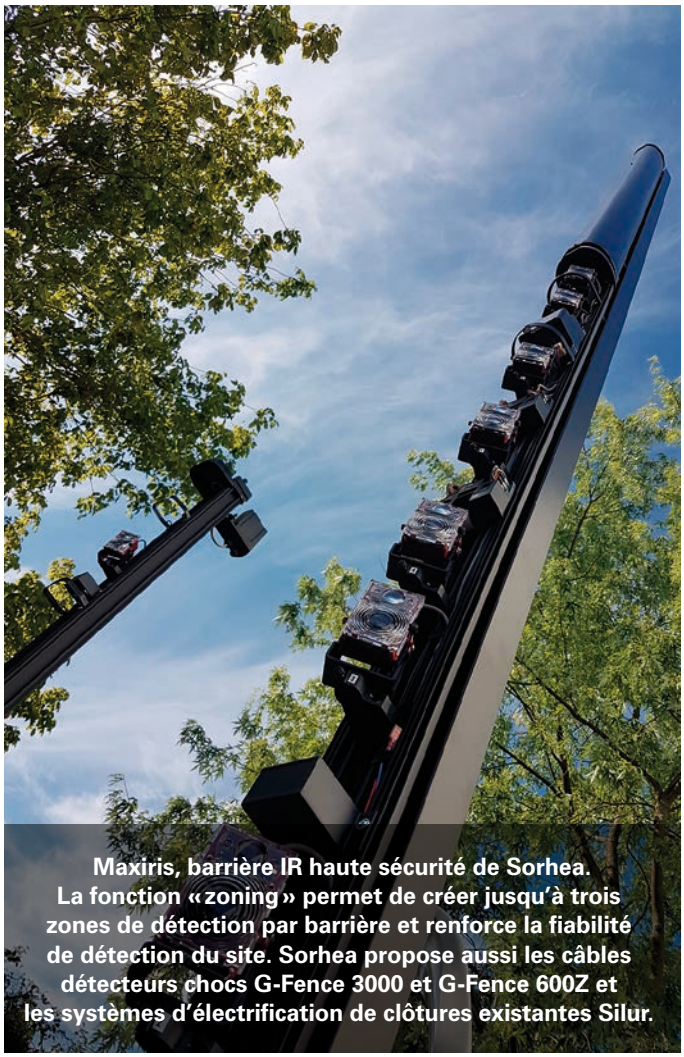
Détection intelligente ou association de technos ?

Dans la détection d'intrusion, l'ennemi – outre l'intrus évidemment – est l'alarme intempestive, la fausse alarme… Grâce à des solutions de plus en plus intelligentes – et associant souvent différentes technologies – les fabricants proposent des systèmes de plus en plus fiables.

Comme pour d'autres applications sécurité, les caméras, à en croire certains, seraient capables aujourd'hui, grâce à leur intelligence embarquée, de remplacer aisément des solutions de détection d'intrusion traditionnelles, intelligentes ou pas. Dans certains cas, c'est sans doute possible. Mais généraliser la chose serait ne pas tenir compte des technologies développées par les fabricants de solutions anti-intrusion qui, elles-aussi, peuvent faire preuve d'intelligence.
« L'intelligence vidéo semble être, pour beaucoup de professionnels de la sécurité, la panacée en matière de détection d'intrusion intelligente, constate Thomas Wolski, Product & Integration Partner Program Marketing Manager BU Security. *Or, les détecteurs d'intrusion sont eux aussi de plus en plus intelligents, pointus… afin d'améliorer leurs performances en matière de détection et de réduire les fausses alarmes dues à des événements extérieurs comme les animaux, un ventilateur qui fonctionne, un courant d'air, l'environnement naturel, etc. Aujourd'hui, la qualité des firmwares intégrés dans les détecteurs permet de réaliser une bien meilleure analyse des vraies et des fausses alarmes. »*

Réduire les fausses alarmes

« Dans l'intrusion, le nerf de la guerre est la capacité de faire remonter rapidement une alarme fiable, tout en limitant les coûts qui peuvent être induits par les fausses alarmes et les déclenchements intempestifs, explique Nicolas Picard, directeur général adjoint de Sorhea. *Longtemps, la barrière infrarouge, le cœur de notre métier, a été la seule réponse technologique à la détection intrusion périmétrique. Aujourd'hui, en raison de la puissance marketing des géants de la vidéosurveillance, les caméras infrarouges se positionnent très clairement comme une alternative à la barrière IR. Or, si les caméras IR peuvent être en effet efficaces en matière de détection d'intrusion intelligente, cela ne sera possible que si elles intègrent de l'analytique fiable. Ce qui n'est pas toujours – loin de là – le cas. Et on se retrouve avec le problème récurrent de l'anti-intrusion : les fausses alarmes… »*
« Pour réduire au maximum le risque de fausses alarmes, il est également possible d'ajuster le degré de sensibilité de détection afin de réduire au maximum le risque de fausses alarmes, de masquer des zones de non-déclenchement (arbres, buissons…), ajoute Pascal Dugast. *Nous avons développé un outil de paramétrage, avec capture d'image, pour nos installateurs, qui garantit l'exacte positionnement du détecteur et de sa caméra embarquée. »* Les fausses alarmes ont toujours été, et sont en-



Maxiris, barrière IR haute sécurité de Sorhea. La fonction « zoning » permet de créer jusqu'à trois zones de détection par barrière et renforce la fiabilité de détection du site. Sorhea propose aussi les câbles détecteurs chocs G-Fence 3000 et G-Fence 600Z et les systèmes d'électrification de clôtures existantes Silur.

