



Document prospectif

Rôle des centrales d'alarme agréées dans la sécurité intégrale

Octobre 2017

L'**Association des centrales d'alarme (ACA)**, l'organisme professionnel des centrales d'alarme agréées, représente plus de 95 % des systèmes d'alarme reliés à une centrale en Belgique.

La liste des membres de l'ACA est consultable sur le site web de l'ACA (www.aca-monitoring.be).

L'ACA se veut indépendante de tous les autres organismes professionnels dans le domaine de la sécurité et du gardiennage et apporte son concours à des initiatives de pour renforcer la sécurité des clients. Pour y parvenir, l'ACA entend être un interlocuteur des autorités, des administrations locales et des acteurs privés et publics de la sécurité.

Sommaire

| | |
|--|----|
| Synthèse | 4 |
| Partie 1 Le secteur aujourd'hui | 10 |
| Partie 2 Tendances | 15 |
| Partie 3 Notre vision | 21 |
| Partie 4 Concrétisation opérationnelle de notre vision | 25 |
| Partie 5 En quête d'un win-win | 29 |
| Partie 6 Notre engagement | 33 |
| Partie 7 Pistes de réflexion pour l'avenir | 35 |
| Annexe | 40 |

incendies pompiers sécurité intégrale
vision rôle police bâtiments à distance possibilités interventions
drones Belgique collaboration homme et technologie
dépôts clandestins prévention filtrer alarmes données cambriolage
parties prenantes valeur ajoutée ACA projets pilotes
caméras chaîne information sécurité live réaction intelligence artificielle
vol travailleurs isolés systèmes connecté

Synthèse

Thème d'actualité, la sécurité est en pleine mutation et se complexifie sans cesse. Afin d'assurer la sécurité de manière efficiente et efficace, il est de plus en plus fréquent que différents acteurs privés et publics de la sécurité unissent leurs forces. L'Association des Centrales d'Alarme (ACA), l'organisme professionnel des centrales d'alarme agréées, a la volonté de mobiliser son savoir-faire unique et d'exploiter les avancées technologiques pour contribuer activement à la sécurité intégrale. L'intérêt de la société doit primer à cet égard.

Le secteur des centrales d'alarme aujourd'hui

Les membres de l'ACA, l'organisme professionnel des centrales d'alarme agréées, représentent plus de **95 % des systèmes d'alarme reliés à une centrale** en Belgique. Leur principale activité consiste à gérer les signaux d'alerte émis par les **systèmes anti-effraction** auxquels peuvent également être raccordés des détecteurs d'incendie et des alarmes techniques. Ils détectent les fausses alertes et assurent un traitement rapide des alarmes selon les modalités définies par la loi. Ils n'avertissent la police, les services d'incendie et/ou les services de secours qu'en cas de nécessité ; ils jouent donc un important rôle de **filtre** vis-à-vis de ces intervenants. Leur disponibilité permanente et des contrats de niveau de service très stricts permettent de garantir une **réaction rapide et ciblée**.

Ils font usage par ailleurs de **technologies avancées** pour assurer une **surveillance à distance**. Les opérateurs de la centrale d'alarme sont capables de fournir, à distance, l'accès à un site ou, grâce à la vidéosurveillance, d'effectuer des rondes virtuelles selon une fréquence convenue.

La sécurité est en mutation et, par conséquent, le secteur suit cette évolution

Plusieurs phénomènes sociaux tels que les flux migratoires, les inégalités de revenus et le terrorisme suscitent un **sentiment accru de risque chez les citoyens et les entreprises**. Les citoyens et les entreprises sont donc plus attentifs à la sécurité et à la protection. Et ils attendent donc de plus en plus **de la part des acteurs de la sécurité qu'ils soient joignables en permanence et qu'ils réagissent immédiatement** – attentes créées par des acteurs de l'économie numérique tels qu'Uber. Ces attentes doivent être mises en balance avec le fait que les acteurs publics dont ceux liés à la sécurité **doivent faire toujours plus avec moins de moyens**.

Il devient donc de plus en plus difficile pour ces derniers de répondre à la demande des citoyens et des entreprises et de continuer à garantir la sécurité. Dans cette quête d'efficacité et d'efficacités, **de nouveaux partenariats public-privé** voient le jour, ce qui permet à chacune des parties de se concentrer sur ses **compétences fondamentales**.

