Preventing physical ATM attacks

DEVELOPING AN EFFECTIVE APPROACH

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.

”

ACKNOWLEDGEMENTS

This document is the fruit of a collaboration between the European Union Agency for Law Enforcement Cooperation (Europol) and European Crime Prevention Network (EUCPN) secretariat. We would like to thank the experts in physical Automated Teller Machine (ATM) attacks who invested time and effort in supporting the creation of this recommendation paper. They contributed by attending the conference on the prevention of physical ATM attacks (January 2019, Brussels) and providing crucial information. In particular we would like to thanks law-enforcement agencies from EU and non-EU ('third') countries, the private sector including the ATM Industry Association (ATMIA), BPost, Centrum voor Criminaliteitspreventie en Veiligheid (CCV), Diebold Nixdorf, the European Association for Secure Transactions Expert Group on ATM and ATS Physical Attacks (EAST EGAP), European Intelligent Cash Protection Association (Euricpa), ING, Febelfin, NCR, Protect, SIOC Banking, Spinnaker, TMD Security and the ministries of interior of Belgium, Croatia, Germany and Spain.

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

CONTENTS

INTRODUCTION

With the number of physical automated teller machine (ATM) attacks and the number of European countries affected increasing, the European Crime Prevention Network (EUCPN) and Europol organised a conference (January 2019) bringing law enforcement together with public and private partners together to look at the prevention of this crime. This recommendation paper summarises the conclusions of this conference to raise authorities' awareness of physical ATM attacks and preventive measures. A limited, yet growing number of countries in the European Union have concerns with physical ATM attacks. In 2017 the financial loss caused was estimated to be over EUR 30 million in Europe. Some countries continue to witness a significant number of physical attacks on ATMs, others have experienced a significant increase in number of these incidents over the last 2 years. This crime area evolves quickly. Some countries were successful in their approach towards addressing physical ATM attacks and recently saw a significant decrease in attacks. On the other hand, countries previously unaffected were confronted with a sudden surge in physical ATM attacks in 2018 due to organised-crime groups (OCGs) expanding their territory. Not only banks are affected, increasingly ATMs from independent providers are attacked because they are often located in more vulnerable premises or locations.

The wide range of different modi operandi (MOs) criminals use to attack ATMs can be divided in two major categories: physical ATM attacks and ATM-related fraud attacks (this includes ATM-logical and malware attacks)[1]. This paper focuses on physical ATM attacks: the forced entry with physical means into ATMs in order to remove their cash. Forced entry can be accomplished by:

> **use of explosives:** attackers use gas or solid explosives to physically breach the ATM safe and gain access to the cash;

> **rip-out/ram-raid attacks:** attackers physically remove the ATM from the installation environment, often using a high-end vehicle;

> **in-situ attacks:** attackers cut through the safe by means of brute force, often using cutting or breaking tools such as angle grinders, sledgehammers, or oxyacetylene torches.

01 FACTORS DETERMINING THE SUCCESS OF A PHYSICAL ATM ATTACK

The success rate of ATM attacks is low; only one third of the attacks are successful. However, even when the attack is unsuccessful, the damage caused (e.g. by explosives) to building structures is equally important, leaving an unsafe environment in the vicinity of the crime scene for local residents, first responders and passers-by. The success of a physical attack depends on a number of factors including an ATM's characteristics, the set-up of an ATM attack and the experience and know-how of the perpetrators.

1. Vulnerability of ATMs

The most vulnerable are through the wall (TTW) ATMs which are situated outside or stand-alone ATMs which are mostly situated inside. ATMs situated inside and fixed in the wall are less vulnerable. When attacking an ATM inside, OCGs prefer ATMs situated in commercial premises over ATMs situated in bank premises where surveillance is typically stronger. Banks mainly operate ATMs located inside or outside a bank building. However, bank remote locations ('bank remote') in the street or in the commercial premises of merchants such as petrol stations, supermarkets, hotels, casinos, airports, etc. are gradually becoming more important with bank branches being closed. Besides banks, also independent providers operate ATMs as a self-standing service without offering other banking services. Their ATMs are often located in retail locations, hospitality and leisure locations, transport locations (railway stations, airports, etc.), public buildings and in the street.[2]

With the increasing popularity of online banking, many bank branches are likely to be closed in the coming years leading to an overall decrease in the number of ATMs.[3] However, this could entail an increase in the number of bank-remote ATMs and independent-provider ATMs located in more vulnerable locations.

