Lettre d'information économique

Sommaire

Décembre 2021

Editorial

Mesdames, Messieurs,

L'aventure entrepreneuriale est doublement guidée, sur les marchés où elle s'applique, par **la réalisation volontaire d'une stratégie commerciale** réfléchie et par **l'adaptation aux effets ou la réaction aux surprises** – souvent concurrentielles, événementielles ou conjoncturelles – qui marquent l'activité économique.

À ce titre, l'été 2021 aura vu se succéder une série d'événements illustrant l'âpreté de cette **confrontation directe ou sous-jacente des volontés** dans la sphère économique et l'occurrence régulière de surprises parfois stratégiques.

Gardant en mémoire la finalité première de l'entreprise, qui vise par ses offres de service à créer de la compétitivité et de la prospérité, la DRSD ambitionne, c'est son mandat, de participer au **juste équilibre entre compétitivité et sécurité économique**. En effet, l'action quotidienne de détection, de caractérisation et d'anticipation des ingérences, dont notre service de renseignement se charge dans une démarche collective, doit constituer une « assurance-vie » pour une compétitivité durable servant les intérêts nationaux.

Parce qu'il n'y a, désormais, plus de frontières entre la protection physique de vos sites, la surveillance des échanges numériques et la vigilance juridique, j'ai choisi de faire de cette neuvième lettre d'information économique **un outil de sensibilisation** sur ces trois périmètres, à travers un état des lieux traitant du phénomène croissant des intrusions aériennes de drones, de la captation logicielle de données et des nouvelles contraintes législatives chinoises à l'export.

Sollicitant de votre part une ample diffusion de ces éclairages, je vous assure de l'appui de la DRSD et de son réseau territorial dans l'**anticipation des atteintes et des contraintes** décrites dans les pages qui suivent.

Général de Corps d'Armée Eric Bucquet

Directeur du Renseignement et de la Sécurité de la Défense

Comprendre PEGASUS

Un logiciel d'espionnage si discret

Qu'est ce que c'est ?

Pegasus est un logiciel espion développé par la société israélienne NSO GROUP à destination d'agences gouvernementales en vue de lutter notamment contre le terrorisme. Celui-ci s'exécute sur les *smartphones* fonctionnant principalement sous IOS ou Android. En juillet 2021, ce logiciel a été mis en lumière par une révélation d'Amnesty International et du consortium de journalistes *Forbidden Stories*. En effet, son utilisation aurait été détournée dans le cadre d'une large campagne d'espionnage qui ciblerait des journalistes, des défenseurs des droits de l'Homme, la sphère politique mais aussi des industriels.

Comment ça fonctionne ?

PHASE D'INFECTION

Les investigations menées ont permis de déterminer, qu'initialement, le processus d'infection des utilisateurs avait recours à l'envoi d'un message contenant un lien permettant l'infection de l'appareil ciblé. Actuellement, il semblerait que les clients de NSO GROUP aient recours à des techniques ne nécessitant plus d'interaction avec la cible et utilisent des techniques d'interception du trafic cellulaire ou de failles dites « zéro click » pouvant exister dans les applications mobiles grand-public comme WhatsApp ou Apple iMessage.

FONCTIONNALITÉS

Pegasus est un maliciel techniquement avancé, qui permet de prendre le contrôle sur le terminal cible et d'en extraire l'ensemble des informations présentes comme les messages (y compris de messageries dites chiffrées), les photos, les contacts… Plus encore, l'opérateur de Pegasus est en mesure de déclencher à distance des enregistrements vidéo et audio, y compris des conversations téléphoniques. De plus, le maliciel est difficilement détectable sur les périphériques puisque non persistant sur l'appareil de la victime.

L'infrastructure attaquante et les méthodes d'installation utilisées permettent une réinstallation de celui-ci après un redémarrage, une remise en configuration d'usine voire un changement de terminal.

Que faire si je pense avoir été ciblé ?

Dans l'hypothèse d'une infection par Pegasus, il convient premièrement de cesser toute utilisation de l'appareil, de l'isoler physiquement et de l'éteindre en retirant la batterie de manière à ce qu'aucune information classifiée ou sensible ne puisse être captée par l'appareil. Puis, un audit du terminal doit être réalisé à l'aide, par exemple, de l'outil *Mobile Verification Toolkit* proposé en source ouverte par AMNESTY INTERNATIONAL.