De plus, la **technologie** est en train de changer la donne en termes de possibilités. Elle peut constituer une substantielle **plus-value** lorsqu'il s'agit d'assurer la sécurité. L'**internet des objets** (ou « Internet of things »), l'**intelligence artificielle** et les **drones** prouvent aujourd'hui déjà leur utilité en matière de sécurité (safety & security). À l'avenir, ces technologies vont encore créer plus de possibilités pour garantir une meilleure sécurité. Ces technologies permettent par exemple aux membres de l'ACA d'assurer une meilleure **vérification** des alertes et un meilleur contrôle des systèmes d'alarme ; elles permettent de fonctionner de manière plus **proactive et même prédictive** et fournissent des **données** intéressantes au secteur – des données qui favorisent une prévention plus efficace à l'appui des services de secours et d'intervention.

Mais, les évolutions technologiques génèrent également des **défis**, comme la **cybercriminalité** et le **respect de la vie privée**. En effet, plus les objets sont connectés à un réseau, plus ils sont vulnérables aux cyberattaques. D'où l'importance croissante d'assurer un excellent **niveau de qualité** pour l'ensemble de la chaîne. La

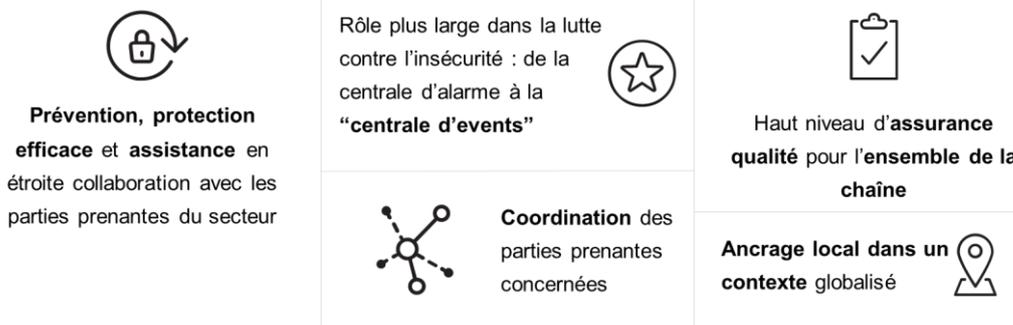
standardisation et l'interopérabilité gagnent elles aussi en importance pour garantir une bonne communication entre les différents systèmes. Enfin, la nécessité de **filtrer** les alarmes va croissante ; le nombre d'alertes et/ou de fausses alertes ne va cesser de croître au fur et à mesure que le nombre d'objets connectés à un réseau va augmenter et qu'ils vont échanger des données.

Les éléments abordés ci-avant et la complexité croissante à assurer la sécurité confirment la nécessité d'une **approche intégrale de la sécurité**. Le secteur entend jouer un rôle actif à cet égard.

Notre vision

Aujourd'hui, le secteur crée de la valeur ajoutée pour différentes parties prenantes en se concentrant sur ses domaines clés que sont le cambriolage et le vol et sur son rôle de filtre des fausses alertes. Mais dans le futur, il veut **faire un usage plus intensif de ses connaissances spécialisées, de sa disponibilité permanente et de ses solutions technologiques avancées** pour contribuer de manière efficiente et efficace à un environnement plus sûr pour les citoyens, les organisations, les entreprises et les autorités. Car **la sécurité est un droit fondamental**.

Pour cela, il a défini les priorités suivantes :



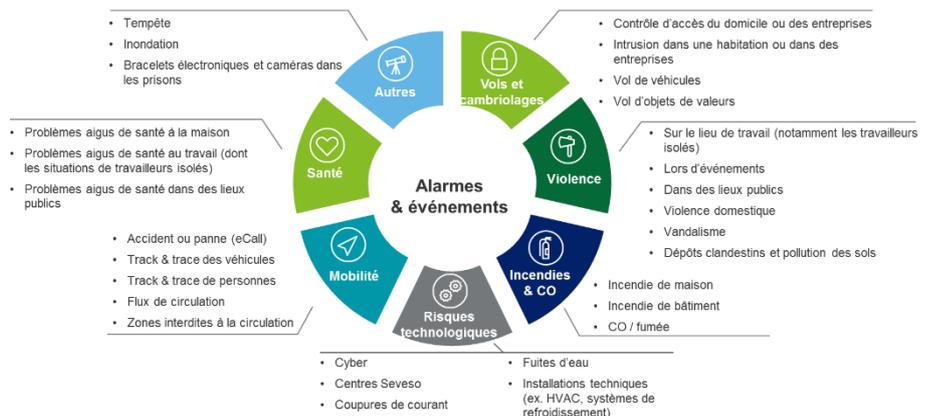
Prévention, protection efficace et assistance en étroite collaboration avec les parties prenantes du secteur

Le secteur entend jouer un rôle majeur à chaque étape de la chaîne de la prévention, de la protection et de l'assistance. Il veut mettre davantage l'accent sur la prévention et passer de la gestion des alertes à la gestion proactive des situations. Parallèlement, il cherche à atteindre un meilleur taux de raccordement des systèmes d'alarme neufs et existants à une centrale d'alarme afin de pouvoir garantir une protection efficace au client final. Et enfin, il souhaite aider les services d'intervention par un échange d'informations (en temps réel) et continuer à porter lui-même assistance aux clients finaux à distance.

