Prévention des attaques physiques contre les distributeurs automatiques de billets

Développer une approche efficace

Remerciements
Le présent document est le fruit d'une collaboration entre l'Agence de l'Union européenne pour la Coopération policière (EUROPOL) et le Secrétariat du Réseau européen de prévention de la criminalité (REPC). Nous tenons à remercier les experts en attaques physiques de guichets automatiques bancaires (GAB) qui ont investi du temps et des efforts pour faciliter l'élaboration de ce document de recommandations. Ils y ont contribué en participant à la conférence sur la prévention des attaques physiques contre les distributeurs automatiques de billets (janvier 2019, Bruxelles) et en fournissant des informations cruciales. Nous tenons tout particulièrement à remercier les services répressifs des pays de l'UE et des pays tiers (« tiers »), le secteur privé, notamment l'ATM Industry Association (ATMIA), BPost, le Centrum voor Criminaliteitspreventie en Veiligheid (CCV), Diebold Nixdorf, le groupe d'experts de l'Association européenne pour les transactions sécurisées sur les attaques physiques contre les distributeurs automatiques de billets et les guichets automatiques (EAST EGAP), l'Association européenne pour la protection intelligente des espèces (Euricpa), ING, Febelfin, NCR, Protect, SIOC Banking, Spinnaker, TMD Security et les ministères de l'Intérieur de Belgique, de Croatie, d'Allemagne et d'Espagne.

Mentions légales
Le contenu de cette publication ne reflète pas nécessairement l'opinion officielle d'un État membre de l'UE ou d'une agence ou institution de l'UE ou des Communautés européennes.

Sommaire

1 Contexte 4
2 Facteurs déterminant le succès d'une attaque physique contre des distributeurs automatiques de billets 5
2.1 Vulnérabilité des distributeurs automatiques de billets 5
2.2 Mise en place d'une attaque de distributeurs automatiques de billets 7
2.3 L'expérience et le savoir-faire des auteurs 7
3 Nécessité d'une approche préventive 9
4 Prévention 10
4.1 Évaluer la situation 10
4.2 Développer une approche préventive 11
4.3 Mettre en œuvre des mesures préventives 13
4.3.1 Réduire les gains 13
4.3.2 Augmenter le risque 16
4.3.3 Intensifier les efforts 19
4.3.4 Mesures parallèles 21
5 Conclusions 24
6 Recommandations pour une approche préventive : vue d'ensemble 26

1 Contexte

Le nombre d'attaques physiques de distributeurs automatiques de billets (DAB) et le nombre de pays européens touchés étant en augmentation, le Réseau européen de prévention de la criminalité (REPC) et Europol ont organisé une conférence (janvier 2019) réunissant les services répressifs et des partenaires publics et privés pour examiner la prévention de cette criminalité. Ce document de recommandations résume les conclusions de cette conférence afin de sensibiliser les autorités aux attaques physiques contre les distributeurs automatiques de billets et aux mesures préventives.

Le large éventail de méthodes différentes (*modi operandi* (MO)) que les criminels utilisent pour attaquer les distributeurs de billets peut être divisé en deux grandes catégories : les attaques physiques des distributeurs de billets et les attaques via la fraude liée aux distributeurs de billets (cela comprend les attaques logiques des distributeurs de billets et les attaques de logiciels malveillants). Ce document se concentre sur les attaques physiques des distributeurs automatiques de billets : l'entrée forcée avec des moyens physiques dans les distributeurs afin de retirer leur argent. L'entrée forcée peut se faire par :

- l'utilisation d'explosifs : les attaquants utilisent du gaz ou des explosifs solides pour percer physiquement le coffre-fort du distributeur automatique et accéder à l'argent ;
- les attaques par arrachage ou bélier : les attaquants retirent physiquement le distributeur automatique de billets de l'environnement d'installation, souvent à l'aide d'un véhicule haut de gamme ;
- les attaques in situ : les attaquants percent le coffre-fort par la force brute, souvent à l'aide d'outils coupants ou brisants tels que des meuleuses d'angle, des marteaux de forgeron ou des torches à oxyacétylène.

Un nombre limité, mais croissant, de pays de l'Union européenne sont préoccupés par les attaques physiques contre les distributeurs automatiques de billets. En 2017, le préjudice financier causé a été estimé à plus de 30 millions d'euros en Europe. Certains pays continuent d'assister à un nombre important d'attaques physiques contre les distributeurs automatiques de billets, d'autres ont connu une augmentation significative du nombre de ces incidents au cours des deux dernières années. Ce domaine de la criminalité évolue rapidement. Certains pays ont enregistré des succès dans leur approche de la lutte contre les attaques physiques contre les distributeurs automatiques de billets et ont récemment constaté une diminution significative des attaques. D'autre part, les pays qui n'étaient pas touchés auparavant ont été confrontés à une augmentation soudaine des attaques physiques contre les distributeurs automatiques de billets en 2018, en raison de l'expansion des groupes criminels organisés (GCO) sur leur territoire. Les banques ne sont pas les seules touchées, mais également, et chaque jour davantage, les distributeurs automatiques de fournisseurs indépendants, car ils se situent souvent dans des locaux ou des lieux plus vulnérables.

2 Facteurs déterminant le succès d'une attaque physique contre des distributeurs automatiques de billets

Le taux de réussite des attaques de distributeurs automatiques de billets est faible ; seul un tiers des attaques sont réussies. Toutefois, même lorsque l'attaque échoue, les dommages causés (par exemple, par des explosifs) aux structures des bâtiments sont tout aussi importants, laissant un environnement dangereux à proximité de la scène du crime pour les résidents locaux, les premiers intervenants et les passants.

Le succès d'une attaque physique dépend d'un certain nombre de facteurs, dont les caractéristiques d'un distributeur automatique de billets, la mise en place d'une attaque de distributeur automatique de billets et l'expérience et le savoir-faire des auteurs.

2.1 Vulnérabilité des distributeurs automatiques de billets

Les distributeurs les plus vulnérables sont ceux situés à l'extérieur (dans le mur (TTW)) ou ceux qui se trouvent à l'intérieur des bâtiments. Lorsqu'ils s'attaquent à un guichet automatique intérieur (isolé), les GCO préfèrent les guichets automatiques situés dans des locaux commerciaux aux guichets automatiques situés dans des locaux bancaires où la surveillance est généralement renforcée. Les banques exploitent principalement des distributeurs automatiques de billets situés à l'intérieur ou à l'extérieur d'un bâtiment bancaire. Les emplacements éloignés des banques (« banque à distance ») dans la rue ou dans les locaux commerciaux des commerçants tels que les stations d'essence, les supermarchés, les hôtels, les casinos, les aéroports, etc. sont de plus en plus nombreux en raison de la fermeture des agences bancaires. Des prestataires indépendants exploitent les DAB comme un service autonome. Leurs guichets automatiques se situent souvent dans des commerces de détail, des lieux d'accueil et de loisirs, des lieux de transport (gares, aéroports, etc.), des bâtiments publics et dans la rue.