En cas d'infection, un changement de numéro téléphonique, entraînant un changement de carte SIM, et une réinitialisation d'usine du téléphone sont *a minima* nécessaires mais peuvent ne pas se révéler suffisant.

Comment se protéger de logiciels espions comme PEGASUS ?

Afin de se protéger ou tout du moins limiter les risques liés à une infection de ses appareils mobiles, quelques règles d'hygiène informatique et de bonnes pratiques sont à respecter, à commencer par ne pas mélanger usages personnel et professionnel...

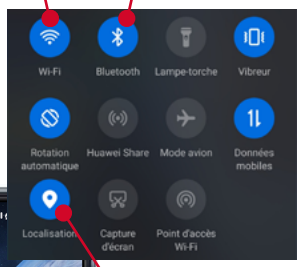
Comprendre PEGASUS

Recommandations

WI-FI
N'utiliser que des réseaux WI-FI de confiance. Sinon, privilégier les réseaux cellulaires aux réseaux WI-FI publiques. En cas d'absolue nécessité d'utilisation de tels réseaux, employer un VPN.

Bluetooth®
Désactiver le Bluetooth® quand il est non utilisé.
Attention, depuis Android 11 le Bluetooth n'est plus systématiquement désactivé en mode avion.

Applications
Limiter le nombre d'applications installées au strict minimum.
Ne les installer que depuis les marchés applicatifs officiels.
Vérifier et limiter les permissions données aux applications.



Géolocalisation
Limiter l'utilisation de la géolocalisation au strict minimum.
Toujours désactiver la géolocalisation après utilisation.

Anti-virus
Utiliser une solution anti-virus reconnue, par exemple, F-SECURE ou AVG (gratuit).

Contrôle
Toujours conserver le contrôle physique de son appareil mobile.
Ne pas connecter de support amovible inconnu.
Ne pas modifier son système ou chercher à obtenir de droit d'administration supérieur sur le système par exemple via rootage ou jailbreak.

Fichier
Ne pas conserver de fichiers sensibles sur son appareil.

VPN
Utiliser un VPN dès lors que la connexion internet n'est pas sûre. Par exemple, PROTONVPN (gratuit).

Téléphonie / Conversation
Ne pas échanger d'informations sensibles via un appareil non configuré pour transmettre ce type d'information.
Éviter les échanges d'informations sensibles à proximité du terminal.

Mise à jour
Mettre à jour le plus tôt possible son appareil après la diffusion d'une mise-à-jour système ou applicative.

Messagerie/Mail
Ne pas avoir de conversation sensible via une messagerie non prévue à cet effet.
Ne pas ouvrir de lien inconnu même provenant de sources connues, privilégier un accès au site via le navigateur WEB.

Accessoires
Ne jamais utiliser d'accessoire dont l'origine n'est pas certaine.
Ne jamais connecter ou laisser connecté son appareil mobile sur un ordinateur ou autre dispositif inconnu.

Les moteurs de recherche

INTRODUCTION

L'objet de cet article est de présenter comment certaines entreprises utilisent leur service de moteur de recherche afin de collecter toujours plus de données. En effet, il est possible de tracer les utilisateurs au travers de leur comportement sur différents sites Internet. Or, force est de constater que les annonceurs publicitaires ne se privent pas d'exploiter les données qui peuvent être collectées au niveau des moteurs de recherche, en vue d'en tirer des informations « monétisables ». À l'inverse, comme on pourra le voir, d'autres sociétés sont plus respectueuses de la vie privée de leurs utilisateurs.

FONCTIONNEMENT SIMPLIFIÉ

Les moteurs de recherche sont des services Web permettant d'effectuer des recherches en ligne pour identifier des ressources à partir d'une requête composée de mots, de symboles ou même d'images. Ils fonctionnent généralement grâce à une indexation préalable du contenu des sites Internet dans des bases de données permettant de cartographier le Web.

Au-delà de ce service « simple », 3 autres types de moteurs de recherches peuvent être identifiés :

- les méta-moteurs, qui puisent leurs résultats à travers plusieurs moteurs de recherche ;
- les moteurs de recherche hybrides, qui fournissent une réponse résultant de leur propre indexation et de celles d'autres moteurs. Ex : DuckDuckGo ou Qwant ;
- les multi-moteurs, qui proposent des formulaires permettant d'interroger un ou plusieurs moteurs au choix.