Rôle plus large dans la lutte contre l'insécurité : de la centrale d'alarme à la « centrale d'événements »

Les évolutions technologiques génèrent de nouvelles possibilités en matière de surveillance. Le secteur souhaite donc passer d'une centrale d'alarme à une centrale « d'événements » qui traite un large éventail d'alertes et gère les événements et les situations.

La liste des domaines dans lesquels le secteur souhaite s'investir en priorité est consultable au chapitre



« Concrétisation opérationnelle de notre vision ». Il est important de signaler à cet égard que le secteur est constitué d'un ensemble dynamique d'entreprises différentes qui se concentreront sur certains domaines en fonction du savoir-faire qui leur est propre.

 **Coordination des parties prenantes concernées**
La centrale d'alarme est le lieu par excellence où sont rassemblées en un seul endroit toutes les données pertinentes à propos des événements et alarmes divers. Ces données peuvent être constituées d'alarmes, mais aussi d'images, de sons, de coordonnées géographiques, etc. La centrale d'alarme est idéalement placée pour analyser toutes ces données, mobiliser les intervenants adéquats et aider ceux-ci à prendre de meilleures décisions. C'est en qualité de « régisseur » que le secteur ambitionne une collaboration intégrée et optimisée avec les parties prenantes concernées.

 **Haut niveau d'assurance qualité pour l'ensemble de la chaîne**
Afin de lutter adéquatement contre les risques actuels et garantir un service efficace, le secteur vise un haut niveau d'assurance qualité pour l'ensemble de la chaîne, et ce en s'appuyant sur les éléments suivants : 1) une certification moderne pour l'ensemble de la chaîne qui respecte les normes européennes ; 2) la qualité technique et l'interopérabilité des systèmes ; et 3) le respect de la vie privée.

 **Ancrage local dans un contexte globalisé**
Le secteur tient à conserver un ancrage local afin, d'une part, de pouvoir mobiliser des opérateurs possédant les compétences linguistiques adéquates et l'expérience du contexte local et, d'autre part, d'être un partenaire à part entière pour apporter sa contribution à l'élaboration de politiques de sécurité en Belgique.

Concrétisation opérationnelle de notre vision

Afin de remplir son rôle de « centrale d'événements », le secteur tient avant tout à s'investir dans un certain nombre de domaines étroitement liés à sa **raison d'être fondamentale** (créer un environnement sûr en collaboration avec d'autres intervenants) dans lesquels il est à même d'exercer ses compétences pour créer de la **valeur ajoutée** pour les parties prenantes concernées :



 **Cambriolage et vol** : exploiter les avancées technologiques pour un service plus performant (p. ex., une meilleure vérification et un fonctionnement prédictif grâce aux caméras intelligentes) et recourir davantage aux services à distance tels que le contrôle d'accès à distance et les rondes virtuelles.

 **Incendie et sécurité des bâtiments** : proposer une réponse intégrée à l'insécurité dans les bâtiments (incendie, monoxyde de carbone, fuites d'eau, etc.) et vérifier les alarmes incendie dans des situations où la technologie le permet. Soutenir également les interventions par l'échange de données et la fourniture d'accès à distance.

 **Criminalité violente, incivilités et dépôts clandestins** : proposer l'appui par caméras pour prévenir la criminalité violente, les incivilités et les dépôts clandestins et y réagir, y compris sur le domaine public. Dans la sphère privée, veiller également sur les personnes confrontées à des situations à risque grâce à la protection rapprochée virtuelle¹.

¹ Assurer une supervision à distance lors de moments à risque tels que l'ouverture et la fermeture et envoyer de l'aide en cas de situation anormale ou présence de personnes suspectes.

 **Travailleurs isolés** : veiller à la sécurité (« safety & security ») des travailleurs isolés, p. ex. les techniciens d’opérateurs de télécoms et de fournisseurs d’énergie, les chauffeurs routiers et les commerciaux.

 **Circulation et mobilité** : contrôle d’accès à distance ou fourniture d’un accès contrôlé aux zones sensibles sur le domaine public (p. ex. zones piétonnes). Également filtrer et vérifier les signaux émis par les caméras intelligentes en rue et proposer des solutions (internationales) pour l’eCall².

Vers un win-win pour toutes les parties prenantes

Le secteur veut créer de la valeur ajoutée pour la société, les citoyens et les parties prenantes publiques et privées dans les domaines prioritaires qu’elle s’est choisis.