Avec la popularité croissante de la banque en ligne, de nombreuses agences bancaires devraient fermer leurs portes dans les années à venir, ce qui entraînera une diminution globale du nombre de distributeurs automatiques de billets. ([1]) Toutefois, cela pourrait entraîner une augmentation du

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

nombre de distributeurs automatiques de billets à distance des banques et des fournisseurs indépendants situés dans des endroits plus vulnérables.

2.2 Mise en place d'une attaque de distributeurs automatiques de billets

La préparation d'une attaque peut prendre plusieurs semaines, voire plusieurs mois. Les auteurs doivent rassembler les **outils et les ressources** nécessaires, tels que les véhicules, les équipements et les points de contact. Les **véhicules** sont un outil essentiel pour les attaques physiques de distributeurs automatiques de billets ; les auteurs se déplacent principalement en voiture et après l'attaque, ils s'enfuient le plus souvent avec des véhicules rapides. Ces derniers sont souvent volés, mais peuvent également être loués ou achetés (par exemple, via l'Internet). La plupart des **équipements** pour les attaques physiques de distributeurs automatiques de billets sont facilement et légalement disponibles dans les magasins normaux. Cela abaisse encore le seuil d'entrée dans ce domaine de la criminalité. La recherche de l'origine d'un outil est difficile pour les services répressifs, de telle sorte que les risques pour les auteurs sont limités. Les GCO actifs dans les attaques physiques de distributeurs automatiques de billets au niveau international ont presque toujours des points de contact dans le pays cible (personnes qui y résident pendant une certaine période) ou ils peuvent utiliser une technique d'attaque éclair. Ces contacts aident les GCO dans la logistique, comme la location de logements, l'achat d'un véhicule ou d'autres équipements, et le repérage des cibles. Certains auteurs internationaux confient totalement la logistique et le repérage aux contacts locaux et se contentent de voyager par route ou par avion pour l'exécution de l'attaque des distributeurs automatiques.

Les GCO effectuent souvent des **recherches** approfondies pour identifier les cibles appropriées ; ils évaluent le moment de la journée où le guichet automatique est rempli, les environs du guichet, les spécificités techniques du guichet, les voies de fuite et les mesures de sécurité mises en place, telles que la vidéosurveillance (CCTV), les capteurs d'alarme et les volets.

Certains GCO prennent un certain nombre de mesures pour **contrer les services de police et de sécurité** avant l'attaque. Ils trafiquent les systèmes d'alarme et l'éclairage public, utilisent des techniques de diversion, mettent en place des barrages routiers ou tentent de trafiquer les véhicules des forces de l'ordre.

2.3 L'expérience et le savoir-faire des auteurs

Les attaques physiques de distributeurs automatiques sont intéressantes pour les criminels car l'argent est immédiatement disponible et il n'est pas nécessaire de disposer d'un réseau étendu pour vendre des biens volés. C'est une alternative pratique pour les criminels déjà actifs dans la criminalité organisée de propriété.

Les GCO doivent réunir **l'expertise et le savoir-faire nécessaires**, car ils constituent un facteur déterminant dans la réussite ou l'échec d'une attaque. L'expertise et le savoir-faire nécessaires dépendent fortement du **type d'attaque**. Les attaques bélier et les attaques *in situ* affichent un mode opératoire simple (principalement l'audace et l'utilisation de la force brute), et ne nécessitent donc généralement pas de compétences spécifiques. Les attaques au gaz combustible et les attaques aux explosifs solides nécessitent un niveau d'expertise plus élevé.

Les auteurs possèdent différents **niveaux de compétence**. D'une part, des groupes très organisés et expérimentés peuvent exécuter une attaque physique réussie contre les distributeurs automatiques de billets en quelques minutes. Ils contrôlent le processus et sont en mesure de limiter le risque qu'ils courent, limitant ainsi les dommages collatéraux. D'autre part, les groupes moins organisés et opportunistes échouent souvent dans leurs tentatives et peuvent causer des dommages importants aux locaux et aux bâtiments du voisinage. On pense que certains des GCO les moins organisés reviennent à des activités traditionnelles de criminalité organisée contre les biens, découragés par les mesures préventives qu'ils ne parviennent pas à surmonter lorsqu'ils s'attaquent aux distributeurs automatiques de billets.

3 Nécessité d'une approche préventive

Les pays où les auteurs d'attaques physiques contre les distributeurs automatiques connaissent un faible taux de réussite ou où le nombre d'attaques physiques contre les distributeurs automatiques est en baisse, démontrent qu'une approche efficace pour contrer les attaques physiques contre les distributeurs automatiques consiste en une combinaison de mesures opérationnelles et préventives. Comme le nombre de GCO actifs dans ce domaine est limité, les arrestations et les sanctions consécutives infligées aux membres du GCO réduisent considérablement le nombre d'attaques. Cependant, une fois libérés, de nombreux auteurs d'attaques contre les distributeurs automatiques de billets reprennent leurs activités. De plus, un groupe peut parfois remplacer rapidement l'auteur arrêté. Dès lors, le besoin de mesures préventives s'impose, qui doivent, de préférence, être intégrées dans un cadre législatif. En outre, l'expérience montre que les mesures de prévention prises dans un pays peuvent inciter les GCO à se tourner vers des cibles plus vulnérables dans d'autres pays. Ce n'est qu'une question de temps avant que les modes opératoires qui apparaissent dans un pays ne s'étendent à d'autres pays. Cela indique clairement **la nécessité d'adopter des mesures préventives et opérationnelles au niveau européen**, avec les partenaires privés, publics et répressifs travaillant en étroite collaboration.

4 Prévention

Pour prévenir et combattre ce type de criminalité, une stratégie claire est nécessaire. Dans ce chapitre, nous fournirons un aperçu des trois étapes généralement mises en œuvre quand on est confronté à des attaques physiques de distributeurs automatiques de billets ou quand on travaille à leur prévention.

Tout d'abord, **l'évaluation de la situation** ; un profil de risque des distributeurs automatiques et de leurs environs doit être établi en tenant compte du montant d'argent disponible (éventuel butin), du risque de dommages collatéraux et du risque de blessures corporelles. Deuxièmement, une **stratégie préventive** doit être élaborée sur la base de l'évaluation des risques. Enfin, les **mesures préventives** doivent être mises en œuvre.