La plupart des moteurs de recherche conservent un historique horodaté des recherches effectuées par les utilisateurs. Ce sont des « logs ». On y retrouve les termes recherchés, les adresses IP et le système d'exploitation des machines à l'origine de la requête. En vue et au prétexte de fournir des services toujours plus personnalisés, ces données, permettant de retracer l'intégralité des recherches d'un utilisateur, sont traitées par des intelligences artificielles afin de connaître toujours mieux ce dernier. Elles peuvent par ailleurs compléter, pour certains navigateurs, les informations relevées depuis d'autres « capteurs » de leur écosystème (applications, systèmes d'exploitation, objets connectés, etc.).

Certains États accèdent à ces données par le biais de réquisitions judiciaires. C'est pourquoi il est important de prêter attention à la localisation du siège social de ces sociétés et des sites de stockage de leurs données (cf. tableau de synthèse).

Les moteurs de recherche

MOTEURS DE RECHERCHE INTRUSIFS

Google

Représentant 92% des recherches en France (tous types d'appareils confondus), Google est un parfait exemple de l'adage : « si c'est gratuit, c'est que c'est vous le produit ».

En effet, l'activité des utilisateurs sur le Web est fichée et répertoriée pour mieux cibler les résultats des recherches et les annonces publicitaires. Le fichage publicitaire dépasse la simple recherche Web. Il tire également profit de toutes les informations disponibles liées aux autres produits de l'entreprise. Il peut s'agir du comportement de navigation, de l'activité sur Gmail et YouTube, de l'historique des positions géographiques, des achats en ligne, des appareils utilisant le système d'exploitation Android, des objets connectés etc. Tout ce qui est lié à Google d'une façon ou d'une autre peut être utilisé pour faire « remonter » des données sur l'activité et les préférences des utilisateurs.

Microsoft Bing

Avec 3,75% du marché Français, Bing, le moteur de recherche de Microsoft, est le deuxième moteur de recherche le plus utilisé, très loin derrière Google. Basé sur le même modèle que ce dernier, il utilise son écosystème (compte Microsoft, Windows, etc.) pour collecter un grand nombre de données sur ses utilisateurs afin d'améliorer sa régie publicitaire.

Yahoo !

Depuis son rachat par Verizon en 2017, Yahoo! tend à améliorer la pertinence de ses résultats. Pour ce faire, l'entreprise a optimisé sa stratégie en matière de traçage publicitaire et cherche à puiser des données dans les services qu'elle propose. Elle a notamment été poursuivie pour le scan des emails passant par son service de messagerie afin de classer les utilisateurs dans des catégories publicitaires.

MOTEURS DE RECHERCHE ALTERNATIFS

Qwant, le moteur de recherche français

La protection de la vie privée est l'atout majeur de Qwant. Créée en 2013, l'entreprise applique la philosophie inverse de Google en s'engageant contre le fichage des internautes et les résultats trop personnalisés. Ainsi, Qwant a mis son code source à disposition de la CNIL pour afficher ses bonnes intentions. La publicité est présente mais limitée à deux annonces par page au maximum et les utilisateurs ne sont pas ciblés.

De plus, Qwant a développé sa propre indexation des pages Web qu'il combine avec d'autres sources de résultats externes au moyen d'algorithmes de classement qui s'améliorent au cours du temps.

Il offre des résultats « neutres » en respectant la vie privée. Son panel de services ne cesse de croître. Le moteur de recherche français apporte donc des informations pertinentes, sans ajout de filtre fondés sur les données personnelles de ses utilisateurs.

Les moteurs de recherche

DuckDuckGo

Le moteur de recherche américain DuckDuckGo se veut radicalement « anti-fichage » des utilisateurs. Depuis sa création en 2008, il s'applique à ne jamais enregistrer les données privées des internautes et à ne pas cibler ses résultats. Les publicités, également non ciblées, sont discrètes : DuckDuckGo n'en affiche jamais plus de deux par page de résultats. Le site protège la vie privée, avec un bémol cependant puisque la société, localisée aux États-Unis, tombe donc sous le coup de la loi américaine qui peut imposer de communiquer des données aux autorités

Alors qu'elle n'était à l'origine qu'un agrégateur de moteurs de recherche, l'entreprise a développé son propre algorithme d'indexation, le DuckDuckBot. Ceci la hisse au rang de moteur de recherche « hybride ». Possédant sa propre base de données, DuckDuckGo s'appuie également sur plus de 400 sources externes dont Wikipédia, Yelp, Bing, Yahoo ou encore Yandex.