Valeur ajoutée pour les parties prenantes publiques

| | |
|--------------------------------|---|
| Société et citoyens | <ul style="list-style-type: none"> • Meilleure sécurité publique et sentiment accru de sécurité • Limitation des dommages potentiels consécutifs à un incendie, au monoxyde de carbone, aux fuites d’eau, aux cambriolages, etc. |
| SPF Intérieur | <ul style="list-style-type: none"> • Élaborer ensemble une politique tournée vers l’avenir qui optimise la collaboration entre les acteurs de la sécurité et l’engagement de ceux-ci et qui soit étayée par des statistiques et des informations objectives issues « du terrain » • Réduire les interventions superflues de la police et des services d’incendie • Stimuler l’innovation |
| Administrations locales | <ul style="list-style-type: none"> • Efficacité économique grâce à une mobilisation optimale des ressources et l’exploitation maximale des caméras existantes sur le domaine public • Prévention et limitation des coûts découlant de la criminalité violente, des incivilités et des dépôts clandestins • Accroissement du sentiment de sécurité des entreprises, des visiteurs et des résidents sans prendre de mesures draconiennes |
| Police | <ul style="list-style-type: none"> • Une plus grande priorité accordée aux missions principales et diminution du nombre d’interventions inutiles • Interventions plus efficaces grâce à l’échange de données et à une détection plus précoce • Accès à des technologies de pointe sans engendrer des coûts d’investissement élevés (en collaboration avec les entreprises de gardiennage) |
| Services d’incendie | <ul style="list-style-type: none"> • Soutien dans la réalisation des objectifs stratégiques • De meilleurs dossiers d’intervention et des interventions plus efficaces grâce à l’échange de données et à une détection plus précoce |

Valeur ajoutée pour les parties prenantes privées

| | |
|----------------------|--|
| Assureurs | <ul style="list-style-type: none"> • Réduire le nombre de demandes d’indemnisation et limiter l’ampleur de ces demandes • Disposer de statistiques et d’informations pour étayer le fonctionnement et la standardisation futurs |
| Installateurs | <ul style="list-style-type: none"> • S’accorder sur l’utilisation des nouvelles technologies et des nouveaux modèles économiques afin de suivre les évolutions technologiques |

² Installé dans les voitures, le système eCall lance automatiquement (ou manuellement au moyen d’un bouton poussoir) un appel d’urgence à une centrale d’alarme en cas d’accident. Aussi, le système communique immédiatement des informations essentielles telles que la position exacte et l’heure de l’accident.

| | |
|--------------------------|---|
| Entreprises | <ul style="list-style-type: none"> • Approche intégrée pour contrer l'insécurité dans les bâtiments • Sécurité accrue pour les travailleurs isolés et le personnel confronté à des situations à risque • Efficience économique par l'augmentation des services à distance |
| Le secteur en soi | <ul style="list-style-type: none"> • De la latitude pour permettre au secteur de se développer et de continuer à investir dans les ressources humaines, l'innovation et les technologies • Reconnaissance en tant que partenaire fiable et compétent |

Notre engagement

Pour concrétiser sa vision et parvenir à un win-win avec les parties prenantes de la sécurité, le secteur souhaite s'engager sur les fronts suivants.



Etre un partenaire à part entière dans la sécurité intégrale

- Constituer une représentation permanente avec une **capacité de dialogue et d'action**
- Etablir des passerelles entre les **fédérations du secteur privé et le SPF Intérieur**
- Collaborer plus étroitement avec les **acteurs privés et publics de la sécurité** et mettre en place des **projets pilotes** au niveau local
- Etre plus actif au sein du **CoESS*** et positionner la Belgique comme le pionnier des centrales d'alarme du futur



Etre à la pointe de l'innovation

- Etre à la **pointe des avancées technologiques**
- Identifier les **applications pertinentes à l'étranger**
- Publier / **communiquer** les enseignements au grand public
- Transformer les centrales d'alarme privées en "**environnement de test**" pour des projets pilotes



Tendre à la standardisation, l'interopérabilité des systèmes et la cybersécurité

- Coordonner et stimuler **l'harmonisation des normes** en Belgique en collaboration avec CoESS*
- S'investir pour apporter une réponse adéquate aux **cybermenaces** et garantir **le respect de la vie privée**

* Confederation of European Security Services

Pistes de réflexion pour l'avenir

Pour jeter les bases des étapes ultérieures, le secteur a élaboré des suggestions concernant la collaboration avec les différentes parties prenantes et a identifié des actions concrètes. La liste complète de ces **actions** est consultable au chapitre « **Partie 7 | Pistes de réflexion pour l'avenir** ».