4.1 Évaluer la situation

Les GCO ont tendance à cibler soit des types spécifiques de distributeurs automatiques de billets, soit des distributeurs automatiques de certains fournisseurs dont les caractéristiques facilitent l'attaque des distributeurs automatiques. Il est donc nécessaire de procéder à une évaluation approfondie du risque d'attaques physiques des distributeurs automatiques de billets, en incluant de préférence toute la chaîne de sécurité des espèces, de l'acheminement à la livraison et au stockage dans le distributeur. Pour établir le profil de risque de chaque DAB, un certain nombre d'éléments doivent être analysés, notamment les suivants.

- Les caractéristiques de la localisation et des environs du distributeur automatique de billets ; des caractéristiques telles que l'emplacement en ville ou à la campagne, la densité de population, la proximité des postes de police, les caméras de reconnaissance automatique des plaques d'immatriculation (ANPR) dans le voisinage, la vidéosurveillance à proximité, etc.
- L'emplacement du distributeur automatique de billets :
    - à l'intérieur ou à l'extérieur d'un bâtiment, dans une agence bancaire ou dans un local éloigné (par exemple, un local commercial), intégré ou fixé à un bâtiment,
    - pour les distributeurs automatiques autonomes : qu'ils soient ancrés ou non,
    - pour les distributeurs automatiques de billets intégrés ou fixés à un bâtiment : s'il existe des faiblesses architecturales, comment le stockage des espèces est-il organisé, etc.
- Le type de distributeur automatique de billets.
- Les fonctionnalités de sécurité incluses dans le distributeur automatique de billets.

- La quantité d'argent liquide dans le distributeur automatique.
- Le type d'attaques physiques de DAB et le mode opératoire à prévoir pour adopter en premier lieu les mesures préventives les plus appropriées.
- Les mesures de sécurité et de prévention déjà prises (systèmes intelligents de neutralisation des billets de banque (IBNS), CCTV, système de brouillard de sécurité (réduction de la visibilité), etc.).

Les autres éléments à évaluer sont l'état de la coopération avec les partenaires et les parties prenantes et la législation. La collaboration entre les services répressifs et les partenaires privés et publics devrait être évaluée afin de créer des alliances pour lutter contre la criminalité. Il est possible que chaque partenaire possède des informations intéressantes pour contribuer à l'évaluation de la situation. La police locale ou les autorités locales sont particulièrement importantes dans ce cadre. La législation doit être évaluée en termes d'établissement d'un cadre juridique pour la prévention, de prise de mesures préventives obligatoires, de condamnation des attaques de distributeurs automatiques de billets, etc.

4.2 Développer une approche préventive

Une fois que la situation a été évaluée et que les principales zones à risque ainsi que les forces et faiblesses de la sécurité du DAB ont été déterminées, une stratégie peut être élaborée (souvent sur la base d'une collaboration public-privé) et des contre-mesures préventives et opérationnelles peuvent être mises en place. Les mesures de prévention devraient viser à réduire les intentions et les capacités des auteurs de ces actes. Pour y parvenir, trois axes d'actions préventives sont proposés, basés sur trois des cinq stratégies de prévention de la criminalité situationnelle de Clarke ([2]) ; réduire les butins, augmenter le risque pour les auteurs et accroître l'effort pour accéder au butin.

Les criminels comparent le profit à espérer et les risques associés (par exemple, avec une attaque de distributeur automatique de billets). En réduisant les chances d'obtenir une récompense facile et en augmentant le risque pour les auteurs, on réduit leurs attentes et leur désir de se livrer à une attaque physique des distributeurs automatiques. D'autres mesures qui augmentent l'effort nécessaire pour avoir accès au DAB affectent les capacités des auteurs. Les auteurs opportunistes, qui échouent souvent dans leurs tentatives, cessent de s'engager dans des attaques de distributeurs automatiques

([2]) Derek Corsnish et 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.

de billets. Pour les professionnels des attaques contre les distributeurs automatiques de billets, le taux de réussite est réduit, ce qui affecte à nouveau le rapport rendement/risque.

En outre, des mesures parallèles telles qu'une stratégie médiatique efficace, une prévention sociale précoce et des mesures visant à réduire le risque de dommages collatéraux aux bâtiments et à assurer la sécurité des riverains, des premiers intervenants et des passants, complètent la stratégie préventive.

D'autres moyens de structurer l'approche sont possibles. Aux Pays-Bas, les autorités appliquent le modèle dit de barrière ([3]). Ce modèle identifie les mesures qu'un criminel doit prendre pour commettre un crime. Il permet également d'identifier les partenaires et les opportunités qui favorisent la criminalité et constitue un instrument utile pour organiser le processus de collecte d'informations sur le domaine de la criminalité. En identifiant chaque étape nécessaire à l'exécution d'une attaque physique de guichet automatique, il est possible d'identifier les obstacles au délit et les meilleurs partenaires pour mettre en place ces obstacles. Le modèle de barrière identifie également les signaux permettant d'alerter les partenaires publics et privés en cas d'attaque physique de guichets automatiques et les signaux qu'ils peuvent personnellement envoyer pour signaler leurs soupçons aux autorités.

Une stratégie bien élaborée est nécessaire pour atténuer les risques qui vont de pair avec le renforcement de la prévention. Les mesures préventives, qui sont très efficaces pour décourager les amateurs et les imitateurs, ont parfois des effets indésirables. Certains groupes se tournent vers des méthodes par tâtonnement pour trouver les distributeurs automatiques vulnérables, endommageant de nombreux distributeurs. Les GCO les plus dangereux et les plus impitoyables commencent à utiliser des modes opératoires plus violents, en passant du gaz aux explosifs solides dans leurs attaques.

Afin de mettre en place un ensemble efficace de mesures préventives, l'installation d'une autorité nationale ayant le pouvoir d'imposer des mesures spécifiques pour les distributeurs automatiques de billets à haut risque, sur la base d'une analyse approfondie de la situation, est la meilleure pratique. Cette approche s'est avérée efficace en France, surtout si un cadre juridique est établi et si les mesures sont mises en œuvre simultanément aux mesures opérationnelles.

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

4.3 Mettre en œuvre des mesures préventives

Les mesures présentées dans ce chapitre et ayant pour objet de prévenir les attaques physiques contre les distributeurs automatiques de billets ont prouvé leur utilité dans différents pays. Elles sont basées sur les conclusions de la conférence sur la prévention et sur les mesures préventives activement promues par les organisations internationales actives dans la sécurité des distributeurs automatiques de billets. De nombreuses mesures sont bien connues. Plusieurs pays ont déjà mis en œuvre un certain nombre de mesures avec succès. Toutefois, les mesures proposées ne sont souvent que partiellement mises en œuvre et ne sont pas intégrées dans la législation.