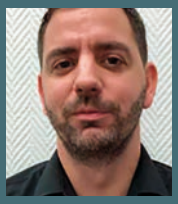
© Sorhea

« En réglant finement la sensibilité et le zoning de nos barrières, nous atteignons des taux de fausses alarmes très bas. »

NICOLAS PICARD, DIRECTEUR GÉNÉRAL ADJOINT CHEZ SORHEA.

LE POINT DE VUE D'UN FABRICANT

ANTHONY GONZALEZ
Référent technique sécurité électronique chez Abus France


© DR

« NE PAS SE LIMITER À LA PÉRIMÉTRIE DU SITE. »

« La détection d'intrusion intelligente ne se limite pas à la périmétrie d'un site. Chez Abus, nous combinons des cylindres électroniques et de l'alarme. Concrètement, quand quelqu'un se présente devant la porte, notre solution, qui s'intègre dans un ensemble plus vaste de contrôle d'accès et de vidéosurveillance, permet ainsi de vérifier, via une caméra asservie, qui il est. Dans les faits, notre solution est donc une combinaison de trois produits : cylindre, alarme et vidéosurveillance connectés entre eux. »

Le capteur thermique de la caméra IP TPC-BF2221 de Dahua permet une détection d'intrusion et fournit un résultat pratiquement identique quelles que soient les conditions.

© Dahua

core, le principal problème de la lutte contre l'intrusion. *« Il faut comprendre que le faux positif est natif à l'environnement de la sécurité,* insiste Xavier Féry, président directeur général de Komanche. *Que le seul moyen de le réduire, de l'éliminer, et de faire de manière fiable de la sécurité est de raisonner en termes d'intégration complète. »*

Marier les technologies

C'est l'association de différentes technologies qui rendra plus sûre la détection. *« Intelligence ou pas, il faut associer des moyens technologiques différents pour parvenir à une détection très fine et au maximum exempte de fausses alarmes et autres déclenchement intempestifs,* conseille Servan Lépine, dirigeant d'Excelium. *On pourra associer barrières physiques, détection enterrée, câbles détecteurs de chocs, vidéosurveillance, barrières IR, hyperfréquence... afin de limiter le volume d'alarmes intempestives. »* Point de vue que partage Anthony Gonzalez, référent technique sécurité électronique chez Abus France : *« L'association de différentes technologies est toujours un plus en matière de lutte contre l'intrusion. La combinaison de barrières électroniques ou infrarouges, avec des détecteurs de mouvements et d'ouverture, permet de croiser les technos et d'être plus efficace. »*

Pour Thomas Wolski également, la combinaison des technologies est pertinente. Et les caméras en font partie. *« Nous sommes aujourd'hui capables d'associer différentes technologies dans les détecteurs d'intrusion pour atteindre des taux d'immunité aux fausses alarmes très satisfaisants. Cependant, la vidéo nous permet de voir ce qui se passe sur le site et nous simplifie la levée de doute. »*

Chez Daitem, on combine aussi détection et intrusion. *« Nous avons développé un détecteur de mouvement double IR (PIR) à capture d'image,* explique Pascal Dugast. *Avec un angle de détection orientable de 90°, il est capable de repérer une* ● ● ●

« Les détecteurs d'intrusion sont eux aussi de plus en plus intelligents, pointus... »

THOMAS WOLSKI, INGÉNIEUR AVANT-VENTE/CHARGÉ DE PROJETS CCTV IP CHEZ BOSCH SECURITY SYSTEMS.

LE POINT DE VUE D'UN FABRICANT

XAVIER FÉRY
PDG de Komanche


© DR

« L'AVENIR DE L'INTRUSION ? LES OBJETS CONNECTÉS. »

« Notre objectif est d'intégrer ou de développer une chaîne de valeur dans laquelle chaque élément est constitué d'intelligence et de sécurité. Cette solution constituée de caméras "K safe" utilise des blocs et optiques certifiés CCC (Common Critéria Certification), elle-même fluidifiée et protégée par son nouveau VMS français "KxvKorp", chiffré en AES 256. Ce VMS, permet de gérer jusqu'à 50 NVR ou 1 000 caméras. Doté d'une supervision native, il permet également de générer et de superviser un journal des alarmes, de faire de la détection de mouvements avancés, de reconnaissance d'objets (véhicules ou personnes), de gestion de lignes ou de détection de couleurs. La supervision permet également de surveiller en temps réel les déclenchements d'alarmes et de visualiser les séquences vidéo associées, même à distance. C'est de cette manière que chaque brique de Komanche réellement intégrée optimise et fluidifie la sécurité des solutions de vidéoprotection tout en optimisant les critères de DAI, par le fait que chaque couche d'intelligence et de sécurité se parlent les unes aux autres. »

En fonction de l'activité du site, des saisons et/ou des conditions météorologiques, les paramètres de détection devront être ajustés pour limiter les détections intempestives.