2. Set-up of an ATM attack

The preparation of an attack can take up to several weeks or even months. Offenders need to collect the necessary tools and resources such as vehicles, equipment, establish the necessary contacts with persons supporting the crime and gather the necessary intelligence on the targets. Vehicles are an essential tool for physical ATM attacks; perpetrators mainly travel by car and after the attack they most often make their escape with fast vehicles. These are often stolen, but can also be hired or purchased (e.g. via the internet). Most of the equipment for physical ATM attacks is readily and legally available in normal shops. This further lowers the threshold for stepping into this crime area. Tracing the origin of a tool is difficult for law enforcement so the risks for the perpetrators are limited. OCGs active in physical ATM attacks at an international level nearly always have contact points in the target country. This is the case both for perpetrators who reside for a longer period in the country to prepare and execute the attack or for perpetrators who use a hit and run technique where they enter the country, execute the ATM attack and leave within hours. These contacts support the OCGs with logistics such as renting accommodation, procuring a vehicle or other equipment, and scouting targets. Some international perpetrators leave the logistics and scouting totally to the local contacts and just travel by road or by air for the execution of the ATM attack itself. OCGs often perform extensive scouting to identify suitable targets; assess the time of day the ATM is filled, the surroundings of the ATM, the technical specifics of the ATM, the escape routes and the security measures that are in place, such as closed-circuit television (CCTV), alarm sensors and shutters. Some OCGs take a number of actions to frustrate law enforcement and security services before the attack. They tamper with alarm systems and public lighting, use diversion techniques, set up road blocks or attempt to tamper with law enforcement vehicles.

3. The experience and know-how of the perpetrators

Physical ATM attacks are attractive for criminals because the money is immediately available and there is no need for an extensive network to sell stolen goods. It is a convenient alternative for criminals already active in organised property crime. OCGs need to gather the required expertise and know-how, as these are a determining factor in the success or failure of an attack. The required expertise and know-how needed depends strongly on the type of attack. Rip-out/ram-raid and in situ attacks have a simple MO (mainly audacity and the use of brute force), so they generally do not require specific skills. Gas attacks and attacks with solid explosives require a higher level of expertise. The attackers show different levels of competence. On the one hand, highly organised and experienced groups can execute a successful physical ATM attack within minutes. They are in control of the process and they are able to limit the risk to themselves thus also limiting the collateral damage. On the other hand, less organised and opportunistic groups often fail in their attempts and can cause significant damage to the premises and buildings in the neighbourhood. Some of the less-organised OCGs return to traditional organised property crime activities, discouraged by the preventive measures they are unable to overcome in attacking ATMs.

02 NEED FOR A PREVENTIVE APPROACH

Countries where perpetrators experience low success rates in physical ATM attacks or where the number of physical ATM attacks are decreasing illustrate that a successful approach for countering physical ATM attacks consists of a combination of operational and preventive measures. As the number of OCGs active in this crime area is limited, arrests and subsequent punishment of OCG-members significantly reduces the number of attacks. However, once released, many ATM attackers restart their activities. Moreover, a group can sometimes replace the arrested perpetrator quickly. Therefore there is a strong need for preventive measures, preferably embedded in a legislative framework. Furthermore, experience shows that prevention measures in one country can drive OCGs towards more vulnerable targets in other countries. 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.

03 PREVENTION

In order to prevent and tackle this type of crime, a clear strategy is needed. In this chapter we will give an overview of the three steps which are generally undertaken when confronted with physical ATM attacks or preparing to prevent them.

First of all the assessment of the situation; a risk profile of the ATMs and their surroundings should be established considering the amount of cash available (possible loot), the risk of collateral damage and the risk of personal injury. Secondly, based on the risk assessment a preventive strategy should be developed. Finally, the preventive measures should be implemented.

1. Assess the situation

OCGs tend to target either specific types of ATMs or ATMs of specific providers with features which facilitate the ATM attack. Therefore it is necessary to execute a thorough assessment of the risk of physical ATM attacks, preferably including the whole cash security chain from transit to delivery to storage in the ATM. To establish the risk profile of each ATM a number of elements should be analysed including the following:

- The characteristics of the site location and the surroundings of the ATM; features such as city or rural location, population density, proximity of police stations, automatic number plate recognition (ANPR) camera in the neighbourhood, CCTV in the vicinity etc.
- The location of the ATM:
  - inside or outside a building, in a bank branch or on a remote (e.g. commercial) premises, built-in or attached to a building,
  - for stand-alone ATM: whether it is anchored or not,
  - for ATMs built-in or attached to a building: whether there are architectural weaknesses, how is the cash storage organised etc.

