psm

PROTECTION SÉCURITÉ MAGAZINE

LES SOLUTIONS POUR LES PROFESSIONNELS DE LA SÛRETÉ – SÉCURITÉ

N° 279
SEPT. / OCT. 2023
28 €

CE NUMÉRO COMPREND LE GUIDE D'ACHAT ANNUEL 2024

ENTRETIEN

PIERRE LIOT DE NORTBÉCOURT
VICE-PRÉSIDENT SECURITY & COMPETITIVE INTELLIGENCE, GROUPE DANONE

VIDÉOSURVEILLANCE

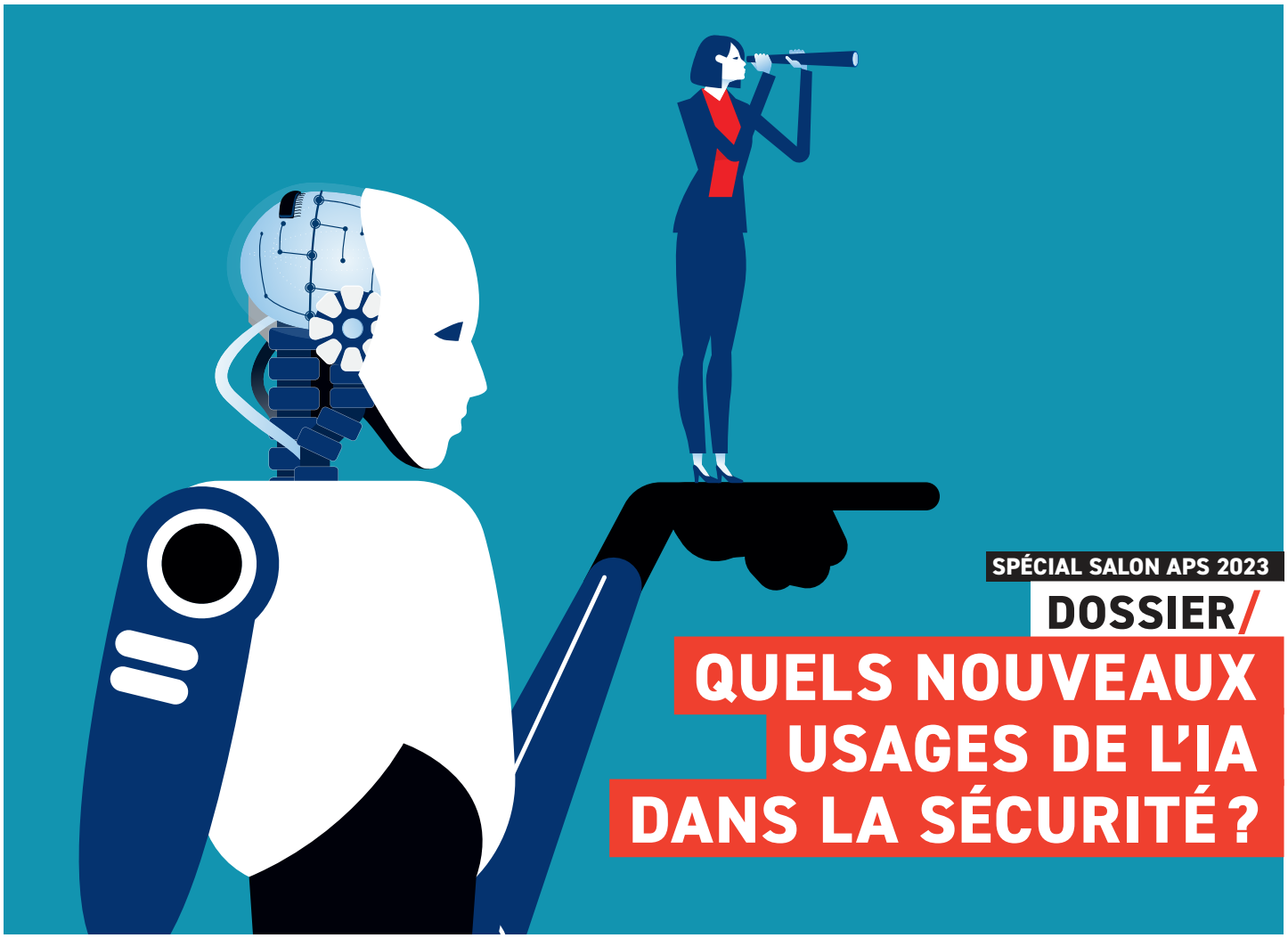
CAMÉRAS ATEX
POUR FAIRE BIEN PLUS QUE DE LA SURVEILLANCE!

