributori di esplosivi e delle aziende autorizzate all'uso di esplosivi. Poiché per un'individuazione precoce sono richiesti sforzi elevati che non danno alcuna garanzia di successo, gli interventi delle forze dell'ordine prima di un attacco sono rari.

Laddove non è possibile un rilevamento tempestivo dei reati, le centrali di allarme sono in grado di emettere rapidamente un avviso in caso di attacco fisico a un ATM. Per consentire l'intervento, devono essere concordate e predisposte normative e protocolli nazionali per una comunicazione rapida tra le centrali d'allarme e le forze dell'ordine. In caso di individuazione precoce o di informazioni in tempo reale, le forze dell'ordine dovranno sempre valutare le tempistiche e le migliori opportunità di intervento. Catturare i criminali in flagranza di reato è molto difficile e può sfociare in situazioni di pericolo perché alcuni gruppi criminali organizzati sono molto violenti e utilizzano armi pesanti.

Affinché un'indagine in seguito a un attacco fisico a un bancomat vada a buon fine, gli agenti delle forze dell'ordine devono comunicare con tutte le parti interessate, dato che ognuna di esse potrebbe disporre di informazioni in grado di contribuire al successo dell'indagine stessa. In tale contesto, naturalmente, sono necessarie la comunicazione e la collaborazione con le vittime principali, le banche o altri fornitori di sportelli bancomat in qualità di soggetti aventi accesso a dati importanti ai fini dell'indagine. Per il fornitore di ATM, le informazioni provenienti dalle forze dell'ordine concorreranno a migliorare le misure di prevenzione. Inoltre, anche i contatti con le associazioni professionali e i produttori si rivelano utili: spesso inviano messaggi di allerta per la sicurezza a cui possono iscriversi altri soggetti interessati. I produttori di ATM hanno una buona panoramica dei diversi tipi di attacchi agli sportelli automatici e dei relativi punti deboli e punti di forza delle misure preventive. Sono molto disponibili a fornire supporto alla polizia con informazioni sugli aspetti tecnici dei bancomat e sui MO utilizzati.

La cooperazione transfrontaliera è essenziale: i paesi dovrebbero condividere informazioni (su sospetti, aggressori di ATM condannati, MO, veicoli sospetti, immagini di attacchi, ecc.) non solo a sostegno delle indagini, ma anche perché i sospetti dichiarati colpevoli in un altro paese possono essere condannati per recidiva.

Infine, la creazione di un database a livello europeo, disponibile per le forze dell'ordine e contenente dati forensi (ad esempio, su diversi tipi di inchiostri di un IBNS, traccianti e marcatori o vetri di protezione degli ATM) potrebbe sostenere fortemente le indagini e collegare i sospetti a una data scena del crimine. La standardizzazione delle tecnologie a livello internazionale è spesso insufficiente: durante la conferenza del gennaio 2019, i partecipanti hanno affermato che la standardizzazione a livello europeo dell'inchiostro e delle etichette anticrimine potrebbe facilitare notevolmente le indagini.

TVCC e dispositivi di ascolto

Le immagini e i dati sonori provenienti dai sistemi di televisione a circuito chiuso e dai dispositivi di ascolto possono andare a sostegno sia dell'individuazione in tempo reale di un attacco (ad esempio per prevenire danni fisici ai primi soccorritori che giungono sulla scena del crimine) che delle successive indagini (ad esempio per identificare i colpevoli e il loro MO). Le immagini delle telecamere a circuito chiuso possono essere combinate con le immagini di sistemi di videosorveglianza pubblici e di altri sistemi nelle vicinanze dell'ATM e con le riprese di autovelox per fornire un quadro più completo dei colpevoli e del loro MO.

Tuttavia, le immagini dei sistemi TVCC sono spesso di scarsa qualità o vengono raramente conservate. Le immagini devono essere di qualità sufficiente per consentire l'identificazione di una persona. Anche in questo caso, la definizione di standard europei per le

telecamere di sicurezza a circuito chiuso faciliterebbe le indagini. Inoltre, poiché i criminali spesso disattivano le telecamere a circuito chiuso prima di un attacco, si potrebbe prendere in considerazione anche l'installazione di sistemi TVCC non visibili o di dispositivi di ascolto in tempo reale.