- The type of ATM. The security functionalities included in the ATM.
- The amount of cash in the ATM. The type of physical ATM attacks and MO to expect in order to adopt the most appropriate preventive measures first.
- The security and preventive measures already taken (intelligent banknote neutralisation systems (IBNS), CCTV, security fog (visibility-reduction) system etc.).

Further elements to be evaluated are the state of cooperation with partners and stakeholders and the legislation. Collaboration between law enforcement, private and public partners should be evaluated to build alliances to combat crime. It is possible that each partner possesses interesting information to contribute to the assessment of the situation. Local police or local authorities are particularly important within that framework. The legislation has to be evaluated in terms of establishing a legal framework for prevention, taking mandatory preventive measures, sentencing for ATM attacks, etc.

2. Develop a preventive approach

Once the situation has been assessed and the main risk areas and the strength and weaknesses in the ATM security have been determined, a strategy can be developed (often build on public-private collaboration) and preventive and operational countermeasures can be put in place. Prevention measures should be aimed at lowering the intent and the capabilities of the perpetrators. In order to achieve this, three axes of preventive actions are proposed based on three out of five strategies of situational crime prevention by Clarke ; reducing the rewards, increasing the risk for the perpetrators and increasing the effort to access the loot.[4]

Criminals make a balance of the return to be expected and the risks associated with an ATM attack. Reducing the chances of getting to an easy reward and increasing the risk for the perpetrators lowers their expectations and their desire to engage in a physical ATM attack. Further measures which increase the effort needed to gain access to the ATM affect the capabilities of the perpetrators. Opportunistic perpetrators, often failing in their attempts, stop engaging in ATM attacks. For professional ATM attackers the success rate is reduced, again affecting the return/risk balance.

Furthermore, parallel measures such as an effective media strategy, early social prevention and measures to reduce the risk of collateral damage to buildings and to ensure the safety of local residents, first responders and passers-by completes the preventive strategy.

Other ways to structure the approach are possible. In the Netherlands, authorities apply the so-called barrier model.[5] This model identifies steps a criminal has to take to commit a crime. It also identifies the partners and the opportunities which enable the crime and it is a useful instrument by which to organise the information-gathering process on the crime area. By identifying each step necessary to execute a physical ATM attack, the barriers to obstruct the crime and the best partners to set up the barriers can be identified. The barrier model also identifies signals to alert the public and private partners on physical ATM attacks and signals they can send out themselves to notify the authorities about their suspicions.

A well-developed strategy is needed, also to mitigate risks which go along with strengthening prevention. Preventive measures which are very effective in discouraging the amateurs and copycats, sometimes have unwanted effects. Some groups turn to trial-and-error

methods to find vulnerable ATMs, leaving a trail of damaged ATMs. More dangerous and ruthless OCGs start using more violent MOs such as moving from gas to solid explosives in their attacks.

Reduced expectations lower the desire of the criminal to engage in this type of crime.

In order to set up an efficient set of preventive measures, the installation of a national authority that has the power to impose specific measures for high-risk ATMs, based on a thorough analysis of the situation, is best practice. This approach has been proven effective in France, especially if a legal framework is established and the measures are implemented together with operational measures.

3. Implement preventive measures

The measures introduced in this chapter to prevent physical ATM attacks have proven their usefulness in different countries. They are based on the conclusions of the prevention conference and on preventive measures actively promoted by international organisations active in ATM security. Many measures are well known. Several countries have already implemented a number of measures with success. However, often the proposed measures are only implemented partially and not embedded in legislation.

As mentioned above, three axes of preventive actions are proposed: reducing the rewards, increasing the risk for the perpetrators and increasing the effort required to access the loot.

3.1 Reduce the rewards

Reducing the rewards from criminal acts is the first axis in preventing physical ATM attacks. As long as the perception of 'easy money' persists, criminals will engage in this type of crime. Lowering the amount of cash available and either removing or destroying the cash, reduces the possibilities of there being interesting loot. Reduced expectations lower the desire of the criminal to engage in this type of crime.