Collaboration avec le SPF Intérieur

Le secteur est désireux d'engager un dialogue avec les directions générales « Sécurité et prévention » et « Sécurité civile » du SPF Intérieur et d'évoluer vers une **concertation structurelle** étayée par des **statistiques objectives**. À cet égard, il souhaite contribuer activement à la **mise en œuvre concrète et à l'évaluation** de la **politique de sécurité**. En matière d'incendie et de sécurité des bâtiments, il peut s'engager à **vérifier** les alarmes lorsque la technologie le permet.

Le secteur attend du soutien de la part du SPF Intérieur pour accélérer ses **projets pilotes** avec d'autres parties prenantes. De son côté, l'ACA impliquera le SPF Intérieur et le tiendra informé des projets pilotes qu'elle met en oeuvre.

Collaboration avec les administrations locales

Le secteur souhaite établir des **partenariats public-privé** avec les administrations locales qui seront précédés par un nombre limité de **projets pilotes** mûrement choisis en collaboration avec d'autres parties prenantes telles que les zones de police locale.

Collaboration avec la police

En ce qui concerne la police, le secteur ambitionne une **collaboration basée sur la chaîne de sécurité** assortie d'un respect mutuel des responsabilités des partenaires impliqués. À l'instar du modèle des « Regionale Toezicht Ruimten » (zones de surveillance régionale) aux Pays-Bas, le secteur souhaite surveiller proactivement le domaine public, et ce sous la houlette de la police. Afin de développer une vision suffisamment fondée sur la réalité du terrain, le secteur propose de mettre sur pied des **projets pilotes** avec les zones de police locale et les administrations locales.

Collaboration avec les services d'incendie

Le secteur propose de mettre sur pied des **projets pilotes** avec une ou plusieurs zones locales d'incendie pour la **vérification** des alarmes incendie et l'**échange d'informations**. Les salles de contrôle des membres de l'ACA peuvent servir d'**environnement de test** à cet effet.

Collaboration avec les assureurs

Les membres de l'ACA souhaitent recueillir et partager des **statistiques** et des **informations** avec les assureurs pour soutenir le fonctionnement de ces derniers. Ils aspirent par ailleurs à être un interlocuteur pour la **certification** (INCERT et BOSEC, par exemple) et à contribuer à l'élaboration d'une approche adéquate relative à la **cybersécurité** des systèmes anti-effraction numériques (basés sur l'IP). En contrepartie, l'ACA attend des assureurs qu'ils favorisent, selon la situation, le **raccordement des systèmes d'alarme à une centrale**.

Collaboration avec les installateurs

L'ACA souhaite une collaboration plus étroite avec l'association belge représentant le secteur de la sécurité électronique (ALIA Security), tant en matière d' cambriolage et de vol que d'incendie et de sécurité des bâtiments. L'ACA entrevoit des opportunités afin de mieux coordonner l'**usage des nouvelles technologies et des nouveaux modèles économiques**.

Collaboration avec les entreprises

Concernant la problématique des **travailleurs isolés** et de la **protection rapprochée virtuelle** en particulier, le secteur entend consulter les représentants des secteurs à haut risque afin d'assurer une meilleure traduction des besoins en solutions efficaces. Le secteur identifiera un secteur d'essai afin de lancer un **projet pilote** conjoint. Son souhait est de parvenir à une **réglementation** et à des **garanties** suffisantes en termes de **qualité**.

Le secteur veut aussi continuer à collaborer étroitement avec les **entreprises de gardiennage** afin de proposer des **solutions globales**.

3. Conclusion

Le secteur veut s'**engager** à être un **partenaire à part entière** dans la sécurité intégrale. L'ACA a une **vision** claire de son rôle et veut créer un **win-win** avec les acteurs publics et privés de la sécurité. Elle invite les parties prenantes à entamer le **dialogue**.



Partie 1 | Le secteur aujourd'hui

Les membres de l'ACA, l'organisme professionnel des centrales d'alarme agréées, représentent plus de 95 % des systèmes d'alarme reliés à une centrale en Belgique. Ils combinent connaissances spécialisées et solutions technologiques pour filtrer les alarmes entrantes et détecter les fausses alertes et assurent un traitement correct et légal de celles-ci.

1. Le secteur des centrales d'alarme aujourd'hui

Les **membres de l'ACA** gèrent les signaux émis par différents systèmes d'alarme tels que les systèmes de détection de cambriolages et les systèmes de suivi (« track & trace »). Il s'agit de centrales d'alarme **agréées** autorisées à mener des activités de surveillance ; leur activité est en lien avec la sûreté de la société. Elles sont supervisées par le ministre de l'Intérieur et doivent satisfaire à des conditions légales pour obtenir leur agrément (valable pour une période de cinq ans).