CONTRÔLE D'ACCÈS

LES SYSTÈMES AUTONOMES
LEUR POTENTIEL SERAIT-IL ENCORE SOUS-EXPLOITÉ ?

INTRUSION

GÉNÉRATEURS DE BROUILLARD
EFFICACES, MÊME DANS LES GRANDS VOLUMES !



SPÉCIAL SALON APS 2023

DOSSIER/

QUELS NOUVEAUX USAGES DE L'IA DANS LA SÉCURITÉ ?

DOSSIER/

SPÉCIAL SALON APS

QUELS NOUVEAUX USAGES DE L'IA DANS LA SÉCURITÉ ?

SOMMAIRE/

1/ DÉPASSIONNONS LE DÉBAT ET SOYONS PRAGMATIQUES ! P. 30

2/ ON SAIT DÉJÀ CE QUI DEVRAIT ÊTRE INTERDIT DEMAIN P. 32

3/ ET L'HUMAIN DANS TOUT ÇA ? P. 34

4/ DES USAGES ÉVIDENTS ET SURPRENANTS ! P. 36

5/ UN APPORT INDÉNIABLE EN MATIÈRE DE CYBERSÉCURITÉ P. 38

À l'occasion du salon APS, qui ouvrira ses portes à Paris le 3 octobre, il est pertinent de s'interroger sur les nouveaux usages de l'IA qui révolutionne – ou va révolutionner – le monde de la sécurité. Qu'on soit offreur ou utilisateur. Sous certaines conditions...

Getty Images

1/ DÉPASSIONNONS LE DÉBAT ET SOYONS PRAGMATIQUES !

Si comme toute technologie l'IA est en soi neutre, ses usages dans la sécurité suscitent des inquiétudes. Ils doivent être encadrés strictement pour permettre aux forces de sécurité d'être plus efficaces.

L'intelligence artificielle (IA) occupe d'ores et déjà une place prépondérante dans le monde de la sûreté-sécurité. Elle est utilisée pour analyser des données à des fins multiples : recherche d'individus, de véhicules, d'objets à partir de critères précis. Et ce, de manière excessivement rapide. Cela dit, le recours à l'IA ne va pas sans susciter de nombreux débats. Un exemple récent : les inquiétudes provoquées par l'usage des algorithmes des caméras à l'occasion de la Coupe du monde de rugby et, surtout, lors des Jeux olympiques de Paris, l'année prochaine.

« On peut comprendre que le recours à l'intelligence artificielle puisse susciter certaines inquiétudes, reconnaît Maître Alain Bensoussan. *Mais le débat autour des nouvelles technologies utilisées dans la sécurité-sûreté est pollué par les cas extrêmes en matière d'usage de ces outils dans certains pays. La technologie, en soi, est neutre. C'est l'usage qu'on en fait qui peut constituer le danger. Je pense qu'on doit raisonner en termes de bénéfices/risques. Il est indéniable que l'introduction de l'IA dans le monde de la sécurité permet de renforcer la sécurité et des biens et personnels, du public comme du privé, d'être plus efficaces. »*

DES DÉRIVES TOUJOURS POSSIBLES

Les gains induits par l'IA ne doivent pas cependant nous aveugler. Il ne faut pas sombrer dans l'angélisme. *« Comme toujours, quelle que soit la technologique, il existe des risques de dérives pour les libertés publiques et individuelles. Il faut donc mettre en place de garde-fous. Et sur ce point, la France, d'une part, et les autorités européennes, d'autre part, ont mis en place un corpus réglementaire qui permet d'encadrer les usages de l'IA pour garantir les libertés individuelles et collectives. L'exemple le plus récent est l'IA Act qui devrait contraindre les usages de l'IA,* ajoute Alain Bensoussan. *Même si, en ce qui concerne la biométrie en temps réel dans les zones publiques, je ne suis pas certain qu'on ait pris la bonne décision. L'IA Act veut l'interdire alors que je pense qu'il aurait mieux valu la surencadrer plutôt que de prohiber l'utilisation. »*

Du côté des entreprises, les directeurs sûreté sont aussi conscients des inquiétudes liées à l'IA. *« Globalement,*

3 QUESTIONS À...

FABRICE LOLLIA, RESPONSABLE SÉCURITÉ FRANCE CHEZ SIEMENS GAMESA, DOCTEUR EN SCIENCES DE L'INFORMATION ET DE LA COMMUNICATION

Quels sont les apports de l'IA pour les directions sûreté des entreprises ?