Lowering the amount of cash

One measure to reduce the reward is by lowering the amount of cash available in an ATM. Ideally, this amount should be restricted to the necessary amount for one day of trading only. Collaboration between banks could ensure cost-effectiveness. In the Netherlands, a number of banks collaborated to establish a bank-independent network of ATMs, called 'Geldmaat'. The goal of the collaboration is to ensure availability, accessibility, affordability and security of cash. This will probably lead to a reduction in the number of ATMs. However, each ATM will not contain more cash, but will be replenished more often. The number of refills will be adapted to the need.

Since offenders mostly attack ATMs between 03.00 and 04.00, it is strongly recommended for stand-alone ATMs (mostly situated in commercial and public premises, which are more vulnerable), to empty the ATM and move the cash to a safe at the end of the day. A warning sign can inform the public that the ATM holds no cash at night. The next day the ATM should be replenished out of sight of customers and with the premises locked. This system is implemented in France where legislation obliges retailers with a stand-alone ATM in the shop to take the cash out at night and leave the ATM open. For other ATMs, the amounts held can be lowered by increasing the refill frequency.

Spoiling the loot and making the money traceable

Intelligent banknote neutralisation systems (IBNS) are a first technique for spoiling the rewards. These systems stain the banknotes with ink to mark them as stolen. Tracers and markers can be added to the IBNS-ink. At the moment these markers are mainly used for forensic purposes, linking the banknote to the crime scene and increasing the perpetrators' risk of being caught. Even though IBNS is an effective preventive measure, there are some considerations.

The European Central Bank does not reimburse stained banknotes[6] (since 2003) but a number of the national central banks of the EU Member States still do. Stained notes are also reintroduced into the legal system via banknote acceptors e.g. in casinos where stained notes are changed for coins and then back to clean notes. An

IBNS creates an extra obstacle for criminals but would be much more effective if it is impossible for criminals to use stained banknotes in the EU. To accomplish this, stained notes should not be accepted by the national central banks. Exceptions can be made for specific circumstances such as a notes stained during a false activation. It is also important to advise the population not to accept stained notes. On a more long-term perspective, banknote acceptors should detect stained notes, and should be installed in banks and in commercial premises such as casinos, car washes, etc. Detecting the ink is difficult and expensive, however a cost-effective solution could be to install infrared systems which detect notes stained with infrared markers. These systems have proved their effectiveness and are a best practice in Belgium and France. When notes with infrared markers are introduced into the ATM, the ATM will accept ('swallow') the money but not credit it to an account. The person introducing the stained banknotes should also be registered.

There are some other considerations when installing IBNS solutions. Several manufacturers provide a number of different IBNS solutions with different activation mechanisms and different types of ink. A first consideration concerns the fact that not all types of IBNS-activation technologies can counter all threats. Some IBNSs work very well for rip-out ram-raid attacks, in situ attacks and gas attacks but do not function in the event of a solid-explosive attack or vice versa. Therefore the technology chosen should be well considered.

Another consideration is the type of ink to choose. In Belgium the national minimum requirements for the IBNS (safety, percentage stained, not washable etc.) are set and independent tests certify that the system meets the national standards and operates according to the manufacturer's claims. It is important to test on real banknotes because there are cheaper inks on the market which work well with fake banknotes but not with real banknotes meaning that the ink can be removed from genuine banknotes by washing. In addition to this, it is recommended that a forensic marker be added to the ink, making it possible to investigate a link between stained banknotes and a specific crime scene.

Best practice shows that IBNS can be very effective especially in combination with other preventive measures. In 2015 France introduced new legislation including articles on the installation of IBNSs and the use of ink with unique DNA. It is the French Gendarmerie which, based on a risk assessment, decides where IBNS and other measures have to be implemented. Since the new legislation strengthened the preventive and operational approach, the number of attacks dropped from 300 in 2013 to 50 in 2018.

Another technique under development to spoil the loot is the use of glue. The effectiveness of glue was proved in the Netherlands, but implementation and running costs are high at the moment. Moreover, glue can be a fire hazard if the system is not activated before an attack since the dispersal of glue particles in the air could produce a combustible mixture. This method is not market ready yet but could be a solution for the future.