CONCLUSION

Facilitée par le développement des technologies, le big data, le machine learning, l'intelligence artificielle, la collecte d'information est omniprésente et inhérente à toute activité numérique. Dans le monde économique *a fortiori,* la recherche d'une information rapide et précise est encore plus primordiale.

Aussi, le choix du « meilleur » moteur de recherche consiste-t-il à fixer le curseur entre le respect de sa vie privée et la pertinence des résultats obtenus. Il appartient donc à l'utilisateur de recourir au moteur de recherche le plus adapté au regard des enjeux de la protection des données face à la pertinence des requêtes.

Les moteurs de recherche

Dites nous qui vous êtes ?

	Google	Bing	Yahoo !	Qwant	DuckDuckGo
Organisme	Google	Bing	Yahoo !	Qwant	DuckDuckGo
Parts de marché	92 %	3,75 %	1,37 %	0,98 %	0,51 %
Nationalité					
Localisation des serveurs					
Source des résultats	Indexation Google	Indexation Bing	Indexation Yahoo	Indexation Qwant combinée à Bing	Indexation DuckDuckGo combinée à plus de 400 sources (Yahoo, Yandex, Yelp, Wikipedia, Bing...)
Données collectées	Données de navigation. Données personnelles Géolocalisation. Centres d'intérêt. remontées de puis diverses sources (Youtube, Android, etc.)	Données de navigation. Données personnelles. Informations de navigateur. Géolocalisation. Centres d'intérêt. Remontées depuis l'écosystème Microsoft (Windows...)	Données de navigation. Données personnelles. Informations de navigateur. Géolocalisation. Centres d'intérêt. Remontées depuis l'écosystème Yahoo (Yahoo mail, Verizon...)	Mots clefs saisis. Informations sur le navigateur. Langue. Empreinte numérique de l'adresse IP (pseudonyme) Zone géographique. Pas de tracking publicitaire	Recherches anonymisées. Ne collecte pas d'informations personnelles. Pas de *tracking* publicitaire.
Conservation des données	Jusqu'à suppression par l'utilisateur. Adresses IP 9 mois. Données de traçage publicitaire 18 mois.	Aussi longtemps que nécessaire. Suppression de l'adresse IP après 6 mois. Suprression des données permettant l'identification après 18 mois	Données de recherche : 18 mois. Données personnelles : 18 mois à compter de la clôture du compte.	Conservation des données associées à un pseudonyme 7 jours, puis 12 mois après anonymisation.	Non communiqué.
Exploitation des données	Publicitaire et pertinence	Publicitaire et pertinence	Publicitaire et pertinence	Statistiques globales	Statistiques globales
Pertinence des résultats	★★★	★★		★	
Respect de la vie privée	★			★★	★★★
Protection des données	★			★★★	★★

Contrôle des exportations chinoises

Nouvelle loi et nouveaux risques pour les entreprises françaises

Depuis 2018, les relations entre la République populaire de Chine (RPC) et les États-Unis ont été marquées par une escalade de tensions. La guerre commerciale et juridique entre les deux pays s'est manifestée par une accumulation de sanctions économiques, commerciales et diplomatiques, comprenant notamment l'adoption de nouvelles législations et réglementations à portée extraterritoriale.

La promulgation par l'Assemblée nationale populaire (ANP) chinoise d'une nouvelle loi sur le contrôle des exportations de biens et technologies sensibles s'inscrit dans cette dynamique de bipolarisation entre les États-Unis et la Chine. Adoptée le 17 octobre 2020 et entrée en vigueur le 1er décembre 2020, cette loi clarifie le cadre juridique en la matière et s'inscrit dans la stratégie globale du gouvernement chinois de renforcer son arsenal législatif afin de se doter de dispositifs à portée extraterritoriale.

L'article 2 de la loi chinoise dispose que **la RPC pourra restreindre, voire interdire, l'exportation des « articles contrôlés »** *(controlled items)*[1] figurant sur **les listes des biens et technologies sensibles** *(« control lists »)* publiées et mises à jour par les autorités chinoises[2]. Ce contrôle **concernera tout transfert hors de la RPC** d'un article contrôlé, mais également **la fourniture de tout article contrôlé à des personnes physiques ou morales étrangères, y compris les transferts sur le territoire chinois** vers des personnes étrangères[3]. En outre, le transfert d'un « article contrôlé » chinois, même s'il se déroule sur le territoire français, tombera également sous le contrôle chinois[4].