Elle nous permet d'être plus réactifs pour détecter des menaces éventuelles, grâce à ses capacités en matière de traitement de très grosses masses de données. Grâce à l'IA, il est ainsi possible de détecter des modèles de comportements anormaux comme ce sera le cas lors des JO de Paris. Elle nous offre aussi la possibilité d'automatiser certains process et de libérer du temps pour les personnels de sûreté en automatisant, par exemple, l'identification des personnes voulant accéder à un site. D'une manière générale, grâce aux données qu'elle fournit, elle nous aide à améliorer la prise de décision. Enfin, en matière de formation, on peut simuler des situations d'urgence. Tous ces usages sont un plus pour améliorer le cadre de la sûreté.

Doit-on craindre que la machine supplante l'homme ?

Pour que l'IA fonctionne et soit acceptée, il faudrait nécessairement maintenir la collaboration homme/machine. L'IA n'est pas là pour remplacer l'homme dans la prise de décision. Elle est et devra être un auxiliaire et demeurer un outil dont l'usage sera conforme au cadre réglementaire défini par les autorités. Évidemment, il sera nécessaire de former les opérateurs à son usage. Une fois cela posé, on pourra assurer, grâce à elle, une sûreté de haut niveau, où l'homme aura toujours, et en dernier recours, la main sur le système.

Existe-t-il d'autres problématiques pour lesquels l'IA sera un auxiliaire précieux pour les entreprises ?

En matière de cybersécurité, il est évident que l'IA devrait nous permettre de réagir quasi en temps réel lors des attaques cyber, mais aussi de les anticiper grâce à sa capacité de détecter des comportements anormaux sur les réseaux.

lorsque j'échange avec mes confrères, je constate que les gens sont plutôt pour l'IA. Tout en comprenant que ce sont certains de ses usages qui peuvent poser problème, reconnaît Fabrice Lollia, responsable sécurité France chez Siemens Gamesa. *La question est donc comment on l'utilise et comment on l'utilisera demain. Utiliser l'IA ne peut se faire sans garder à l'esprit certaines questions importantes: qui sera responsable en cas d'erreur de la machine ? Quels sont les biais introduits dans les algorithmes et qui peuvent induire des dérives, des erreurs ? Quid de la transparence les employés, les citoyens savent-ils quand et comment est utilisée l'IA et pour faire quoi ?»* ■

APS

APS PRATIQUE

DU 3 AU 5 OCTOBRE
PARIS – PORTE DE VERSAILLES
PAVILLON 5.2

Mardi 3 et mercredi 4 octobre de 9 heures à 18 heures et jeudi 5 de 9 heures à 17 heures

→ **Badge gratuit : www.salon-aps.com/fr-fr/participer.html**
→ **www.salon-aps.com**

PAROLE D'EXPERT

CHEMS AKROUF, ENSEIGNANT À L'UNIVERSITÉ PANTHÉON-ASSAS

« L'IA est une avancée majeure pour la sécurité urbaine. »

L'IA est déjà un outil indispensable à la sécurité-sûreté. Elle constitue, quoi qu'on en dise, une avancée majeure pour les centres de supervision urbaine (CSU) et pour la sécurité sur la voie publique. Elle permet de détecter des infractions, de verbaliser automatiquement, de fournir en temps réel des informations sur l'état du trafic et ainsi améliorer la gestion des flux dans une ville. Les données qu'elle fournit peuvent aussi être utilisées pour, *a posteriori,* adapter la voirie en fonction de sa fréquentation réelle. Pour la lutte contre la criminalité, elle est aussi très efficace pour rechercher des individus, non pas à partir de données biométriques, mais grâce à des critères «non intrusifs» comme la couleur d'un vêtement, d'un sac, d'une casquette…

2/ ON SAIT DÉJÀ CE QUI DEVRAIT ÊTRE INTERDIT DEMAIN

L'IA Act devrait permettre de définir la doctrine européenne en matière d'usages futurs de l'IA. Il en interdit certains très clairement. Pour mieux pousser le recours à une IA non intrusive ?

Dès qu'on parle d'IA, tout le monde pense reconnaissance faciale, identification des personnes, données biométriques… Tout cela parasite le débat, car l'IA permet de faire bien autre chose et d'utiliser son « intelligence » autrement. Aujourd'hui et encore plus, sans doute, demain. Chez Kooping, Marc Decombas, son président-directeur général et membre du pôle d'expertise Technologies numériques et innovations du GPMSE, ajoute : *« Les technologies et les usages de l'IA évoluent très vite. Il faut les encadrer. Mais est-ce possible ? Aujourd'hui, 400 millions de personnes utilisent quotidiennement ChatGPT. Comment la loi peut-elle faire pour suivre et encadrer un usage qui se généralise à ce point ? L'IA Act est une des réponses. »*

DES USAGES INTERDITS PAR L'IA ACT

L'IA Act a posé des limites importantes quant aux usages possibles de l'IA. Ainsi, selon ce texte, qui vient d'entrer dans sa troisième phase, *« les systèmes d'IA présentant un niveau de risque inacceptable pour la sécurité des personnes seront donc interdits, comme ceux qui sont utilisés pour la notation sociale (classifiant les personnes*

SPÉCIAL SALON APS 2023

CONTRÔLE D'ACCÈS : BIOSTAR2 DE SUPREMA

La plateforme de contrôle d'accès Biostar2 a obtenu les certifications ISO 27001 (sécurité) et ISO 27701 (protection des données personnelles), garantissant ainsi son haut niveau de protection contre les failles de sécurité et les vulnérabilités potentielles.