3.2 Increase the risk

A second axis for the prevention of physical ATM attacks is to deter potential perpetrators from committing crimes by increasing the risk of detection and punishment. Besides the risk of physical injury when using explosives for ATM attacks, the main risk for a criminal is a prison sentence when caught either in the act ('red-handed') or after an investigation. In order to lower the desire of the potential perpetrators, the risk of detection and punishment has to be increased. For society, catching and convicting the criminals is, of course, also a very effective prevention method if there is subsequent punishment, as we have seen in several countries.

Information sharing

Key in the detection and punishment of ATM attackers is information sharing between all stakeholders in the fight against physical ATM attacks, including ATM providers, law-enforcement authorities (police, prosecutor etc.), public authorities, the manufacturers both of ATMs and of security and protection devices, professional associations, ATM providers (banks and independent providers), security companies and alarm centres monitoring and responding to alerts. Ideally, this would be both at a national and international level.

Early detection of an upcoming physical ATM attack is difficult. Only in cases with almost flawless information exchange at international level between law-enforcement partners and private partners (security companies and ATM providers) is early detection possible. A wide range of indicators have to be monitored including early warning messages between law-enforcement agencies about OCGs on the move, information on ('hot') vehicles which were used in ATM attacks, information from security companies or neighbourhood watches on

suspicious behaviour detected within the area surrounding the ATM, suspicious transactions detected by ATM providers and other sensing methods. Other possible police measures for early detection are the monitoring of stolen cars, manufacturers and distributors of explosives and companies authorised to use explosives. The efforts necessary to achieve early detection are demanding and have no guarantee of success, therefore law-enforcement interventions before an attack are rare.

If early detection is not possible, alarm centres are able to issue a warning quickly in the event of a physical ATM attack. In order to enable intervention, national regulations and protocols for fast communication between alarm centres and law enforcement have to be agreed and set up. In the event of either early detection or of real-time information, law enforcement will always have to evaluate the timing and the best opportunity for intervention. Catching the criminals red-handed is very difficult and can lead to dangerous situations because some OCGs are very violent and use heavy weapons.

For the successful investigation of physical ATM attacks after an attack, law-enforcement officers have to communicate with all stakeholders, since any one of those could hold information contributing to the success of an investigation. Of course, communication and collaboration with the primary victims, the banks or other ATM providers is necessary: they have access to data which is important for the investigation. For the ATM provider, information from law enforcement will help to improve prevention measures. Furthermore, contacts with professional associations and manufacturers prove to be useful: they often send out security-alert messages to which other interested stakeholders can subscribe. ATM manufacturers have a good overview of the different types of ATM attacks and the corresponding weaknesses and strengths of preventive measures. They are very willing to give support to the police with information on the technical aspects of the ATMs and on the MOs used.

Cross-border cooperation is essential: countries should share information (on suspects, convicted ATM attackers, MOs, suspicious vehicles, images of attacks etc.), not only in support of the investigation but also because suspects convicted in another country can be sentenced for reoffending (recidivism).

Finally, the creation of a database at a European level, available to law enforcement and containing forensic data (e.g. on different types of IBNS inks, tracers and markers or ATM protection glass) could strongly support investigations and link suspects to a specific crime scene. Standardisation of technologies at an international level is often insufficient: during the January 2019 conference participants mentioned that EU-level standardisation of ink and crime tags could greatly facilitate investigations.

CCTV and listening devices

The image and sound data from CCTV systems and listening devices can increase real-time detection of an attack, prevent physical harm to first responders coming on the crime scene and support subsequent investigations. The CCTV images can be combined with images from public and other CCTV systems in the neighbourhood of the ATM and traffic radar footage to provide a more complete picture of the perpetrators and their MO. However, CCTV images are often of poor quality or poorly stored. The images should be of sufficient quality to enable the identification of a person. Again, setting European standards for security CCTV would facilitate investigations. Also, since perpetrators often disable CCTV cameras before an attack, the installation of non-visible CCTV or of real-time listening devices could also be considered.

Punishment and offender rehabilitation

Consistent and severe punishment proves to have a preventive effect. The arrest of an OCG has an immediate effect on the number of ATM attacks. However, the release from prison from ATM attackers also often leads to a new surge of attacks. This means that short sentences lead to perpetrators being active again very quickly. The minimum and maximum penalties for criminals convicted for each type of physical ATM attack varies among Member States. Scientific research shows that increasing the severity of sentences does not necessarily enhance the deterrent effect.[7] Therefore it might be interesting to look into correctional (and offender-based) rehabilitation programmes in order to reduce the high recidivism.