Ces dispositions extraterritoriales sont spécifiquement **conçues en miroir des lois et réglementations américaines** de contrôle des exportations[5]. **Elles offrent ainsi un nouvel outil politique aux autorités chinoises, justifiant l'imposition de conditions, voire le refus,** de certaines exportations vers l'étranger pour des raisons de sécurité et d'intérêt nationaux. Les biens, les services et les technologies sensibles sont concernés y compris les algorithmes, les drones ou encore la 5G, domaine dans le lequel la Chine est leader. La liste n'est pas encore arrêtée et les contrôles vont s'intensifier.
En conséquence, le gouvernement chinois pourra **imposer des mesures de rétorsion sur des technologies particulières pour lesquelles la RPC dispose d'avantages comparatifs de niche**, notamment à l'encontre de certains pays qui agiraient au détriment des industriels chinois[6].

[1] Les articles (biens, technologies, services, données techniques…) contrôlés par la loi couvrent : les articles à double usage, les articles militaires, les articles à usage nucléaire, et tout autre bien, technologie, service, ou article qui peuvent être liés à la préservation de la sécurité nationale et des intérêts nationaux chinois.
[2] Le système de contrôle des exportations sera supervisé par le Conseil des affaires d'État et la Commission militaire centrale de la RPC.
[3] Cette définition très large reprend le concept américain « d'exportation présumée » *(« deemed export »)* inscrit dans la réglementation de contrôle des exportations des biens à double usage *Export Administration Regulations* (EAR).
[4] Article 44 de la loi.
[5] La loi *Arms Export Control Act* (AECA) et sa réglementation de mise en œuvre *International Traffic in Arms Regulations* (ITAR) pour ce qui concerne le contrôle des exportations d'articles à usage militaire, et la loi *Export Controls Act* (ECA) et sa réglementation de mise en œuvre *EAR* pour ce qui concerne le contrôle des exportations de biens à double usage.
[6] Article 48 de la loi.

Contrôle des exportations chinoises

Nouvelle loi et nouveaux risques pour les entreprises françaises

Si les modalités d'application de ces nouvelles mesures restent encore incertaines, l'extension de la sphère d'influence économique et commerciale de la Chine, notamment dans le cadre des nouvelles routes de la soie (Belt and Road Initiative), lui permettra de disposer d'outils puissants pour mobiliser son droit hors de son territoire. Cette nouvelle loi sur le contrôle des exportations représente une nouvelle contrainte réglementaire pour les entreprises françaises qui s'approvisionnent en biens intermédiaires et technologies stratégiques en Chine.

Face à cette nouvelle contrainte législative qui affecte l'ensemble des transferts impliquant une entité chinoise, il convient d'assurer une veille spécifique tenant compte des dernières évolutions juridiques et réglementaires chinoises.

Sur le site du Ministère des armées, une page spécifique vous donne accès à des agents pour vous accompagner dans vos démarches, que vous trouverez ci-dessous :

PROCÉDURE ET INFORMATIONS

- **Informations sur les opportunités à l'international :** faire sa demande sur démarches simplifiées

  https://www.demarches-simplifiees.fr/commencer/minarm-entreprises

- **Informations sur les procédures de contrôle des exportations d'armement :** email à envoyer à yves.mauboussin@intradef.gouv.fr

- **ART 90 :** dossier à télécharger sur ixarm :

  https://www.ixarm.com/fr/soutien-financier-aux-exportations

  puis à renvoyer complété à dga-di-article90.contact.fct@intradef.gouv.fr

- **Les aides individuelles directes :** formulaire à demander à sylvie.petitimbert@intradef.gouv.fr

- **Le label « UAF » :** demande à adresser à dga.pme.fct@intradef.gouv.fr

PME-ETI, LE MINISTÈRE DES ARMÉES EST À VOTRE ÉCOUTE

0 800 02 71 27

Appel gratuit

Ou https://www.demarches-simplifiees.fr/commencer/minarm-entreprises

Un agent du ministère des Armées prendre en charge votre demande en toute confidentialité et jusqu'à son terme.