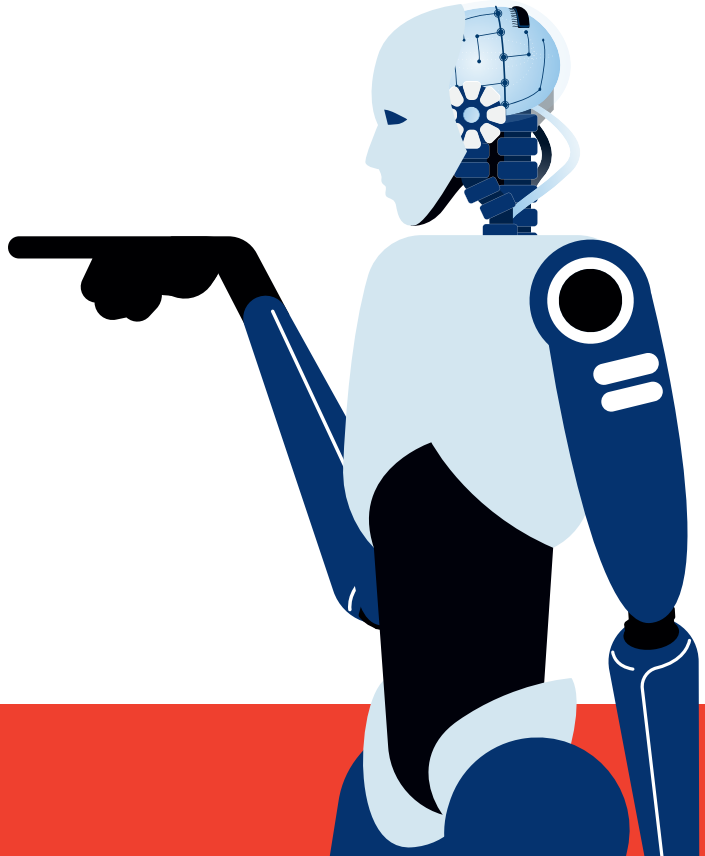
→ **Stand B10**

IA ET SÉCURITÉ

Marc Decombas animera une table ronde « Applications de l'IA dans les missions de sécurité ».

→ **le 4 octobre lors du salon APS**

> *« En matière d'IA dans la sécurité, il vaut mieux surencadrer certains usages plutôt que les interdire. »*
>
> MAÎTRE ALAIN BENSOUSSAN, AVOCAT.



en fonction de leur comportement social ou de leurs caractéristiques personnelles). » L'IA Act précise aussi ce qui devrait être interdit. Entre autres : les systèmes d'identification biométriques à distance en « temps réel » dans les espaces accessibles au public ; les systèmes d'identification biométrique à distance *a posteriori*, à la seule exception des forces de l'ordre pour la poursuite de crimes graves, et seulement après autorisation judiciaire ; les systèmes d'identification biométrique utilisant des caractéristiques sensibles (genre, race, statut, religion, etc.) ; les systèmes de police prédictive ; la saisie non ciblée d'images faciales provenant d'internet ou de séquences de vidéosurveillance pour créer des bases de données de reconnaissance faciale, etc. *« Tout cela, selon moi, va dans le bon sens, car il dit clairement ce qu'on peut accepter ou non. On ne peut faire ce que l'on veut avec l'IA et ce sont les usages qui définiront ce qu'on veut. Il faut dédramatiser le débat et expliquer à tout le monde que l'IA ne rime pas nécessaire avec biométrie. Et qu'il existe aujourd'hui des applications de l'IA non intrusives et qui permettront d'accroître la sécurité de tous »*, conclut Marc Decombas. ■

PAROLE D'EXPERT

MARC DECOMBAS, PDG DE KOOPING

« Nous arriverons nécessairement à du tracking, de la détection. »

L'IA Act va permettre de « verrouiller » le marché européen en ce qui concerne l'IA. Il sera nécessaire aux groupes anglo-saxons, asiatiques…, d'intégrer les contraintes imposées dans leurs solutions. Mais on ne pourra pas stopper le recours à l'IA. Notamment dans la sécurité. Mais l'IA Act va nous obliger à poursuivre nos efforts pour développer d'autres technologies, d'autres usages moins intrusifs que les applications biométriques de l'IA. Je pense que fondamentalement, on arrivera à des solutions de tracking, de détection… à l'instar de ce qui va être expérimenté lors des JO de Paris. Si cela fonctionne correctement. Le recours à l'IA en matière de biométrie doit être très strictement encadré et réservé à des cas de force majeure. Et dans des conditions, elles aussi, strictement définies.