Punizione e riabilitazione degli autori dei reati

Una punizione coerente e severa dimostra di avere un effetto preventivo. Sebbene l'arresto di un gruppo criminale organizzato abbia un effetto immediato sul numero di attacchi agli ATM, la scarcerazione di chi assalta sportelli automatici comporta spesso anche una nuova ondata di rapine. In altri termini, la brevità delle sentenze fa sì che i colpevoli tornino in attività molto rapidamente. Le pene minime e massime per i criminali condannati per ogni tipo di attacco fisico a un ATM variano da uno Stato membro all'altro. Alcuni ritengono che sanzioni più elevate fungerebbero da deterrenti per i potenziali autori di reati. La ricerca scientifica[5], tuttavia, dimostra che un inasprimento delle pene non necessariamente comporta un maggiore effetto deterrente. Pertanto, potrebbe essere interessante esaminare i programmi di riabilitazione correttiva (e basata sull'autore del reato) per ridurre l'elevata recidiva.

3.3 Aumentare lo sforzo

Il terzo asse per prevenire gli attacchi fisici agli ATM comprende azioni che richiedono un maggiore sforzo per compiere l'atto criminale da parte dell'autore del reato.

Garantire un ambiente resistente al crimine

Se dalla valutazione del rischio (cfr. sopra) si evince che uno sportello ATM si trova in un ambiente ad alto rischio, il luogo deve essere smantellato e l'ATM trasferito in un'area a basso o medio rischio. Questo dovrà senz'altro avvenire nel caso in cui l'analisi dimostri che l'edificio potrebbe crollare se un bancomat fosse attaccato con l'uso di esplosivi. Potrebbe essere attuata una legislazione in materia per applicare tali misure nei casi ad alto rischio. Oltre a diminuire il numero di sportelli automatici in ambienti a rischio elevato, per ridurre la necessità dei bancomat, sarebbe opportuno incoraggiare i pagamenti senza contanti.

Laddove non è possibile trasferire il bancomat, occorre adottare il massimo numero di misure di sicurezza quali, ad esempio, l'uso di dissuasori antirapina, lampioni e altri arredi urbani per limitare l'accesso all'edificio, sistemi di arresto dei veicoli, l'installazione di un'illuminazione stradale adeguata, una maggiore sorveglianza palese o nascosta e dispositivi antifurto come un sistema di alterazione delle banconote. Quando viene attaccato un luogo non identificato come ad alto rischio, questo deve essere riconosciuto come tale ed è necessario aggiungere misure di sicurezza supplementari. Ai fini di un aggiornamento dello strumento di valutazione del rischio, bisognerebbe prendere in considerazione i nuovi fattori. La rivalutazione di questo rischio dovrebbe essere un'operazione ricorrente.

Rafforzare gli ATM

I produttori di ATM offrono una gamma standard di sportelli automatici dotati di una serie di caratteristiche di sicurezza classificate secondo i gradi di sicurezza del Comitato europeo di normalizzazione (CEN). Generalmente gli sportelli automatici presentano una marcatura CEN che va dal grado più basso, CEN1, a quello più alto, CEN4. Il grado è stabilito in funzione di caratteristiche come la robustezza del corpo del distributore e la resistenza agli attacchi. La resistenza ai gas è offerta per lo più come opzione (CEN-GAS). I modelli standard possono essere potenziati con ulteriori misure di protezione. Di solito, queste funzioni vengono installate da terzi per garantire la conformità alla legislazione locale e l'adeguamento del modello di base alle esigenze dei clienti locali. Le caratteristiche di sicurezza aggiuntive includono vari sensori per attivare un sistema di neutralizzazione del gas o un IBNS in caso di attacco *in situ* o di attacco con esplosivi e serrande potenziate e serrature di caveau per impedire l'accesso non autorizzato alla cassaforte nel caso in cui la saracinesca principale sia stata compromessa. Per gli ATM portatili e autonomi è importante utilizzare sistemi di ancoraggio che offrano una protezione supplementare contro gli attacchi di sfondamento con auto-ariete. È inoltre possibile includere dei sistemi di tracciamento nell'ATM a sostegno degli inquirenti quando il bancomat viene trasportato altrove prima dell'apertura.