Comme mentionné ci-dessus, trois axes d'actions préventives sont proposés : réduire les butins, augmenter le risque pour les auteurs et accroître l'effort nécessaire pour accéder au butin.

4.3.1 Réduire les gains

Réduire les gains des actes criminels est le premier axe de la prévention des attaques physiques contre les distributeurs automatiques de billets. Tant que la perception de « l'argent facile » persistera, les criminels se livreront à ce type de crime. En réduisant la quantité d'argent disponible et en retirant ou en détruisant l'argent, on réduit les possibilités de s'approprier un butin intéressant. Des attentes réduites diminuent le désir du criminel de se livrer à ce type de crime.

4.3.1.1 *Réduire le montant des liquidités*

Une des mesures permettant de réduire le gain consiste à diminuer la quantité d'argent liquide disponible dans un distributeur automatique. Idéalement, ce montant devrait être limité au montant nécessaire pour une seule journée ouvrée. La collaboration entre les banques pourrait garantir la rentabilité. Aux Pays-Bas, un certain nombre de banques ont collaboré pour mettre en place un réseau de distributeurs automatiques de billets indépendant des banques, appelé « Geldmaat ». L'objectif de cette collaboration est de garantir la disponibilité, l'accessibilité, la capacité et la sécurité des espèces. Cela entraînera probablement une réduction du nombre de distributeurs automatiques de billets. Toutefois, chaque distributeur ne contiendra pas plus d'argent, mais sera réapprovisionné plus souvent. Le nombre d'appoints recharges sera adapté aux besoins.

Étant donné que les auteurs s'attaquent principalement aux distributeurs automatiques entre 3 et 4 heures, il est fortement recommandé pour les distributeurs autonomes (situés pour la plupart dans des locaux commerciaux et publics, qui sont plus vulnérables), de vider le distributeur et de mettre l'argent dans un coffre-fort à la fin de la journée. Un panneau d'avertissement peut informer le public que le distributeur automatique ne conserve pas d'argent la nuit. Le lendemain, le distributeur doit être réapprovisionné hors de la vue des clients alors que les locaux sont fermés. Ce système est mis en œuvre en France où la législation oblige les détaillants disposant d'un distributeur automatique de billets autonome dans le magasin à retirer l'argent la nuit et à laisser le distributeur ouvert. Pour les autres distributeurs, les montants détenus peuvent être réduits en augmentant la fréquence des réapprovisionnements.

4.3.1.2 *Détériorer le butin et rendre l'argent traçable*

Les systèmes intelligents de neutralisation des billets de banque (IBNS) désignent une première technique de détérioration des butins. Ces systèmes tachent les billets de banque avec de l'encre pour les marquer comme volés. Des traceurs et des marqueurs peuvent être ajoutés à l'encre IBNS. Actuellement, ces marqueurs sont principalement utilisés à des fins médico-légales, ce qui permet de relier le billet à la scène de crime et d'augmenter la probabilité que les auteurs soient arrêtés. Même si l'IBNS est une mesure préventive efficace, il convient de tenir compte de quelques considérations.

La Banque centrale européenne ne rembourse pas les billets tachés ([4]) (depuis 2003), mais plusieurs banques centrales nationales des États membres de l'UE le font toujours. Les billets maculés sont également réintroduits dans le système légal via les casinos. Un IBNS crée un obstacle supplémentaire pour les criminels, mais serait beaucoup plus efficace s'il était impossible pour les criminels d'utiliser des billets de banque tachés dans l'UE. Pour ce faire, les billets tachés ne doivent pas être acceptés par les banques centrales nationales. Des exceptions peuvent être faites dans des circonstances spécifiques, telles que, par exemple, des billets maculés lors d'une fausse activation. Il est également important de conseiller à la population de ne pas accepter les billets tachés. Dans une perspective à plus long terme, les lecteurs de billets devraient détecter les billets tachés et être installés dans les banques et dans les locaux commerciaux tels que les casinos, les carwashs, etc. La détection de l'encre est difficile et coûteuse, mais une solution rentable pourrait consister à installer des systèmes infrarouges qui détectent les billets tachés de marqueurs infrarouges. Ces systèmes ont prouvé leur efficacité et constituent une bonne pratique en Belgique et en France. Lorsque des billets maculés de marqueurs infrarouges sont introduits dans le distributeur automatique, celui-ci accepte

([4]) Décision de la Banque centrale européenne, Les valeurs unitaires, les spécifications, la reproduction, l'échange et le retrait des billets de banque en euros, 2003.

(« avale ») l'argent mais ne le crédite pas sur un compte. La personne qui introduit les billets tachés doit également être enregistrée.

D'autres considérations doivent être prises en compte lors de l'installation de solutions IBNS. Plusieurs fabricants proposent différentes solutions IBNS avec différents mécanismes d'activation et différents types d'encre. Une première considération concerne le fait que tous les types de technologies d'activation IBNS ne peuvent pas contrer toutes les menaces. Certains IBNS fonctionnent très bien pour les attaques-bélier, les attaques *in situ* et les attaques au gaz, mais ne fonctionnent pas en cas d'attaque à l'explosif solide ou vice versa. La technologie choisie doit donc être bien réfléchie.
Une autre considération concerne le type d'encre à choisir. En Belgique, les exigences nationales minimales pour l'IBNS (sécurité, pourcentage de taches, non lavable, etc.) sont fixées et des tests indépendants certifient que le système répond aux normes nationales et fonctionne selon les indications du fabricant. Il est important de faire des tests sur de vrais billets de banque, car il existe sur le marché des encres moins chères qui fonctionnent bien avec les faux billets, mais pas avec les vrais billets : cela signifie que l'encre peut être éliminée des vrais billets par lavage. En outre, il est recommandé d'ajouter un marqueur médico-légal à l'encre, ce qui permet d'établir un lien entre les billets tachés et une scène de crime spécifique.

Les meilleures pratiques démontrent que l'IBNS peut être très efficace, surtout en combinaison avec d'autres mesures préventives. En 2015, la France a introduit une nouvelle législation incluant des dispositions sur l'installation d'IBNS et l'utilisation d'encre à ADN unique. C'est la police militaire française (gendarmerie) qui, sur la base d'une évaluation des risques, décide où l'IBNS et d'autres mesures doivent être mises en œuvre. Depuis que la nouvelle législation a renforcé l'approche préventive et opérationnelle, le nombre d'attaques est passé de 300 en 2013 à 50 en 2018.