2 QUESTIONS À...

FABIEN DHAINAUT, RESPONSABLE SÉCURITÉ DES PERSONNES ET DES BIENS, CAISSE D'ÉPARGNE HDF ET COPRÉSIDENT DE L'AGORA DES DIRECTEURS DE LA SÉCURITÉ

Dans quel cadre utilisez-vous l'IA ?
Il faut tout d'abord rappeler que nous n'en sommes encore qu'aux prémices en ce qui concerne les usages et les applications de l'IA dans le monde de la sûreté-sécurité. Cela dit, à la Caisse d'Épargne HDF, nous nous servons déjà de l'intelligence embarquée dans nos caméras Axis et systèmes vidéo pour expérimenter du comptage dans nos agences, analyser les flux de personnes, identifier les zones chaudes ou froides... Nos caméras nous permettent aussi de faire de la reconnaissance de véhicules pour identifier, par exemple, une voiture qui stationnerait plusieurs fois devant une ou plusieurs agences... Dans le cadre d'un pilote, nous utilisons aussi l'intelligence de l'ensemble de nos capteurs (caméras, audio, lumière...) pour la protection du travailleur isolé afin de détecter des chutes, des situations anormales, etc.

Avez-vous d'autres projets en matière d'IA ?
Un gros chantier tourne autour de l'usage des métadonnées. À ce sujet, nous échangeons beaucoup avec les équipes de fabricants –Azur Soft, Pryntec, Genetec, Axis– afin d'étudier l'adaptation de leurs solutions pour exploiter au mieux nos métadonnées. L'IA doit permettre aux directeurs sûreté de faire bien plus que de la simple hypervision. Il nous faut réfléchir à l'exploitation des métadonnées et leur analyse pour remonter des situations anormales, des signaux d'alerte pour éventuellement identifier des pistes d'amélioration ou adapter nos process sûreté. C'est sur ce type d'usage que je travaille afin de disposer plus rapidement des données de nos 380 agences dans les Hauts-de-France, pour être plus efficace, plus réactif et fournir, tous les trois mois, lors de notre «comité sécurité» un état des lieux en matière de risques et de ce que nous allons devoir traiter.

SPÉCIAL SALON APS 2023

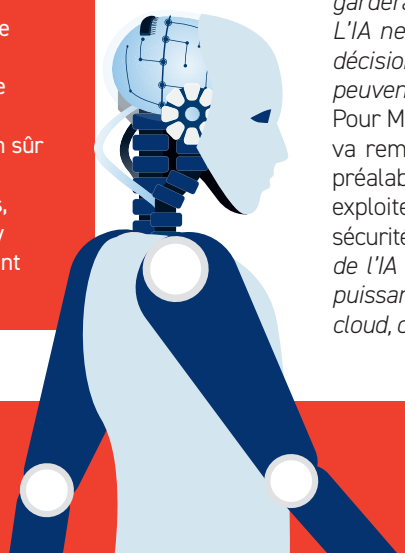
“ Des temps forts à ne pas manquer ! ”

JEAN-FRANÇOIS SOL DOURDIN, DIRECTEUR DU SALON APS

Cette édition réserve de nombreux temps forts autour de l'innovation et des grands enjeux métier avec la remise des Trophées APS mardi 3 octobre, le village des Start-up et le programme de conférences. À noter mardi 3, la session sur le protocole de sécurisation SSCP par la SPAC, mercredi, l'intervention d'AXA Climate sur les impacts du changement climatique ou jeudi un point sur la sécurité privée avec le GES. Une nouveauté cette année : les «parcours marchés» pour organiser sa visite autour de 18 marchés verticaux (administration publique, bancaire, éducation, santé, etc.). Et bien sûr le networking et la convivialité avec l'after-work mercredi 4 jusqu'à 20 heures Au menu: cocktails, animation musicale et Coupe du monde de rugby avec l'intervention de Marc Lièvremont, consultant et ancien sélectionneur du XV de France.

3/ ET L'HUMAIN DANS TOUT ÇA ?