Misure architettoniche

Durante l'installazione di uno sportello ATM, si consiglia di utilizzare macchine ad accesso posteriore. In questo caso l'esecutore del reato dovrà entrare nell'edificio e accedere al retro della macchina per rubare il denaro. I bancomat portatili e autonomi sono i più vulnerabili.

Pertanto una riduzione del numero di questo tipo di sportelli automatici aumenterebbe la sicurezza. L'obbligo di installare un ATM in un locale a prova di scasso ridurrebbe automaticamente l'uso degli sportelli automatici autonomi.

Sistema nebbiogeno

L'impiego di un sistema a cannone nebbiogeno consente di riempire rapidamente una stanza con una fitta nebbia, impedendo all'intruso di vedere. Questa nebbia di sicurezza rende spesso impossibile l'esecuzione dell'attacco all'ATM. Il sistema permette di rallentare quantomeno l'autore del reato, lasciando il tempo necessario per l'intervento delle forze dell'ordine. Il sistema di sicurezza nebbiogeno è collegato al sistema di allarme e può essere attivato in due modi: automaticamente, mediante sensori di allarme come rilevatori di movimento (di notte) o tramite sensori di manipolazione delle serrande degli ATM; oppure mediante una centrale di allarme per evitare troppi falsi allarmi. Per gli sportelli automatici da esterno, il sistema nebbiogeno può essere applicato sulla parte posteriore del bancomat in modo tale da riempire la stanza retrostante con la nebbia e azzerare la visibilità degli intrusi.

I sistemi nebbiogeni possono fornire la protezione di un determinato punto di uno sportello automatico situato in spazi aperti all'interno di stazioni di servizio, supermercati, ecc. In questo modo si evita che la nebbia riempia tutta l'area. Questo tipo di protezione si rivela più efficace quando la nebbia proviene da diversi angoli o quando riempie lo spazio dietro l'ATM nel caso

di uno sfondamento con auto-ariete. Attualmente sono in corso test per valutare se installare i cannoni nebbiogeni all'interno dell'ATM stesso, anziché nella stanza in cui si trova. Alla nebbia possono inoltre essere aggiunti marcatori del DNA che macchiano i rapinatori e i loro indumenti.

3.4 Misure parallele

Al fine di garantire un'attuazione efficiente ed efficace delle misure preventive di cui sopra, occorre prendere in considerazione una serie di provvedimenti paralleli. Queste misure sono indispensabili per consentire o rafforzare un approccio preventivo e operativo olistico volto ad affrontare gli attacchi fisici agli ATM.

Legislazione

In alcuni paesi la legislazione obbliga i fornitori di ATM ad adottare misure preventive; in altri l'istituzione di patti e accordi tra banche e forze dell'ordine garantisce un approccio ben gestito per affrontare gli attacchi fisici agli sportelli automatici. Le aree in cui possono essere prese in considerazione misure normative includono:

- l'incorporazione di misure preventive;
- quadri giuridici per consentire la collaborazione tra le forze dell'ordine e i partner pubblici e privati; e
- una rielaborazione delle sentenze qualora le pene imposte agli autori di attacchi fisici a sportelli ATM siano troppo basse.

Tuttavia, spesso sono solo gli istituti bancari a essere obbligati a rispettare tali misure e i fornitori di ATM indipendenti non sono vincolati da queste leggi o accordi. Si tratta di un punto debole comune sul piano di un quadro normativo.

Alcuni paesi non attuano alcuna regolamentazione, ma cercano di convincere i fornitori di sportelli automatici ad adottare misure preventive, sensibilizzandoli sui diversi settori criminali e sulle tendenze esistenti: nei paesi con un elevato numero di banche indipendenti questo si rivela però particolarmente difficile.