L'utilisation de **colle** est une autre technique en cours de développement et ayant pour objet de détériorer le butin. L'efficacité de la colle a été démontrée aux Pays-Bas, mais les coûts de mise en œuvre et de fonctionnement sont actuellement élevés. De plus, la colle peut engendrer un risque d'incendie si le système n'est pas activé avant une attaque, car la dispersion des particules de colle dans l'air pourrait produire un mélange combustible. Cette méthode ne peut encore être commercialisée, mais pourrait être une solution d'avenir.

4.3.2 Augmenter le risque

Un deuxième axe pour la prévention des attaques physiques contre les distributeurs automatiques de billets consiste à dissuader les auteurs potentiels de commettre des crimes en augmentant le risque de détection et de sanction. Outre le risque de blessures physiques lors de l'utilisation d'explosifs pour des attaques de distributeurs automatiques de billets, le principal risque pour un criminel réside dans une peine de prison lorsqu'il est pris sur le fait (« en flagrant délit ») ou après une enquête. Afin de réduire le désir des auteurs potentiels, le risque de détection et de sanction doit être augmenté. Pour la société, arrêter et condamner les criminels est, naturellement, une méthode de prévention très efficace en cas de sanction ultérieure, comme nous l'avons vu dans plusieurs pays.

4.3.2.1 *Partage d'informations*

Le partage d'informations entre toutes les parties prenantes dans la lutte contre les attaques physiques contre les distributeurs automatiques de billets, notamment les fournisseurs de distributeurs automatiques de billets, les autorités répressives (police, procureur, etc.), les pouvoirs publics, les fabricants de distributeurs automatiques de billets et de dispositifs de sécurité et de protection, les associations professionnelles, les fournisseurs de distributeurs automatiques de billets (banques et fournisseurs indépendants), les sociétés de sécurité et les centres d'alarme, est essentiel pour détecter et punir les auteurs. Idéalement, ce partage devrait être instauré au niveau tant national qu'international.

Une détection précoce d'une prochaine attaque physique contre un guichet automatique est difficile. Une détection précoce n'est possible que si le partage d'informations au niveau international entre les partenaires des services répressifs et les partenaires privés (sociétés de sécurité et fournisseurs de distributeurs automatiques de billets) ne connaît aucun accroc. Un large éventail d'indicateurs doit être surveillé, notamment les messages d'alerte rapide entre les services répressifs concernant les GCO en mouvement, les informations sur les véhicules (« chauds ») qui ont été utilisés dans des attaques de DAB, les informations des entreprises de sécurité ou des surveillances de quartier sur les comportements suspects détectés dans la zone entourant le DAB, les transactions suspectes détectées par les fournisseurs de DAB et d'autres méthodes de détection. D'autres mesures policières possibles pour une détection précoce sont la surveillance des voitures volées, des fabricants et distributeurs d'explosifs et des entreprises autorisées à utiliser des explosifs. Les efforts

nécessaires pour parvenir à une détection précoce sont exigeants et n'ont aucune garantie de succès, c'est pourquoi les interventions des forces de l'ordre avant une attaque sont rares.

Si une détection précoce est impossible, les centres d'alarme sont en mesure d'émettre rapidement un avertissement en cas d'attaque physique d'un distributeur automatique de billets. Afin de permettre l'intervention, des réglementations et des protocoles nationaux pour une communication rapide entre les centres d'alarme et les forces de l'ordre doivent être convenus et mis en place. En cas de détection précoce ou d'information en temps réel, les services répressifs devront toujours évaluer le moment et la meilleure opportunité d'intervention. Il est très difficile d'arrêter les criminels en flagrant délit et cela peut induire des situations dangereuses, car certains GCO sont très violents et utilisent des armes lourdes.

Pour que l'enquête menée après une attaque physique de guichet automatique soit couronnée de succès, les agents des forces de l'ordre doivent communiquer avec toutes les parties prenantes, car une d'entre elles pourrait détenir des informations contribuant au succès d'une enquête. Bien entendu, la communication et la collaboration avec les premières victimes, les banques ou les autres fournisseurs de distributeurs automatiques de billets, sont nécessaires : ils ont accès à des données importantes pour l'enquête. Pour le fournisseur de guichets automatiques, les informations fournies par les services répressifs contribueront à améliorer les mesures de prévention. En outre, les contacts avec les associations professionnelles et les fabricants s'avèrent utiles : ils envoient souvent des messages d'alerte de sécurité auxquels les autres parties intéressées peuvent souscrire. Les fabricants de DAB possèdent une bonne vue d'ensemble des différents types d'attaques de DAB et des faiblesses et forces correspondantes des mesures préventives. Ils sont totalement disposés à apporter leur soutien à la police en lui fournissant des informations sur les aspects techniques des distributeurs automatiques de billets et sur les modes opératoires utilisés.

La coopération transfrontalière est essentielle : les pays devraient partager des informations (sur les suspects, les personnes condamnées pour des attaques de distributeurs automatiques de billets, les modes opératoires, les véhicules suspects, les images d'attaques, etc.), non seulement pour soutenir l'enquête, mais également parce que les suspects condamnés dans un autre pays peuvent être condamnés pour récidive.

Enfin, la création d'une base de données au niveau européen, accessible aux services répressifs et contenant des données médico-légales (par exemple, sur différents types d'encres IBNS, de traceurs et de marqueurs ou de vitres de protection des distributeurs automatiques) pourrait

substantiellement faciliter les enquêtes et permettre de relier les suspects à une scène de crime spécifique. La standardisation des technologies au niveau international est souvent insuffisante : lors de la conférence du mois de janvier 2019, les participants ont indiqué que la standardisation de l'encre et des marques de délit au niveau de l'UE pourrait grandement faciliter les enquêtes.

4.3.2.2 *CCTV et dispositifs d'écoute*

Les images et le son des systèmes de vidéosurveillance et des dispositifs d'écoute peuvent faciliter tant la détection en temps réel d'une attaque (par exemple, pour éviter que les premiers intervenants qui arrivent sur les lieux du crime ne subissent des dommages physiques) que les enquêtes ultérieures (par exemple, pour identifier les auteurs et leur mode opératoire). Les images de la CCTV peuvent être combinées avec les images des systèmes publics et autres systèmes de CCTV situés à proximité du distributeur automatique de billets et les images des radars de circulation afin de fournir une image plus complète des auteurs et de leur mode opératoire.

Cependant, les images de la CCTV sont souvent de mauvaise qualité ou mal stockées. Les images doivent être de qualité suffisante pour permettre l'identification d'une personne. Là encore, l'établissement de normes européennes pour la vidéosurveillance de sécurité faciliterait les enquêtes. En outre, comme les auteurs de ces crimes désactivent souvent les caméras de vidéosurveillance avant une attaque, l'installation de caméras de vidéosurveillance invisibles ou de dispositifs d'écoute en temps réel pourrait également être envisagée.