© Excelium

présence jusqu'à 15 mètres. Il envoie alors une alarme et une séquence d'images consultables sur portable ou tablette, afin d'effectuer une levée de doute.»

Les caméras : une vraie alternative ?

Nombreux sont ceux qui répondent oui. Mais à condition d'être conscients de certaines contraintes et limites. *«Grâce à notre capacité de régler très finement la sensibilité et le zoning de nos barrières infrarouges et de nos câbles à détection de chocs, nous parvenons à atteindre des taux de fausses alarmes très bas,* indique Nicolas Picard. *La question n'est pas tant de savoir si la détection doit être intelligente. Il faut plutôt se demander quels sont les moyens techniques de la rendre plus efficace. Pour cela, le plus efficace est d'associer différentes technologies.»* Avant de poursuivre : *«En ce qui concerne l'alternative que constituent les caméras, il ne faut pas perdre de vue le fait que le coût d'acquisition et de maintenance de ces dernières peut être élevé, voire rédhibitoire pour certains sites. Ce qui n'est pas le cas pour nos solutions de détection d'intrusion et notamment le câble à détection de chocs pour les grands périmètres.»*

Pour d'autres, combiner les technologies ne suffit pas. C'est le cas de Xavier Féry qui conclut : *«On entend beaucoup parler de détection d'intrusion intelligente avec des moyens classiques de l'anti-intrusion ou grâce aux caméras dites intelligentes. Dans cette approche, on organise que la cohabitation de modules différents. Or, tout cela n'est pas efficace. Ces différents systèmes se contentent de cohabiter mais ils n'interagissent pas dans un environnement qui ferait que chaque brique vient renforcer l'autre. Il faut que les différentes couches soient totalement intégrées. Par ailleurs, au risque de faire hurler certains de mes confrères, la plupart des solutions de DAI (détection automatique d'incidents) est perturbée par 20 à 30 % de faux positifs.»* ■

2 QUESTIONS À

SERVAN LÉPINE

Dirigeant d'Excelium

© DR

La détection par l'image est-elle la panacée en matière de lutte contre l'intrusion ?

Elle a des avantages certains mais son efficacité dépend de la qualité des algorithmes et de l'évolution de l'environnement dans lequel elle est déployée. Ce type de détection est programmée pour des zones précises, selon certains paramètres. Pour maintenir son efficacité, elle requiert un pilotage actif afin d'ajuster ses paramètres selon les saisons, les évolutions du site, etc.

Avec les solutions de plus en plus intelligentes qui constituent l'écosystème de la lutte contre l'intrusion, l'homme a-t-il encore un rôle majeur à jouer ?

Évidemment. Les technologies les plus intelligentes actuellement nécessitent encore un opérateur compétent, aguerri, formé pour interpréter les informations transmises par les détecteurs, quels qu'ils soient. L'opérateur est encore utile pour effectuer la levée de doute et pour gérer ou ajuster les paramètres des moyens de détection. De toute manière, il n'y a pas de recette miracle en détection d'intrusion. Même le deep learning doit apprendre constamment. Il faut associer les technologies afin que les défaillances de l'une soient corriger par les autres, car chaque technologie a ses vulnérabilités.

LE POINT DE VUE D'UN FABRICANT

DIDIER DUHAUBOIS

Ingénieur support technique chez Dahua

© DR

«LE THERMIQUE EST UNE SOLUTION PERTINENTE.»

«Les caméras peuvent venir en soutien d'une installation anti-intrusion "classique". Ainsi, notre caméra IP TPC-BF2221 est équipée de deux capteurs (utilisant le spectre visible et thermique) permettant, à l'aide de la fonction de détection vidéo intelligente (IVS), de détecter des objets en mouvement et de les classifier à l'aide de la fonction AI Perimeter selon leur type (humain, véhicule, etc.) afin de créer une alerte uniquement sur le type d'objet souhaité. Elle est, en plus, équipée d'un flash et d'un haut-parleur pour informer l'intrus de sa détection. L'utilisation d'un capteur utilisant le spectre thermique est une solution très pertinente en extérieur pour réaliser une détection d'intrusion, car elle fournit un résultat pratiquement identique quelles que soient les conditions (jour, nuit, brouillard, etc.) contrairement à une détection par un capteur utilisant le spectre visible tributaire du niveau de luminosité.»