È imperativo garantire che l'effettiva attuazione delle misure preventive comprenda modifiche della legislazione e della regolamentazione sia a livello nazionale che internazionale che vincolino tutti i tipi di fornitori di ATM. Idealmente la legislazione dovrebbe essere allineata a livello UE per evitare che forti misure preventive integrate nella legislazione di un paese spingano i gruppi criminali organizzati verso altri paesi con una regolamentazione meno stringente.

Strategia mediatica

Un altro asse importante della strategia preventiva è costituito da una strategia mediatica consolidata mirante a ridurre le aspettative e il desiderio degli aggressori degli ATM a commettere questo reato. È opportuno sottolineare i bassi tassi di successo e gli elevati rischi per gli autori del reato, la comunicazione relativa alle ricompense ("bottino") o i dettagli sull'attacco ai danni dello sportello automatico, come il tipo di bancomat interessato o il MO evitato. D'altro canto, è necessaria un'ampia comunicazione incentrata sugli arresti dei

sospetti e sulle conseguenti punizioni in seguito a una condanna.

Collaborazione rafforzata

Sebbene si sia parlato molto dell'esigenza di una maggiore collaborazione e di uno scambio di informazioni, si tratta di un aspetto che non viene enfatizzato mai abbastanza. Del resto, lo scambio di informazioni operative a livello internazionale è l'attività principale di Europol. Oltre a questa trasmissione reciproca di dati, la conferenza sulla prevenzione ha mostrato la chiara necessità di aumentare la cooperazione e la condivisione di informazioni multidisciplinare e multilivello tra tutti i soggetti interessati, tra cui le forze dell'ordine, le autorità pubbliche, i produttori di ATM e di dispositivi di sicurezza e protezione, le associazioni professionali, i fornitori di ATM (banche e fornitori indipendenti), le società di sicurezza e le centrali di allarme. Ciò deve avvenire a livello locale, nazionale e internazionale.

Riduzione del rischio di danni collaterali

In caso di attacchi con esplosivi solidi, alcuni gruppi criminali organizzati si lasceranno dietro del materiale. Ciò può creare situazioni pericolose per i primi soccorritori o per i civili (che vivono nel quartiere o che sono di passaggio), motivo per cui deve essere garantita la loro sicurezza. Come avviene in Belgio, è necessario sviluppare e allineare fra loro i protocolli e le procedure che devono essere seguiti dai primi soccorritori (sia quelli delle forze dell'ordine che quelli dei fornitori di ATM). Un'altra buona pratica in questo contesto è l'esempio portato dai Paesi Bassi, dove per valutare la situazione si utilizzano i filmati delle telecamere a circuito chiuso relative all'attacco allo sportello ATM. È possibile stipulare accordi con le centrali di allarme per rendere immediatamente disponibili queste immagini.

Prevenzione sociale

Spesso i gruppi criminali organizzati cercano giovani da reclutare. Pertanto potrebbero essere creati dei progetti tesi a stroncare sul nascere questi processi di reclutamento. La polizia o gli assistenti sociali dovrebbero essere attenti a tali processi e potrebbero intervenire avvicinandosi personalmente ai potenziali esecutori dei reati.

04 CONCLUSIONI

Negli ultimi due anni, il numero di paesi europei interessati da attacchi fisici ai danni di sportelli ATM è aumentato. A questo proposito, Europol ed EUCPN hanno quindi deciso di collaborare per raccogliere le migliori misure volte a combattere e a prevenire tale reato.

Un approccio di successo per contrastare gli attacchi fisici agli ATM consiste in una combinazione di misure operative e preventive, preferibilmente integrate in un quadro legislativo. Per evitare che provvedimenti forti in un paese spingano i gruppi criminali organizzati a spostarsi verso paesi più vulnerabili, si raccomanda di adottare tali misure a livello europeo.

Al fine di prevenire e affrontare questo tipo di criminalità, occorre stabilire una chiara strategia articolata in tre fasi: valutazione della situazione, sviluppo di un approccio preventivo basato sulla valutazione del rischio e attuazione delle misure preventive.