4.3.2.3 *Punition et réhabilitation des auteurs*

Des sanctions cohérentes et sévères ont démontré leur effet préventif. L'arrestation d'un GCO a un effet immédiat sur le nombre d'attaques de distributeurs automatiques de billets. Cependant, la libération des auteurs d'attaques sur les distributeurs automatiques de billets engendre souvent une nouvelle vague d'attaques. Cela signifie que les peines courtes permettent aux auteurs de reprendre très rapidement leurs activités. Les sanctions minimales et maximales applicables aux criminels condamnés pour chaque type d'attaque physique contre les distributeurs automatiques de billets varient selon les États membres. Certains estiment que des peines plus lourdes dissuaderont les auteurs potentiels. Toutefois, des recherches scientifiques ([5]) démontrent que l'augmentation de la

([5]) David Weisburd, David P. Farrington et Charlotte Gill, « Conclusion : What Works in Crime Prevention Revisited », David Weisburd,

sévérité des peines ne renforce pas nécessairement l'effet dissuasif. Il pourrait donc être intéressant de se pencher sur les programmes de réhabilitation correctionnelle (et axée sur l'auteur) afin de réduire le taux élevé de récidive.

4.3.3 Intensifier les efforts

Le troisième axe, qui vise à prévenir les attaques physiques contre les distributeurs automatiques de billets, prévoit des mesures qui rendent l'exécution de l'acte criminel plus exigeante pour l'auteur.

4.3.3.1 *Garantir un environnement résilient à la criminalité*

Si l'évaluation des risques (cf. supra) démontre qu'un distributeur automatique de billets se situe dans un environnement à risque élevé, le bâtiment devrait être dépourvu de son distributeur et ce dernier devrait être transféré dans une zone à risque faible ou moyen. Tel est certainement le cas si l'analyse démontre que le bâtiment pourrait s'effondrer si un distributeur automatique de billets est attaqué avec des explosifs. Une législation pourrait être mise en œuvre pour appliquer ces mesures dans les cas à risque élevé. Outre la réduction du nombre de distributeurs automatiques de billets dans les environnements à haut risque, les paiements sans numéraire devraient être encouragés pour réduire le besoin de distributeurs automatiques.

S'il s'avère impossible de transférer le DAB, un maximum de mesures de sécurité doivent être prises : par exemple, l'utilisation de bornes anti-attaque bélier, de lampadaires et d'autres éléments de mobilier urbain pour restreindre l'accès au bâtiment, des systèmes d'arrêt des véhicules, l'installation d'un éclairage public adéquat, une surveillance accrue, visible ou cachée, et des dispositifs antivol tels qu'un système de dégradation des billets de banque. Lorsqu'un bâtiment est attaqué à un endroit qui n'a pas été identifié comme étant à haut risque, il doit être identifié comme tel et des mesures de sécurité supplémentaires doivent être ajoutées. Les nouveaux facteurs doivent être pris en compte dans l'outil d'évaluation des risques afin de l'actualiser. La réévaluation de ce risque devrait être une opération récurrente.

David P. Farrington et Charlotte Gill, *What works in Crime Prevention and Rehabilitation*. Cambridge: Springer, 2016, 311.

4.3.3.2 *Renforcer les distributeurs automatiques de billets*

Les fabricants de DAB proposent une gamme standard de DAB dotés de plusieurs éléments de sécurité qui sont classés selon les niveaux de sécurité du Comité européen de normalisation (CEN). En général, les distributeurs automatiques de billets portent un marquage CEN allant du CEN1, le plus bas, à CEN4, le plus élevé. Des caractéristiques telles que la force et la résistance du caisson aux attaques déterminent la note. La résistance au gaz est principalement proposée en option (CEN-GAS). Les modèles standards peuvent être complétés par des mesures de protection supplémentaires. Généralement, des tiers installent ces fonctionnalités pour assurer la conformité avec la législation nationale et l'adaptation du modèle de base aux exigences des clients nationaux. Parmi les dispositifs de sécurité supplémentaires figurent divers capteurs permettant d'activer un système de neutralisation des gaz ou IBNS en cas d'attaque *in situ* ou à l'aide d'explosifs, ainsi que des volets et des serrures de chambre forte renforcés pour empêcher l'accès non autorisé au coffre-fort quand le volet principal est compromis. Pour les distributeurs automatiques de billets portables et autonomes, il est important d'utiliser des systèmes d'ancrage qui offrent une protection supplémentaire contre les attaques par arrachage ou bélier. Des systèmes de suivi peuvent être inclus dans le DAB pour aider les enquêteurs lorsque le DAB est transporté vers un autre endroit avant son ouverture.

4.3.3.3 *Mesures architecturales*

Lors de l'installation d'un distributeur automatique de billets, il est conseillé d'utiliser des machines avec accès par l'arrière. Dans ce cas, l'auteur doit entrer dans le bâtiment et accéder à l'arrière de la machine pour voler l'argent. Les distributeurs automatiques de billets portables et autonomes sont les plus vulnérables. Une réduction du nombre de ces DAB permettrait d'accroître la sécurité. L'obligation d'installer les distributeurs automatiques de billets dans un local anti-effraction diminuerait automatiquement l'utilisation des distributeurs autonomes.

4.3.3.4 *Système de brouillard*

Un canon à brouillard remplit rapidement une pièce d'un brouillard dense, de sorte que l'intrus ne peut rien voir. Ce brouillard de sécurité rend souvent impossible l'exécution de l'attaque des distributeurs automatiques de billets. Au minimum, le système ralentit l'auteur des faits, laissant le temps aux services de police d'intervenir. Le système de brouillard de sécurité est relié au système d'alarme et peut être activé de deux façons. Il peut être déclenché automatiquement par des

capteurs d'alarme tels que les détecteurs de mouvement (la nuit) ou les capteurs de manipulation du volet du DAB. Il peut également être activé par un centre d'alarme afin d'éviter un nombre trop élevé de fausses alertes. Pour les distributeurs automatiques de billets fixés dans un mur et en plein air, le système de brouillard peut être installé à l'arrière du distributeur afin de remplir la pièce située à l'arrière avec du brouillard et réduire à zéro la visibilité des auteurs de l'infraction.

Les systèmes de brouillard peuvent assurer la protection ponctuelle d'un distributeur automatique de billets situé dans des espaces ouverts dans les stations-service, les supermarchés, etc. Cela permet d'éviter que le brouillard ne remplisse toute la zone. La protection par brouillard est plus efficace lorsque ce dernier provient de différents angles ou lorsqu'il remplit l'espace derrière le distributeur automatique de billets dans le cas
d'une attaque bélier.. Des tests sont en cours afin de déterminer si des canons à brouillard peuvent être installés dans le distributeur automatique de billets lui-même, plutôt que dans la pièce où se trouve le distributeur. Des marqueurs ADN qui tachent les auteurs et leurs vêtements peuvent être ajoutés au brouillard.