Lutte anti-drones :

Des risques et des menaces

Une alarme retentit dans le poste de sécurité : un objet volant de petite taille a été détecté à quelques mètres des clôtures de l'entreprise. Les agents de sécurité de permanence transmettent l'alerte à leur supérieur hiérarchique. Après analyse rapide, ce dernier est catégorique : il s'agit d'un drone de loisir volant à basse altitude. L'axe de progression de l'objet laisse présager un survol de l'entreprise et de l'ensemble des infrastructures d'ici à peine quelques minutes, tout juste le temps de se préparer, d'informer la direction sûreté ; voire de l'intercepter. En application des règles en vigueur, décision est prise de neutraliser le drone par brouillage via les antennes implantées sur le site.
Mais alors que l'opérateur active le brouillage, le drone poursuit tout de même sa progression. En urgence, un second équipier armé d'un autre brouilleur se place au niveau de la clôture intérieure afin de neutraliser le drone. Le brouillage n'a de nouveau aucun effet sur le drone.
Malgré la mise en œuvre de ces moyens de neutralisation, le drone survole plusieurs zones sensibles de l'emprise. L'objet disparaît sans difficulté, sans qu'aucun télé pilote n'ait pu être localisé malgré les patrouilles effectuées par les équipes de sûreté/ sécurité.

Analyse de la menace

En l'état actuel de la technologie, le cas présenté ci-dessus ne relève pas de la science-fiction. Un tel enchaînement de faits peut se reproduire dans n'importe quelle emprise de la sphère défense, militaire ou civile. Les potentielles menaces engendrées par l'approche et l'intrusion d'un drone (terrorisme, espionnage, subversion, etc.) n'ont pas pu être entravées par les contre-mesures déployées sur le site.
L'évolution rapide des capacités techniques des drones permet à des individus disposant de compétences assez basiques de diriger un vol de drone sans connexion entre ce dernier et une télécommande. Les systèmes de brouillages, dont le principe est de rompre la liaison entre le drone et la télécommande pour le faire chuter ou atterrir en urgence, sont donc de facto inefficaces. Un tel drone ainsi configuré peut donc ainsi effectuer un vol sans être inquiété et atteindre l'objectif fixé par son propriétaire (largage d'un engin explosif, captation d'images et de vidéos, etc.).
Faute de pouvoir identifier les individus mettant en œuvre le drone, et l'appareil n'ayant pu être récupéré, il est impossible de déterminer leurs motivations : repérage en vue de réaliser une action malveillante, espionnage via la transmission en temps réel des images captées par la caméra dont le drone est équipé, etc.
Dans la perspective de l'organisation de la coupe du monde de rugby en 2023 et des Jeux Olympiques de Paris en 2024, les menaces liées aux survols de drones peuvent s'avérer prégnantes.

Perspectives dans la lutte anti-drones

Les technologies de lutte anti-drone (LAD) sont un domaine d'activité particulièrement dynamique. Plusieurs solutions ont aujourd'hui été développées et testées avec un taux de réussite plus ou moins satisfaisant.
Première étape, la détection des drones de loisirs demeure difficile[1], notamment en raison de leurs faibles surface équivalente radar (SER) et altitude de vol.
Par ailleurs, comme évoqué, le brouillage offre quelques lacunes : certains drones du commerce pouvant être programmés pour réaliser un circuit de manière autonome et revenir à leur base sans interaction avec un télé-pilote, ce qui rend le brouillage inefficace.

[1] Olivier DUJARDIN, « Pourquoi les radars ont-ils des difficultés à détecter les drones ? », Note renseignement, technologie et armement n°32/juin 2021, CF2R.

Lutte anti-drones :

Des risques et des menaces

De plus, parce que certains drones disposent de technologies capables de transmettre des données à distance en temps réel, la neutralisation et la récupération du drone n'empêchent pas la captation d'informations sensibles.

S'agissant des essaims de drones, bien que réservée encore aujourd'hui à quelques organisations détenant un savoir-faire complexe et des moyens techniques conséquents, cette capacité[2] est de plus en plus accessible et représente une menace et un défi supplémentaire.

Une attaque à caractère terroriste avec des drones de loisirs est ainsi tout à fait possible, même en l'absence de moyens et de compétences très pointus. En avril dernier, les cartels de la drogue mexicains ont attaqué des forces de sécurité nationales en employant des drones remplis d'explosifs[3].