Un grand nombre voit dans l'IA une menace pour la place de l'homme dans certains process. Avant de se poser cette question, demandons-nous si les infrastructures nécessaires à l'IA seront à la portée de tous ?



« *Dès qu'on parle d'IA, on fait peur. Et beaucoup se demandent si on aura encore besoin d'eux demain,* constate Marc Vaillant, président-directeur général d'Azur Soft et membre du GPMSE [Groupement professionnel des métiers de la sécurité électronique] et partenaire de l'Agora des directeurs de la sécurité. *Rassurons-les tout de suite, du moins en ce qui concerne le monde de la sécurité: c'est l'homme qui gardera la main sur le système et prendra la décision. L'IA ne sera utilisée comme une "contributrice" à la décision de l'opérateur, comme les images ou les sons peuvent l'être pour faire des levées de doute.»*
Pour Marc Vaillant, avant de se demander si la machine va remplacer l'homme, il faut se poser une question préalable: disposera-t-on des moyens techniques pour exploiter totalement le potentiel de l'IA en matière de sécurité ? *«En effet, pour se servir pleinement du potentiel de l'IA pour la sécurité-sûreté, il va falloir disposer de puissance de calcul très importante. Et sans recourir au cloud, cela risque d'être difficile. Par ailleurs, aujourd'hui,*

le monde de la sécurité, notamment dans les entreprises, fait preuve d'une certaine réticence quant à l'usage du cloud pour gérer la sécurité parce que les données de sécurité, quelles qu'elles soient sont des données sensibles. Par ailleurs, beaucoup ne pourront pas s'offrir la puissance de calcul nécessaire à l'usage de l'IA. Il est donc évident, avant de parler de nouveaux usages, de se demander d'abord, si on dispose des infrastructures nécessaires. »

VERS UN ASSISTANT VIRTUEL EN SÉCURITÉ

Cela dit, la collaboration machine to machine n'est pas inenvisageable avec l'IA. *« Dans les aéroports, par exemple, ce MtoM, grâce aux objets connectés, permettra de compter le nombre de personnes dans telle ou telle partie de l'aéroport*, explique Fabrice Lollia. *Mais la collaboration MtoM devra se faire nécessairement au bénéfice des agents et opérateurs. On pourra ainsi voir apparaître une sorte "d'assistant virtuel de sécurité" qui aura pour mission d'orienter l'agent sur le terrain ou l'opérateur devant son écran, vers telle ou telle chose, incident, anomalie... en lui laissant la liberté d'analyser l'information, la situation, pour, si nécessaire, agir, engager tel scénario, telle intervention... La sécurité, même avec de l'IA, ne pourra pas se faire sans l'humain. Sur un tel sujet, on ne peut pas laisser la machine être la seule décisionnaire... »* ■

APS

SPÉCIAL SALON APS 2023

APPLI NOUVELLE GÉNÉRATION CHEZ RECONEYEZ

Reconeyez propose une application de notification push dans le cadre de sa solution de sécurité extérieure autonome.
Avec cette appli, les utilisateurs reçoivent des alarmes vérifiées et les images d'alarme de leur site sur leur appareil intelligent en quelques secondes.
→ **Stand G20**

ACCESSECURITY
SALON EUROMÉDITÉRRANÉEN
CYBERSÉCURITÉ & SÛRETÉ
06-07 MARS 2024
MARSEILLE CHANOT
LE RDV BUSINESS & INNOVATION
#ACCESSECURITY
ACCESSECURITY.FR
RÉSERVEZ VOTRE STAND :

PAROLE D'EXPERT

ÉRIC LEBIGOT, DIRECTEUR DU LAB D'INTELLIGENCE ARTIFICIELLE, CHAPSVISION

« Ne nous focalisons pas sur le couple IA et biométrie ! »

L'IA est évidemment très utilisée en vidéosurveillance. Pour de la surveillance périmétrique, détecter des personnes… Avec des projets européens comme Prevent sur les usages de la vidéo, on devrait assister à sa généralisation pour détecter des objets, car des tests avec acteurs ont démontré que cela fonctionnait bien dans les gares. On propose aussi, grâce à notre filiale Acic by ChapsVision, des solutions de surveillance intelligente des tunnels ferroviaires pour y détecter des personnes ou des blocages d'un tunnel de tramway comme nous le faisons déjà à Nice. Nous travaillons aussi sur la détection d'affrontements, sans oublier la détection des dépôts sauvages de déchets. Se focaliser sur l'usage de l'IA en biométrie masque sa réelle utilité.

SPÉCIAL SALON APS 2023

CAMÉRAS THERMIQUES À DOUBLE SPECTRE HANWHA

Caméras intelligentes (IA) à double spectre pour analyse visuelle et thermique d'une même zone, en simultané. Les modèles TNM-C4940TD, TNM-C4950TD et TNM-C4960TD sont équipés de deux objectifs qui génèrent une image thermique VGA et une image visuelle 4 K.