Outre les centrales d'alarme agréées, il existe également en Belgique plusieurs centrales et centres d'appel dont les activités ne sont pas régies par la loi, par exemple :

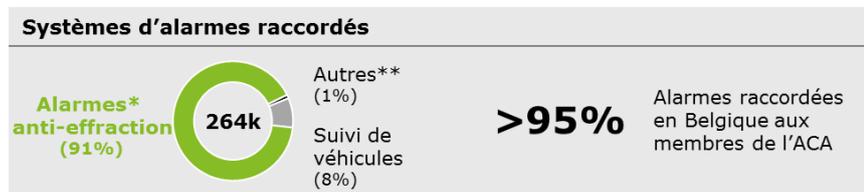
- les centrales répondant aux appels urgents des services de secours (centres d'appel d'urgence 100/112 pour les services d'incendie ou

une assistance médicale, et les centres de communication et d'information 101 pour la police) ;

- les centrales pour l'assistance voyage et dépannage et les centrales de soin (p. ex., Europ Assistance, Touring, Mutas et la Croix jaune et blanche) ;
- les centrales d'alarme internes des grandes entreprises.

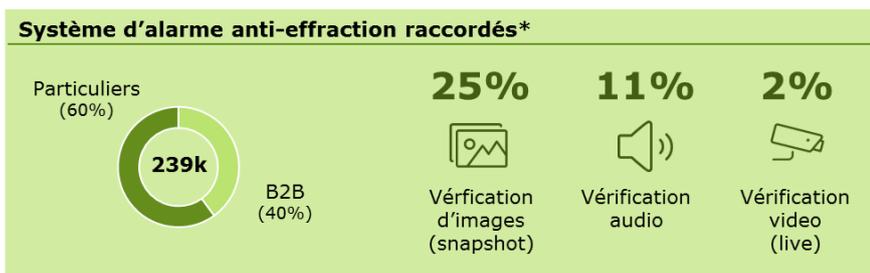
Les membres de l'ACA **contrôlent les signaux reçus, les interprètent, vérifient** s'il s'agit d'une alerte réelle et **avertissent le propriétaire ou l'occupant** de l'immeuble/du bien surveillé ou la personne de contact, conformément aux instructions convenues au préalable. Si besoin est, ils avertissent également les **services de police et de secours**, et ce toujours après avoir vérifié l'alarme. Ils peuvent aussi faire appel à des **agents de gardiennage** pour effectuer une intervention après alarme. L'**installation** de ces systèmes est effectuée par un installateur agréé. Plusieurs membres de l'ACA proposent des services intégrés et, par conséquent, des services d'installation également ; d'autres travaillent en étroite collaboration avec des installateurs indépendants.

En 2016, environ **264 000 systèmes d'alarme étaient raccordés** aux centrales des membres de l'ACA soit plus de **95 %** de l'ensemble des raccordements en Belgique. L'**activité principale** du secteur consiste à gérer les **systèmes d'alarme anti-effraction** auxquels peuvent également être raccordés des **détecteurs d'incendie** et des **alarmes techniques** (91 % du nombre total de raccordements).



* Systèmes d'alarme anti-effraction raccordés à une centrale d'alarme en incluant les systèmes auxquels sont raccordés des détecteurs incendies et / ou les alarmes techniques