4.3.4 Mesures parallèles

Afin d'assurer la mise en œuvre efficace et effective des mesures préventives susmentionnées, plusieurs mesures parallèles doivent être envisagées. Ces mesures sont indispensables pour permettre ou renforcer une approche préventive et opérationnelle globale pour faire face aux attaques physiques contre les distributeurs automatiques de billets.

4.3.4.1 *Législation*

Dans plusieurs pays, la législation impose aux fournisseurs de DAB de prendre des mesures préventives. Dans d'autres pays, l'établissement de conventions et d'accords entre les banques et les forces de l'ordre garantit une approche dûment gérée afin de lutter contre les attaques physiques contre les distributeurs automatiques de billets. Les domaines dans lesquels des mesures réglementaires peuvent être envisagées sont les suivants :

- l'intégration de mesures préventives ;
- des cadres juridiques permettant la collaboration entre les services répressifs et les partenaires publics et privés ;

- un remaniement des peines si les auteurs d'attaques physiques contre les distributeurs automatiques sont trop peu sanctionnés.

Toutefois, seuls les établissements bancaires sont souvent tenus de s'y conformer et les fournisseurs indépendants de distributeurs automatiques ne sont pas liés par ces lois ou accords. Il s'agit d'un point faible commun dans un cadre réglementaire.

Certains pays n'appliquent aucune réglementation, mais tentent de persuader les fournisseurs de distributeurs automatiques de prendre des mesures préventives en les sensibilisant aux domaines et aux tendances de la criminalité : cela s'avère particulièrement difficile dans les pays comptant un grand nombre de banques indépendantes.

Il est impératif de veiller à ce que la mise en œuvre effective des mesures préventives comprenne des modifications de la législation et de la réglementation, tant au niveau national qu'international, liant tous les types de fournisseurs de DAB. Idéalement, la législation devrait être alignée au niveau de l'UE pour éviter que les mesures préventives fortes intégrées dans la législation d'un pays ne poussent les GCO à se déplacer dans d'autres pays où la réglementation est moins stricte.

4.3.4.2 *Stratégie médiatique*

Un autre axe important de la stratégie de prévention est une stratégie médiatique bien établie qui vise à réduire les espoirs et les envies des auteurs d'attaques contre les distributeurs automatiques de billets de se livrer à ce crime. Les faibles taux de réussite et les risques élevés pour les auteurs de l'attaque ont déjà été mis en exergue ; la communication sur les gains (« butin ») ou les détails sur l'attaque du DAB, tels que le type de DAB touché ou le MO évité. D'autre part, il est nécessaire de communiquer largement sur les arrestations de suspects et les sanctions qui en découlent après une condamnation.

4.3.4.3 *Une collaboration renforcée*

Le renforcement de la collaboration et de l'échange d'informations a été largement abordé, mais on ne saurait trop insister sur ce point. L'échange d'informations opérationnelles au niveau international est l'activité principale d'Europol. Outre cet échange d'informations, la conférence sur la prévention a mis en évidence la nécessité impérieuse d'accroître la coopération multidisciplinaire et à plusieurs niveaux ainsi que le partage d'informations entre toutes les parties concernées, notamment les

services répressifs, les autorités publiques, les fabricants de distributeurs automatiques de billets et de dispositifs de sécurité et de protection, les associations professionnelles, les fournisseurs de distributeurs automatiques de billets (banques et fournisseurs indépendants), les entreprises de sécurité et les centres d'alarme. Cela doit inclure le niveau local, national et international.

4.3.4.4 *Réduire le risque de dommages collatéraux*

En cas d'attentats à l'aide d'explosifs solides, certains GCO laisseront du matériel derrière eux. Cela peut créer des situations dangereuses pour les premiers intervenants ou les civils (qui vivent dans le voisinage ou sont présents sur les lieux). Leur sécurité doit être assurée. Comme tel est le cas en Belgique, les protocoles et les procédures à suivre par les premiers intervenants (tant ceux des forces de l'ordre que ceux des fournisseurs de DAB) doivent être élaborés et alignés les uns sur les autres. Une autre bonne pratique dans ce contexte est l'exemple des Pays-Bas, où les images de vidéosurveillance de l'attaque du DAB sont utilisées pour évaluer la situation. Des accords avec des centres d'alarme peuvent être conclus afin que ces images soient immédiatement disponibles.

4.3.4.5 *Prévention sociale*

Souvent, les GCO essaient de recruter des jeunes. Des projets pourraient être mis en place pour faire échouer ces processus de recrutement à un stade précoce. La police ou les travailleurs sociaux devraient être attentifs à ces processus et pourraient intervenir en approchant personnellement les auteurs potentiels.

5 Conclusions

Au cours des deux dernières années, le nombre de pays européens touchés par des attaques physiques de distributeurs automatiques de billets a augmenté. À cet égard, Europol et le REPC ont collaboré pour rassembler les meilleures mesures de prévention et de lutte contre ce crime.

Une approche efficace pour contrer les attaques physiques contre les distributeurs automatiques de billets consiste en une combinaison de mesures opérationnelles et préventives, de préférence intégrées dans un cadre législatif. Afin d'éviter que des mesures fortes dans un pays ne poussent les GCO à se déplacer vers des pays plus vulnérables, il est recommandé d'adopter ces mesures au niveau européen.

Pour prévenir et combattre ce type de criminalité, une stratégie claire devrait être établie en trois étapes : l'évaluation de la situation, l'élaboration d'une approche préventive basée sur l'évaluation des risques et la mise en œuvre des mesures préventives.

L'évaluation des risques d'attaques physiques contre un DAB doit inclure les caractéristiques du DAB et de ses environs, la coopération avec les partenaires et les parties prenantes pour créer des alliances afin de lutter contre ce crime et l'évaluation du cadre préventif et juridique. Une fois la situation évaluée, une stratégie fondée sur la collaboration entre les secteurs public et privé et sur des contre-mesures préventives et opérationnelles devrait être mise en place. L'objectif des mesures préventives est de réduire l'intention et les capacités de l'auteur à s'engager dans une attaque physique contre le DAB. Pour y parvenir, trois axes d'actions préventives sont proposés : réduire les gains, augmenter le risque et accroître l'effort. Des mesures parallèles devraient compléter la stratégie de prévention. L'installation d'une autorité nationale ayant le pouvoir d'imposer ces mesures nécessaires est une bonne pratique.