→ **Stand D19**

4/ DES USAGES ÉVIDENTS ET SURPRENANTS !

Dans les villes, les gares, les tunnels… les usages de l'IA vont se généraliser. Parallèlement, elle pourrait bien permettre aux professionnels de la sécurité de se simplifier la vie.

Bien que d'actualité ou testés – comme dans le cadre des Jeux olympiques de Paris –, certains usages de l'IA vont se populariser. *« Si les tests sont probants en 2024, on pourrait assister au déploiement de systèmes permettant de détecter des personnes, d'en assurer le suivi grâce à leur gestuel. Cela se fait et n'utilise pas le visage,* explique Marc Decombas. *Avec une limite tout de même : la puissance de calcul qui se fera dans le cloud. Or, la sécurité est encore sensible dès qu'on parle cloud. Cela dit, on devrait assister à une diversification des usages de l'IA, bien au-delà de la détection d'intrusion dans les villes »,* ajoute le dirigeant de Kooping. Pour Éric Lebigot, directeur du Lab d'intelligence artificielle (ChapsLab) chez ChapsVision : *« Il faut se poser la vraie question : comment les forces de sécurité peuvent-elles être les plus efficaces ? Avec ou sans l'IA ? C'est pour cela que l'IA est nécessaire et qu'on ne doit pas se focaliser sur les seules images. La détection sonore intelligente est un des usages de l'IA. Elle se fait déjà, mais de manière assez limitée. Elle pourrait se généraliser pour détecter des coups de feu, des sons anormaux, etc. »*

L'IA RÉDIGERA POUR VOUS !

Étonnamment, l'IA devrait aussi permettre de simplifier la vie des donneurs d'ordres et de leurs prestataires. En effet, comme le rappelle Marc Decombas, *« la sécurité, c'est beaucoup de réglementations, de rédactions de documents divers et variés comme des appels d'offres. Les outils comme ChatGPT sont aujourd'hui parfaitement capables, et de manière très fiable, de rédiger de tels documents. »*
Ce que confirme Nicolas Le Saux, dirigeant d'Atao Consulting et chercheur associé à la faculté de droit de l'université de Nice : *« Avec ce qui est déjà disponible en matière d'IA, certaines choses faciles, utiles et à forte valeur ajoutée pour les différents acteurs de la sécurité – clients et prestataires – sont quasiment à la portée de tous. ChatGPT est d'ores et déjà capable de rédiger en quelques minutes un cahier de consignes détaillées pour les agents sur site, en français et en anglais. Nous l'avons testé et cela fonctionne parfaitement. Ce type d'usage permettra aux directeurs sûreté-sécurité, ainsi qu'aux prestataires, de gagner du temps, en se libérant de tâches chronophages, pour se consacrer à d'autres, à plus forte valeur ajoutée. »* ■

3 QUESTIONS À...

NICOLAS LE SAUX, DIRIGEANT D'ATAO CONSULTING, MEMBRE D'ASIS INTERNATIONAL

En quoi l'IA va bouleverser le monde de la sécurité ?

On pense, en premier lieu, à ses usages comme la détection d'anomalies, d'incidents... mais il en est d'autres, moins évidents, mais qui n'en constituent pas moins de réelles avancées pour les cadres de la sécurité-sûreté. Par exemple, en ce qui concerne la barrière de la langue. Dans la sécurité privée, des agents issus du rang ont parfois des problèmes en anglais. L'IA peut permettre de combler cette lacune en rédigeant, à leur place, des rapports... On peut aussi utiliser des outils comme ChatGPT pour aider à répondre à des appels d'offres. Elle permet aussi de coder des logiciels comme Excel ou d'analyse de données, sur plusieurs années d'incidents, pour les analyser. On peut encore utiliser ChatGPT pour coder en Python dans des logiciels d'analyse statistique pour démontrer des corrélations entre des incidents sur un site et des incidents sur la voie publique. L'IA démocratise l'accès aux données, leur exploitation et fait qu'elles ne sont plus uniquement réservées grandes entreprises.

Existe-t-il tout de même des risques ?

Ces outils ne sont pas ouverts et ne fonctionnent que sur des données jusqu'à une certaine date. Pour ChatGPT, septembre 2021. Ils peuvent dire des bêtises, car ils utilisent ce qu'ils trouvent sur internet. Ou inventer certaines choses. En outre, l'IA est sujette, on le sait, à des biais cognitifs...

Quelle est la prochaine étape pour ces nouveaux usages ?