La valutazione del rischio relativo agli attacchi fisici agli ATM dovrebbe includere le caratteristiche dello sportello automatico e dell'ambiente circostante, la cooperazione con i partner e i soggetti interessati per creare alleanze destinate a combattere questo reato e la valutazione del quadro preventivo e legale. Una volta valutata la situazione, sarebbe opportuno stabilire una strategia basata sulla collaborazione fra il settore pubblico e privato e su contromisure operative e preventive. L'obiettivo di queste ultime è quello di ridurre l'intento e le capacità del possibile autore di un attacco fisico a un bancomat. Per raggiungere tale obiettivo, vengono proposti tre assi di azioni preventive: ridurre i premi, accrescere il rischio e aumentare lo sforzo. La strategia di prevenzione dovrebbe inoltre essere completata dall'adozione di misure parallele. L'istituzione di un'autorità nazionale che abbia il potere di imporre queste misure necessarie è la migliore prassi da seguire.

Riducendo le ricompense si diminuisce il desiderio del criminale di commettere questo tipo di reato. Diminuire la quantità di contante disponibile negli sportelli automatici limitando il denaro rifornito a quello sufficiente per un solo giorno di trading o svuotare gli ATM (più vulnerabili) nelle ore notturne sono misure in grado di ridurre le aspettative del criminale. Un altro metodo è quello di rovinare il bottino e rendere il denaro tracciabile. In tale contesto è possibile applicare un sistema IBNS, che macchia le banconote contrassegnandole come rubate. Questo metodo si rivela più efficace quando è impossibile per i criminali spendere il denaro o rimettere in circolazione le banconote nel sistema legale. Ciò può essere realizzato dalle banche e dai cittadini non accettando biglietti macchiati per il pagamento e installando accettatori di banconote in grado di individuare e rifiutare tali biglietti. A questo proposito, l'investimento in sistemi a infrarossi che rilevano le banconote macchiate con marcatori a infrarossi si è dimostrato una soluzione economica in Belgio e in Francia. Durante la fase di installazione dell'IBNS, i paesi dovrebbero considerare attentamente i meccanismi di attivazione scelti, i requisiti minimi per la neutralizzazione delle banconote e l'aggiunta di un marcatore forense all'inchiostro.

Un secondo asse per la prevenzione degli attacchi fisici agli ATM è quello di dissuadere i potenziali autori dal commettere reati **aumentando il rischio** di essere scoperti e puniti. Il segreto per l'individuazione e la punizione degli aggressori degli sportelli automatici risiede nella raccolta di informazioni e nella condivisione di informazioni tra tutti i soggetti interessati, sia a livello

nazionale che internazionale. Lo scambio di informazioni di immagini TVCC di alta qualità e di dati sonori può aumentare le possibilità di individuazione precoce e il buon esito delle indagini. Per evitare che le telecamere a circuito chiuso o i dispositivi di ascolto siano disattivati prima dell'attacco, è possibile prendere in considerazione l'installazione di telecamere a circuito chiuso non visibili o di dispositivi di ascolto in tempo reale. La creazione di un database forense e la standardizzazione delle tecnologie a livello europeo potrebbe facilitare notevolmente la cooperazione internazionale e le indagini. Pertanto, potrebbe essere interessante esaminare i programmi di riabilitazione correttiva (e basata sull'autore del reato) per ridurre l'elevata recidiva.

Il terzo asse per prevenire gli attacchi fisici agli ATM comprende misure volte a **aumentare lo sforzo** necessario all'esecutore per compiere l'atto criminale. L'installazione di un ATM in un ambiente resistente alla criminalità dotato delle massime misure di sicurezza comporterà uno sforzo maggiore per qualsiasi criminale intenzionato ad assaltarlo. Inoltre, è possibile migliorare la protezione standard degli sportelli automatici tramite una serie di funzioni di sicurezza aggiuntive. Al di là di queste misure, l'installazione di un sistema nebbiogeno può fungere da deterrente per l'esecutore del reato o rallentare quantomeno l'attacco.