** Autres: systèmes d'alarme uniquement techniques, incendie et / ou de personnes

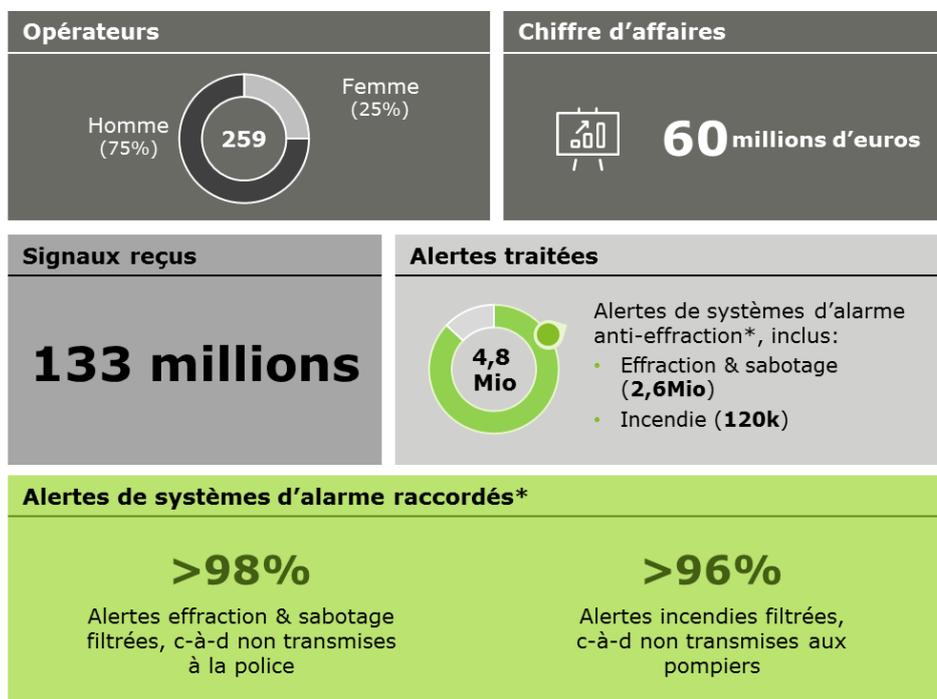


* Systèmes d'alarme anti-effraction raccordés à une centrale d'alarme en incluant les systèmes auxquels sont raccordés des détecteurs incendies et / ou les alarmes techniques

Les alarmes anti-effraction reliées à une centrale d'alarme appartiennent aussi bien à des particuliers (60 % des raccordements) qu'à des entreprises (40 %). Au-delà des détecteurs et capteurs « traditionnels », le recours aux **technologies avancées**, telles que la vérification par images et la vérification vidéo en direct est de plus en plus fréquent. Ces technologies avancées évoluent en permanence.

Le secteur est relativement **petit** en termes de chiffre d'affaires et de nombre de travailleurs, mais crée par contre une **importante valeur ajoutée** pour les services de secours et d'intervention grâce à son rôle de filtrage des (fausses) alertes. En 2016, **plus de 98 %** des alertes d'intrusion et de

sabotage ont été **filtrées** et n'ont donc pas été transmises à la **police**. **Plus de 96 %** des alarmes incendie ont été filtrées pour les **services d'incendie**.



* Systèmes d'alarme anti-effraction raccordés à une centrale d'alarme en incluant les systèmes auxquels sont raccordés des détecteurs incendies et / ou les alarmes techniques

2. Suivi et traitement efficaces des alarmes grâce à des connaissances spécialisées et à la technologie

Les activités au sein des centrales d'alarme agréées sont assurées **24 heures sur 24 et 7 jours sur 7** par des **opérateurs d'alarme** spécialement formés à cette tâche. En cas d'alerte, ils prennent les mesures utiles en respectant toujours les **instructions** convenues au préalable et les **procédures (légales)**.

Les opérateurs d'alarme sont la cheville ouvrière du secteur et de ses clients. Pour les soutenir de manière optimale et assurer la sécurité des citoyens, des organisations et des entreprises de manière efficace, le secteur recourt largement aux **technologies** avancées. L'utilisation de la **vidéosurveillance**, par exemple, permet aux centrales de garantir une surveillance à distance. Ainsi, les opérateurs de la centrale d'alarme de contrôle peuvent consulter, selon une fréquence convenue, les images provenant de plusieurs caméras et effectuer ainsi une « **ronde virtuelle** ». C'est donc la centrale d'alarme qui amorce cette ronde virtuelle, qui n'est pas déclenchée par un signal d'alerte. Comme il est possible de suivre ce qui se passe en direct, la vidéosurveillance permet de recueillir d'autres informations utiles en cas d'alarme ou d'incident et, donc, de prendre plus rapidement des mesures appropriées.

Par ailleurs, les opérateurs peuvent fournir, à distance, l'accès à un site (« **services de portier vidéo** ») ou s'adresser à distance à des personnes indésirables (« **dissuasion audio** »).

Enfin, le secteur traite aussi de plus en plus des **signaux générés par des caméras intelligentes**. Ces caméras font office de détecteur et servent notamment à identifier le franchissement d'un périmètre et les incendies.



3. Valeur ajoutée pour un nombre important de parties prenantes

Même si la législation belge n'impose pas le raccordement des systèmes d'alarme à une centrale, ce raccordement présente de nombreux **avantages** :

- **Vérification et interprétation par un être humain** avec, par conséquent, un **filtrage** efficace d'un très grand nombre de fausses alertes : le secteur permet d'éviter de relayer 98 % des alarmes à la police et 96 %, aux services d'incendie ;
- Possibilité d'**interagir** avec un opérateur professionnellement qualifié dans des situations de stress ;
- Disponibilité 24 heures sur 24 et 7 jours sur 7, contrats de niveau de service stricts et possibilité de transmission directe aux services de l'ordre et/ou de secours après vérification afin de **garantir une réaction rapide et appropriée** ;
- **Tranquillité d'esprit** pour le client final : réaction efficace et rapide même lorsque le client final n'est pas présent dans le bâtiment ;
- **Fiabilité et qualité** : les opérateurs sont triés sur le volet par le SPF Intérieur et les services de sûreté. Ils sont sélectionnés sur la base de critères d'admission très stricts³, en effet, chaque opérateur reçoit une formation légale de 70 heures, puis une formation plus approfondie délivrée en interne. Aussi, les centrales agréées sont fréquemment contrôlées par des services d'inspection externes. Par ailleurs, les membres de l'ACA sont certifiés ISO⁴ et/ou INCERT⁵ ; ils respectent des normes de qualité très strictes et sont régulièrement