3.3 Increase the effort

The third axis to prevent physical ATM attacks contains actions that make it more demanding for an offender to carry out the criminal act.

Ensuring a crime-resistant environment

If the risk assessment shows that an ATM is situated in a high-risk environment, the location should be dismantled and the ATM transferred to a low- or medium-risk area. This is certainly the case if the analysis demonstrates that the building could collapse if an ATM is attacked by use of explosives. Legislation could be implemented to enforce such measures in high-risk cases. Aside from reducing the number of ATMs in high-risk environments, cashless payments should be encouraged to reduce the need for ATMs. If it is not possible to transfer the ATM, a maximum of security measures should be taken: e.g. the use of anti-ram-raid bollards, lampposts and other street furniture to restrict access to the building, the installation of adequate street lighting, increased overt or covert surveillance and anti-theft devices such as IBNS. When a location is attacked at a location that was not identified as high risk, it should be identified as such and extra security measures added. The new factors should be taken into account in the risk-assessment tool in order to update it. The reassessment of this risk should be a recurring operation.

Ideally legislation should be aligned at EU level to avoid that strong preventive measures embedded in legislation in one country drive the OCGs to other countries with less strict regulation.

Reinforcing the ATMs

ATM manufacturers offer a standard range of ATMs which have a number of safety features which are rated according to the European Committee for Standardisation (CEN) grades of security. Generally ATMs have a CEN-marking ranging from the lower grade CEN1 to the highest, CEN4. Features such as body strength and resistance to attacks determine the grade. Gas resistance is mostly offered as an option (CEN-GAS). The standard models can be enhanced with additional protection measures. Usually third parties are installing these features to ensure compliance with local legislation and adjustment of the basic model to the requirements of local customers. Extra security features include various sensors to activate a gas-neutralisation system or IBNS in the event of an in situ or attack with explosives and enhanced shutters and vault locks to prevent unauthorised access to the safe where the main shutter is compromised. For portable, stand-alone ATMs, it is important to use anchoring systems which offer extra protection against rip-out/ram-raid attacks. Tracking systems can be included in the ATM to support investigators when the ATM is transported to another location before opening.

Architectural measures

When installing an ATM, it is suggested to use rear access machines. In this case the perpetrator has to enter the building and gain access to the rear of the machine to steal the cash. Portable, stand-alone ATMs are the most vulnerable. A reduction of the number of these ATMS would increase security. The obligation to install ATMs in a crime-resistant room would automatically decrease the use of stand-alone ATMs.

Fog system

A fog cannon quickly fills a room with a dense fog, so the intruder cannot see anything. This security fog often makes it impossible to execute the ATM attack. At the very least, the system slows the perpetrator down leaving time for police services to intervene. The security fog system is connected to the alarm system and can be activated in two ways. It can be triggered automatically by alarm sensors such as motion detectors (at night) or ATM-shutter-manipulation sensors. It can also be activated by an alarm centre in order to avoid too many false alarms. For through-the-wall outdoor ATMs, the fog system can be applied at the back of the ATM to fill the room behind with fog and reduce the perpetrators' visibility to zero. Fog systems can provide point protection of an ATM located in open spaces in petrol stations, supermarkets, etc. This avoids the fog filling the whole area. The fog protection is most successful when the fog is coming from different angles or when it fills the space behind the ATM in the case of a ram-raid. Tests are ongoing to see whether fog cannons can be installed within the ATM itself, instead of in the room where the ATM is located. DNA markers which stain the perpetrators and their clothes can be added to the fog.

3.4 Parallel measures

In order to ensure the efficient and effective implementation of the preventive measures mentioned above, a number of parallel measures have to be considered. These measures are indispensable to enable or strengthen a holistic preventive and operational approach to address physical ATM attacks.

Legislation

In a number of countries legislation obliges ATM providers to take preventive measures. In other countries the establishment of agreements between banks and law-enforcement agencies ensure a well-run approach to address physical ATM attacks. Areas where regulatory measures can be considered include:

- embedding of preventive measures in legislation;
- legal frameworks to allow collaboration between law enforcement and public and private partners;
- a reworking of sentencing if the penalties for the perpetrators of physical ATM attacks are too low.

However, often it is only banking institutions that are obliged to comply and independent ATM providers are not bound by these laws or agreements. This is a common weak point in a regulatory framework.