Les entreprises, grandes ou petites, pourront travailler sur des bases de données internes ou privatives. Sans avoir recours nécessairement à des applications «propriétaires», de tel ou tel prestataire. Enfin, l'IA permet d'identifier plus facilement les points faibles d'un dispositif grâce à des tests d'intrusion et donc de tester ses procédures.

SPÉCIAL SALON APS 2023

LE VILLAGE START-UP D'APS

Avec, entre autres, Akidaia et sa solution de contrôle d'accès non connectée ; Artifeel avec la 1re alarme 100 % autonome ; RFence et ses solutions de surveillance de l'environnement radiofréquence ; MLT Software et son logiciel pour la gestion, le suivi des entreprises de sécurité privée.

5/ UN APPORT INDÉNIABLE EN MATIÈRE DE CYBERSÉCURITÉ

La cybersécurité sera un des domaines d'application où l'IA apportera bien plus d'efficacité aux DSI et directions sûreté, pour anticiper et lutter contre les cybermenaces.

La généralisation de l'IP et des réseaux dans la sécurité pose le problème de la cybersécurité de ces infrastructures. En effet, si d'une manière très ambivalente, la multiplication des outils numériques dédiés à la sûreté/sécurité d'un site augmente les capacités opérationnelles et la création de «data» utiles pour les entreprises et leurs directions sûreté, elle augmente aussi la surface d'attaque cyber du système d'information auquel ils sont connectés. *«Sur ce point de la menace cyber, l'IA devrait permettre de faire des progrès substantiels et d'être bien plus efficace,* souligne Damien Lescos, président de SitinCloud. *Malheureusement, un grand nombre d'entreprises sont loin d'être matures en matière de cybersécurité. Par ailleurs, dans les entreprises on est encore trop souvent dans une logique de silo. Par exemple, les DSI et directeurs sûreté ne communiquent pas assez et le réseau sur lequel sont déployées les caméras est géré comme le réseau des imprimantes. Or, la matière l'IA peut permettre et permettra de bien mieux gérer la sécurité de ces réseaux. D'intégrer sûreté et cybersécurité.»* Cette problématique cyber est d'autant plus prégnante que le développement – lui aussi exponentiel – de l'IoT accroît le nombre de failles possibles dans les réseaux des entreprises.

L'IA POUR DÉTECTER PRÉCOCEMENT

Le recours à l'IA permettra, comme on l'a vu, de détecter des failles, des comportements anormaux, en amont et ainsi d'anticiper une éventuelle attaque ou, dans le pire des cas, d'y réagir plus vite. *«L'IA permettra de mettre en place des réseaux autosupervisés. C'est-à-dire qu'on laissera le système apprendre des comportements normaux, pour ensuite être capable de détecter ceux qu'il jugera comme anormaux,* ajoute Damien Lescos. *Puis des classes comme des comportements, finalement anodins, ou comme devant faire l'objet d'une alerte ou d'une réponse.»*

La cybersécurité de vos réseaux passe donc par le déploiement de solutions vous permettant de savoir ce qui se passe sur lesdits réseaux. Il sera donc profitable de se doter d'un outil qui permet de donner de la visibilité sur qui communique avec qui, qui fait quoi… Et, après un incident, savoir ce qui s'est passé pour corriger la faille. En bref, d'IA capable de détecter des anomalies de comportements ou affectant des caméras et autres capteurs… ■

PAROLE D'EXPERT

DAMIEN LESCOS, PRÉSIDENT DE SITINCLOUD

« L'IA permettra aux systèmes d'apprendre. »

Aujourd'hui, grâce à l'IA, on peut laisser les systèmes apprendre à détecter des comportements anormaux sur les réseaux, quel que soit leur usage. L'IA est capable, par rapport à des comportements habituels, d'en détecter des inhabituels. C'est le premier étage de la fusée cybersécurité/IA. La prochaine étape va consister à permettre à l'IA de classer les comportements, après apprentissage, mais aussi de comprendre qu'une attaque peut se dissimuler derrière un comportement apparemment normal. Ce n'est pas le plus simple, mais il faut comprendre et garder à l'esprit que les attaques cyber peuvent se confondre, dans bien des cas, avec des comportements normaux.
En mettant ces données à disposition des techniciens, elle leur permettra d'arbitrer et de prendre la bonne décision.

SPÉCIAL SALON APS 2023

MAXIBUS-NEO : LE DERNIER-NÉ DE SORHEA

Sorhea profite du salon APS pour lancer son nouveau concentrateur d'alarmes Maxibus-Neo. Ce dernier dispose d'une puissance de calcul importante, permettant notamment d'intégrer une technologie supplémentaire : l'analyse vidéo.
→ **Stand C39**