I suddetti provvedimenti potranno poi essere rafforzati mediante una serie di **misure parallele**, come la creazione di un quadro giuridico che obblighi tutti i fornitori di ATM ad attuare le misure preventive, lo sviluppo di una strategia mediatica consolidata, una maggiore collaborazione a livello locale, nazionale e internazionale, delle linee guida per i primi soccorritori al fine di ridurre al minimo il rischio di danni collaterali e l'investimento nella prevenzione sociale per sventare i processi di reclutamento di criminali.

RACCOMANDAZIONI PER UN APPROCCIO PREVENTIVO: PANORAMICA

Sviluppare una risposta efficace per prevenire gli attacchi fisici agli ATM

Valutare la situazione

> Definire il profilo di rischio degli ATM nel proprio paese/ nella propria regione.

> Individuare partner e soggetti interessati nella lotta contro gli attacchi fisici agli ATM e valutare la collaborazione.

> Valutare il quadro giuridico per affrontare gli attacchi fisici agli ATM a livello nazionale e internazionale.

Sviluppare un approccio preventivo

> Stabilire i (principali) rischi da coprire e le priorità.

> Stabilire le migliori misure preventive per coprire questi rischi considerando tre assi principali.

> Stabilire misure preventive parallele necessarie per rafforzare le misure preventive adottate.

Misure preventive che possono essere adottate per:

01

Ridurre le ricompense

> Ridurre la quantità di contante.
  - Svuotare l'ATM di notte.
  - Aumentare il numero/la frequenza dei rifornimenti.

> Rovinare il bottino.
  - Sistemi intelligenti di neutralizzazione delle banconote (IBNS).
  - Marcatori a infrarossi nell'inchiostro IBNS per rilevare i biglietti macchiati mediante accettatori di banconote.
  - In fase di sviluppo: colla.

02

Aumentare il rischio

> Condivisione transfrontaliera delle informazioni per:
  - l'individuazione precoce o in tempo reale di un possibile attacco a un ATM,
  - il rafforzamento dell'approccio operativo,
  - la condanna dei recidivi,
  - lo scambio di dati forensi a livello europeo.

> TVCC e dispositivi di ascolto.

> Punizione e riabilitazione degli autori dei reati.

03

Aumentare lo sforzo

> Garantire un ambiente resistente alla criminalità.
  - Cambiare l'ubicazione di ATM ad alto rischio.
  - Misure di sicurezza: ostacoli fisici, sorveglianza, ecc.

> Rafforzare i bancomat con serrande, materiali resistenti a gas o esplosivi solidi, ecc.

> Misure architettoniche come macchine ad accesso posteriore.

> Sistemi nebbiogeni di sicurezza.

Misure parallele per rafforzare l'approccio preventivo

> Legislazione efficace comprendente misure preventive contro gli attacchi fisici agli ATM, conseguenti sentenze, ecc.

> Strategia mediatica efficace per scoraggiare gli autori dei reati.

> Maggiore collaborazione tra tutti i soggetti interessati (pubblici, privati, forze dell'ordine) nella lotta contro gli attacchi fisici agli ATM.

> Riduzione del rischio di danni collaterali per i primi soccorritori o i civili (ad esempio residenti nel quartiere o di passaggio).

> Prevenzione sociale per evitare il reclutamento di giovani per questo tipo di reato.

ENDNOTES

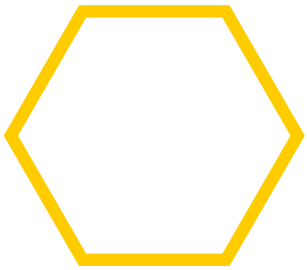
1 Willem Pieter de Groen, Zachary Kilhoffer and Roberto Musmeci, *The future of EU ATM markets: impacts of digitalisation and pricing policies on business models*, CEPS report, 2018

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), 41-96.

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

4 Decisione della Banca centrale europea relativa a tagli, specifiche, riproduzione, sostituzione e ritiro delle banconote in euro, 2003

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



CONTACT DETAILS

EUCPN Secretariat
Phone: +32 2 557 33 30
Email: eucpn@ibz.eu
Website: www.eucpn.org, www.europol.europa.eu

TWITTER.COM/EUCPN
FACEBOOK.COM/EUCPN
LINKEDIN.COM/COMPANY/EUCPN