En **réduisant les gains**, l'envie du criminel de se livrer à ce type de crime diminue. Réduire la quantité d'argent liquide dans les DAB en limitant le réapprovisionnement à ce qui est suffisant pour une journée de transactions seulement, ou en vidant les DAB (les plus vulnérables) la nuit, est une mesure qui permet de réduire les espoirs du criminel. Une autre méthode consiste à détériorer le butin et à rendre l'argent traçable. Dans ce contexte, on peut avoir recours à l'IBNS, qui colore les billets et les marque comme volés. Cette méthode est la plus efficace, car les criminels ne peuvent dépenser cet argent ni réintroduire ces billets dans le système légal d'argent liquide. Pour ce faire, les banques et le public ne doivent pas accepter de paiement avec des billets maculés et doivent installer des lecteurs de billets capables de détecter et de refuser les billets tachés. À cet égard, l'investissement dans des systèmes infrarouges qui détectent les billets tachés par des marqueurs

infrarouges s'est avéré être une solution rentable en Belgique et en France. Lors de l'installation d'un IBNS, les pays doivent examiner attentivement les mécanismes d'activation choisis, les exigences minimales pour la neutralisation des billets et l'ajout d'un marqueur médico-légal à l'encre.

Un deuxième axe de prévention des attaques physiques contre les distributeurs automatiques de billets consiste à dissuader les auteurs potentiels de commettre des crimes en **augmentant le risque** de détection et de sanction. La collecte et le partage d'informations entre toutes les parties prenantes, tant au niveau national qu'international, sont essentiels à la détection et à la sanction des auteurs d'attaques contre les distributeurs automatiques de billets. L'échange d'images et de données sonores de haute qualité provenant de la vidéosurveillance peut augmenter les probabilités de détection précoce et de réussite des enquêtes. Afin d'éviter que la vidéosurveillance ou les dispositifs d'écoute soient désactivés avant l'attaque, l'installation d'une vidéosurveillance invisible ou de dispositifs d'écoute en temps réel peut être envisagée. La création d'une base de données médico-légales et la normalisation des technologies au niveau européen pourraient grandement faciliter la coopération et les enquêtes internationales. Si les auteurs sont arrêtés et condamnés, il pourrait donc être intéressant de se pencher sur les programmes de réhabilitation correctionnelle (et axée sur l'auteur) afin de réduire le taux élevé de récidive.

Le troisième axe visant à prévenir les attaques physiques contre les distributeurs automatiques de billets comprend des mesures visant à **intensifier l'effort** que l'auteur doit nécessairement consentir pour réaliser l'acte criminel. L'installation d'un distributeur automatique de billets dans un environnement résilient à la criminalité, avec un maximum de mesures de sécurité, rendra l'attaque d'un distributeur automatique de billets plus exigeante pour les auteurs. En outre, la protection standard des distributeurs automatiques de billets peut être renforcée par plusieurs dispositifs de sécurité supplémentaires. Outre ces mesures, l'installation d'un système de brouillard peut dissuader l'auteur ou au moins ralentir l'attaque.

Plusieurs **mesures parallèles** renforceront les mesures susmentionnées, telles que la création d'un cadre juridique obligeant tous les fournisseurs de DAB à mettre en œuvre les mesures préventives, l'élaboration d'une stratégie médiatique bien établie, le renforcement de la collaboration aux niveaux local, national et international, l'élaboration de lignes directrices pour les premiers intervenants afin de réduire les risques de dommages collatéraux et l'investissement dans la prévention sociale pour saper les processus de recrutement des criminels.

6 Recommandations pour une approche préventive : vue d'ensemble

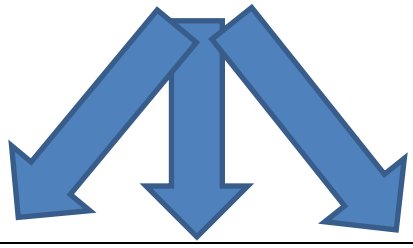
Élaborer une réponse efficace pour prévenir les attaques physiques contre les distributeurs automatiques de billets

Évaluer la situation

Établir le profil de risque des distributeurs automatiques de billets dans votre pays/région
Identifier les partenaires et les parties prenantes dans la lutte contre les attaques physiques de DAB et évaluer la collaboration
Évaluer le cadre juridique pour lutter contre les attaques physiques contre les distributeurs automatiques de billets au niveau national et international.

Développer une approche préventive

Déterminer les (principaux) risques à couvrir et les priorités
Déterminer les meilleures mesures préventives pour couvrir ces risques en considérant trois axes principaux.
Déterminer les mesures préventives parallèles nécessaires pour renforcer les mesures préventives prises.



Les mesures préventives qui peuvent être prises pour		
Réduire les gains	Augmenter le risque	Intensifier les efforts
– Réduire le montant des liquidités ○ Vider le distributeur automatique de billets la nuit. ○ Augmenter le nombre/fréquence des réapprovisionnements. – Détériorer le butin. ○ Les systèmes intelligents de neutralisation des billets de banque (IBNS). ○ Marqueurs infrarouges dans l'encre IBNS pour permettre aux lecteurs de billets de détecter les billets maculés.	– Partage d'informations transfrontalier pour : ○ la détection précoce ou en temps réel d'une éventuelle attaque de guichet automatique, ○ le renforcement de l'approche opérationnelle, ○ la condamnation des récidivistes, ○ l'échange de données médico-légales au niveau européen. – Vidésosurveillance et dispositifs d'écoute.	– Garantir un environnement résilient à la criminalité ○ Changement d'emplacement des distributeurs automatiques de billets à haut risque. ○ Mesures de sécurité : obstacles physiques, surveillance, etc. – Renforcer les distributeurs automatiques de billets avec des volets, résistants aux gaz ou aux explosifs solides, etc. – Mesures architecturales telles que les machines avec accès par l'arrière

○ En cours de développement : colle.	– Sanction et réhabilitation des auteurs	– Systèmes de brouillard de sécurité.

Mesures parallèles pour renforcer l'approche préventive

- Une législation efficace comprenant des mesures préventives contre les attaques physiques des distributeurs automatiques de billets, des peines consécutives, etc.
- Une stratégie médiatique efficace pour décourager les auteurs.
- Collaboration renforcée entre toutes les parties prenantes (publiques, privées, forces de l'ordre) dans la lutte contre les attaques physiques contre les distributeurs automatiques de billets.
- Réduire le risque de dommages collatéraux pour les premiers intervenants ou les civils (par exemple, ceux qui vivent dans le voisinage ou qui sont présents sur les lieux).
- Prévention sociale évitant aux jeunes d'être recrutés pour ce (type de) crime.