Some countries do not implement any regulation but try to persuade ATM providers to take preventive measures by raising their awareness of the crime area and the trends. In countries with a high number of independent banks this proves to be particularly difficult. It is imperative to ensure that the effective implementation of the preventive measures includes changes in legislation and regulation both at national and international level binding all types of ATM providers. Ideally legislation should be aligned at EU level to avoid that strong preventive measures embedded in legislation in one country drive the OCGs to other countries with less strict regulation.

Media strategy

Another important axis in the preventive strategy is a well-established media strategy which is aimed at decreasing the expectations and the desire of the ATM attackers to engage in this crime. Low success rates and the high risks for the perpetrators have to be stressed; communication about rewards ('loot') or details about the ATM attack such as type of ATM affected or MO avoided. On the other hand, extensive communication on the arrests of suspects and subsequent punishment after a conviction is necessary.

Enhanced collaboration

Enhanced collaboration and information exchange have been mentioned extensively but cannot be stressed enough. Operational information exchange at the international level is the core business of Europol. Besides this information exchange, the prevention conference showed the clear need for increasing multidisciplinary and multilevel cooperation and information sharing between all relevant stakeholders including law-enforcement agencies, public authorities, manufacturers of ATMs and security and protection devices, professional associations, ATM providers (banks and independent providers), security companies and alarm centres. This has to include the local, national and international level.

Reducing risk of collateral damage

In the event of attacks with solid explosives, some OCGs will leave material behind. This can create dangerous situations for first responders or civilians (either living in the neighbourhood or passing by). Their safety has to be ensured. As is the case in Belgium, protocols and procedures to be followed by first responders from law enforcement and from the ATM providers have to be developed and aligned with each other. Another best practice in that context is the example of the Netherlands, where usage of CCTV footage from the ATM attack is used to assess the situation. Agreements with alarm centres can be established in order to make these images immediately available.

Social prevention

Often OCGs look for young persons to recruit. Projects could be set up to frustrate these recruitment processes in an early stage. Police or social workers should be attentive for these processes and could intervene by personally approaching the potential perpetrators.

04 CONCLUSIONS

Over the last 2 years the number of European countries affected by physical ATM attacks increased. In this regard, Europol and the EUCPN worked together to gather the best measures to combat and prevent this crime.

A successful approach for countering physical ATM attacks consists of a combination of operational and preventive measures, preferably embedded in a legislative framework. In order to avoid that strong measures in one country drive OCGs towards more vulnerable countries, it is recommended to adopt these measures at European level.

To prevent and tackle this type of crime a clear strategy should be established in three steps: the assessment of the situation, the development of a preventive approach based on the risk assessment and the implementation of the preventive measures.

The risk assessment for physical ATM attacks should include the characteristics of the ATM and its surroundings, the cooperation with partners and stakeholders to build alliances to combat this crime and the evaluation of the preventive and legal framework. Once the situation has been assessed a strategy built on public-private collaboration and preventive and operational countermeasures should be established.
The aim of the preventive measures is to lower the intent and the capabilities of the perpetrator to engage in a physical ATM attack. In order to achieve this, three axes of preventive actions are proposed: reduce the rewards, increase the risk and increase the effort. Parallel measures should complete the preventive strategy. The installation of a national authority that has the power to impose these necessary measures is best practice.

By **reducing the rewards**, the desire of the criminal to engage in this type of crime decreases. Lowering the amount of cash in ATM by limiting the replenished cash to that sufficient for 1 day of trading only, or emptying the (most vulnerable) ATMs at night is one measure to reduce the expectations of the criminal. Another method is to spoil the loot and make the money traceable. In this context IBNS, which stains the notes and marks them as stolen, can be applied. This method is most effective when it is impossible for criminals to spend this money or to reintroduce these notes into the legal cash system. This can be achieved by banks and the public not accepting stained notes for payment and by installing banknote acceptors that can detect and refuse stained notes or that accept but do not credit the stained notes. In this regard, the investment in infrared systems which detect stained notes with infrared markers has proven to be a cost-effective solution in Belgium and France. When installing IBNS, countries should thoroughly consider the chosen activation mechanisms, the minimum requirements for the staining of the banknotes and the adding of a forensic marker to the ink.

The aim of the preventive measures is to lower the intent and the capabilities of the perpetrator to engage in a physical ATM attack.

Measures which deter potential perpetrators from committing crimes by

increasing the risk of detection and punishment, are the second axis to prevent physical ATM attacks. Key in the detection and punishment of ATM attackers is information gathering and sharing between all stakeholders, both at national and international level.