Face aux difficultés des fusils brouilleurs, les armes à énergie dirigée (AED), notamment laser et à micro-ondes, peuvent sembler une solution. Plusieurs pays (États-Unis, Israël, etc.) et entreprises (*BAE Systems, Verus Research*, etc) investissent dans ces technologies. Elles permettraient d'éviter l'usage d'armes à feu (fusil à pompe), qui représentent actuellement le dernier recours en termes de LAD, notamment en dehors du territoire national.

En France, plusieurs acteurs investissent au profit d'une solution AED française. En juillet 2021, Mme Florence Parly, ministre des armées, a assisté à la démonstration du système Helma-P, développé par la société CILAS et qui devrait être opérationnel d'ici 3 ans ; la plupart des industriels envisageant des systèmes opérationnels pour 2024.

En outre, certaines contraintes, notamment juridiques, subsistent concernant la destruction d'un bien appartenant à autrui ou le risque de blessures causées à un tiers résultant de la chute du drone.

Recommandations

Comme évoqué, il n'existe pas de solutions techniques 100% satisfaisantes pour se prémunir d'une menace drone pourtant bien réelle.

Aussi convient-il de s'appuyer sur une combinaison judicieuse de moyens déjà existant en évitant les surcoûts.

Si la vidéosurveillance et certains systèmes de détection peuvent aider à déceler une menace, ils ne remplacent pas la vigilance humaine du personnel de sûreté et de l'ensemble des salariés qui doivent être sensibilisés à cet égard au travers de mises en situation concrètes.

Il est conseillé de relever le maximum de détails possibles tels que les horaires, le nombre, la marque et le type de drone, la trajectoire et la direction, l'altitude, la présence d'équipements (caméra, lumières…), etc.

Il convient, par ailleurs, de signaler systématiquement tout type de survols de drone à vos correspondants DRSD et de porter plainte auprès des services de police et de gendarmerie.

Si l'activité de votre entreprise nécessite un jour de recourir à une prestation de services mettant en œuvre des drones, il est préférable de bien cadrer contractuellement l'exercice tout comme de tenir informé votre voisinage professionnel.

[2] Spectacles aériens lumineux pour l'ouverture des Jeux Olympiques d'hiver en Corée du Sud en 2018 et pour le Nouvel An en Chine en 2020, et usage militaire dans le Haut-Karabakh dès 2020.

[3] https://www.20min.ch/fr/story/les-cartels-attaquent-avec-des-drones-641890069041

Gardons contact

De l' IGI 1300 revue à la future IM900 très attendue : l'adaptation transitoire de la procédure relative aux ATAP

La protection du secret de la défense nationale (PSDN) connait depuis le 13 novembre 2020 des évolutions majeures dont la déclinaison règlementaire au niveau du ministère des Armées se traduira par l'émission prochaine d'une nouvelle version de l'IM 900 tenant compte de certaines spécificités, contraintes et préconisations des acteurs de la base industrielle et technologique de la Défense (BITD).

Ce nouveau cadre règlementaire, en voie de finalisation , ne révolutionne pas pour autant les fondements et principes de la PSDN mais implique toutefois depuis le 9 août 2021, des obligations notables pour les établissements détenteurs d'informations sur support classifiés (ISC). Ces derniers ont ainsi l'obligation de produire une analyse de risque dont la réalisation est un des critères examinés pour la délivrance d'un avis technique d'aptitude physique (ATAP) qualifiant les locaux prévus d'abriter des ISC. Si l'annexe 30 de l'IGI 1300 précise que cette analyse de risque peut être réalisée « le cas échéant » par le service enquêteur, cette disposition, répondant aux besoins d'un autre ministère, ne s'applique pas aux entreprises de défense lesquelles restent responsables de la réalisation de ces analyses.

Ce faisant, considérant les situations et niveaux d'acculturation disparates des entreprises relevant de la BITD pour produire leur analyse de risque, une phase transitoire à fin d'adaptation peut être mise en œuvre par la DRSD à la demande de l'industriel. Déterminée en concertation avec l'agent référent de la DRSD, cette phase, n'excédant pas deux ans, donnera lieu à l'émission d'un ATAP avec réserve. Sans constituer un obstacle à la détention d'ISC, l'ATAP avec réserve formalisera ainsi l'absence d'une analyse de risque et l'engagement de l'établissement à produire ce document dans un délai fixé par la DRSD en concertation avec l'officier de sécurité. L'examen de l'analyse de risque à l'issue de ce délai permettra ensuite de lever la réserve temporaire en validant définitivement l'ATAP.