Information exchange of high-quality CCTV images and sound data can increase the chances of early detection and successful investigation. To avoid that CCTV or listening devices are disabled before the attack, the installation of non-visible CCTV or real-time listening devices can be considered. The creation of a forensic database and the standardisation of technologies at European level could greatly facilitate international co-operation and investigations. If offenders are caught and convicted it might be interesting to look into correctional (and offender-based) rehabilitation programmes to reduce the high recidivism.

The third axis to prevent physical ATM attacks includes measures **to increase the effort** needed by an offender to carry out the criminal act. The installation of an ATM in a crime-resistant environment with a maximum of security measures will make it more demanding for offenders to attack an ATM. Furthermore, the standard ATM protection can be enhanced with a number of additional security features. On top of these measures, the installation of a fog system can deter the perpetrator or at least slow the attack down.

A number of **parallel measures** will strengthen the abovementioned measures such as creating a legal framework which obliges all ATM providers to implement the preventive measures, developing a well-established media strategy, the enhanced collaboration at local, national and international level, guidelines for first responders in order to reduce to risk of collateral damage and the investment in social prevention to undermine the criminal-recruitment processes.

Factsheet

RECOMMENDATIONS FOR A PREVENTATIVE APPROACH: OVERVIEW

Develop an effective answer to prevent physical ATM attacks

Assess the situation

> Establish the risk profile of ATM's in your country/region

> Identify partners and stake-holders in the fight against physical ATM attacks and evaluate the collaboration

> Evaluate the legal framework for tackling physical ATM attacks on national and international level

Develop a preventative approach

> Determine the (main) risks and priorities

> Determine the best preventative measures to cover these risks by considering the three main axes

> Determine parallel measures needed to strengthen the preventative measures taken

Preventive measures which can be taken to:

01

Reduce the awards

> Lower the amount of cash
  - Empty the ATM at night
  - Increase the number of replenishments
> Spoil the loot
  - Intelligent Banknote Neutralisation System (IBNS)
> Infrared markers in IBNS ink to detect stained notes by bank note acceptors
> Under development: glue

02

Increase the risk

> Cross border information sharing in view of:
  - Early or real time detection of a possible ATM attack
  - Strenghtening of the operational approach
  - Conviction of recidivism
  - Exchange of forensic data on European level
> CCTV and listening devices
> Consequential punishment and offender rehabilitation

03

Increase the effort

> Ensuring a crime resistant environment
  - Changing location of high risk ATM's
  - Security measures: physical obstacles, surveillance, ...
> Reinforcing ATM's with shutters, resistant to gas or solid explosives, ...
> Architectural measures such as rear access machines
> Fog system

Parallel measures to strenghten the preventive approach

> Effective legislation including preventive measures against physical ATM attacks, consequential sentencing, etc.

> Effective media strategy discouraging perpetrators.

> Enhanced collaboration between all stakeholders (public, private, law enforcement) in the fight against physical ATM attacks.

> Reduce risk of collateral damage to first responders or civilians living in the neighbourhood or passingby.

> Social prevention avoiding youngsters to be recruited for (this type of) crime.

ENDNOTES

1 Trend Micro and Europol (2017), *Cashing in on ATM Malware*

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

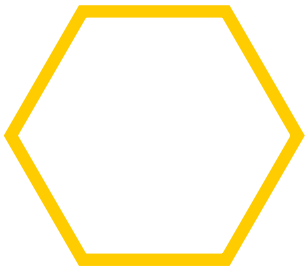
3 Ibidem

4 Derek Cornish and Ronald V.Clarke, (2003 p. 41-96), *Opportunities, precipitators and criminal decisions: a reply to Wortley's critique of situational crime prevention*, Crime prevention Studies 16

5 Centrum voor Criminaliteitspreventie, *Barrieremodellen*, available on www.barrieremodellen.nl

6 European Central Bank (2013), 2013/ 211/ EU: *European Central Bank decision of the European Central Bank, The denominations, specifications, reproduction, exchange and withdrawal of euro banknotes*

7 David Weisburd, David P. Farrington and Charlotte Gill (2016), *Conclusion: What Works in Crime Prevention Revisited*. David Weisburd, David P. Farrington and Charlotte Gill (2016, p. 311), *What works in Crime Prevention and Rehabilitation*



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