³ Conditions d'admission : extrait de casier judiciaire vierge datant de 6 mois maximum, réussite d'un examen psychotechnique

⁴ ISO 9001:2015

⁵ L'autorisation d'utiliser la marque INCERT découle d'une certification attestant de la conformité des centrales d'alarme par rapport au « Règlement pour la certification des centrales d'alarme » et aux « Spécifications pour les centrales de surveillance T020 » édités par le Comité électrotechnique belge (CEB).

soumis à des contrôles qui garantissent une protection optimale. Enfin, les différents membres de l'ACA disposent également de services et de structure interne de contrôle opérationnel.

Partie 2 | Tendances

Différentes mutations sociales, économiques et technologiques ont une incidence majeure sur la sécurité, y compris donc sur le secteur des centrales d'alarme.

1. Tendances sociales

1.1 Sentiment accru de risque

Différents phénomènes sociaux tels que la **migration**, les **inégalités de revenus** et le **terrorisme** suscitent un sentiment accru de risque chez le citoyen et parmi les entreprises. Lors d'un récent sondage organisé par De Standaard par exemple, plus de la moitié des Flamands (51 %) ont indiqué se demander si, à l'avenir, ils vivraient toujours dans un pays. Le **vieillessement de la population** joue également un rôle à cet égard. D'après ce sondage, on doit ce résultat en majeure partie à la génération plus âgée (les plus de 56 ans) qui craint nettement plus l'insécurité que les jeunes.

De plus, l'**agressivité** reste un fléau dans différents milieux, notamment au **travail**. Le personnel des magasins, des hôpitaux et des instances publiques est régulièrement confronté à la violence. La vaste catégorie des **travailleurs isolés** est elle aussi vulnérable aux agressions et y est encore confrontée, elles travaillent seules et sans supervision directe. Citons par exemple les techniciens d'opérateurs de télécommunications et de fournisseurs d'énergie et les travailleurs mobiles tels que les chauffeurs de poids lourds et les commerciaux.

1.2 Demande d'accessibilité permanente et de réaction immédiate aux acteurs de la sécurité

Les acteurs de l'économie numérique tels qu'Uber ont profondément redéfini les attentes des gens qui, désormais, veulent accéder à un service **où et quand ils le souhaitent**. Ces attentes se sont étendues à tous les prestataires de services : les gens attendent des acteurs de la sécurité aussi qu'ils soient accessibles en permanence et qu'ils réagissent immédiatement.

2. Tendances économiques

2.1 Partenariats public-privé pour une efficacité et une efficacité optimales

Garantir la sécurité publique n'est plus une tâche qui relève des seuls pouvoirs publics, mais une responsabilité qui incombe à chacun. De plus, toutes les parties concernées visent une efficacité et une efficacité maximales compte tenu de la **pression qui consiste à faire toujours plus avec moins de moyens**. C'est pourquoi, de plus en plus de partenariats public-privé voient le jour, dans le cadre desquels chaque acteur se concentre le plus possible sur ses **compétences fondamentales**.

2.2 Internationalisation du secteur et modifications de la chaîne de valeur

La criminalité n'est pas un phénomène local. Le secteur reçoit aussi de plus en plus de demandes de soutien de la part de clients internationaux et constate une internationalisation et un développement croissants des **activités transfrontalières**.

D'ailleurs, le secteur connaît une vague de **consolidation**, les acquisitions étant généralement opérées par des **groupes internationaux**, c'est surtout pour les petits acteurs que les exigences strictes d'investissement deviennent trop lourdes.

De **nouveaux acteurs** se lancent également sur le marché : plusieurs entreprises technologiques et opérateurs de télécommunications proposent à présent des solutions en matière de sécurité, principalement pour le marché résidentiel. Le secteur s'attend à ce que ces nouveaux venus contribuent à **stimuler** la pénétration sur le marché des systèmes d'alarme assortis d'une surveillance. En Belgique, le taux de pénétration des systèmes d'alarme reliés à une centrale est encore et toujours inférieur (3 %) à celui de plusieurs pays tels que la Norvège (17 %), la Suède (11 %), l'Irlande (11 %) et l'Espagne (7 %).

3. Tendances technologiques

L'utilisation des technologies peut représenter une plus-value considérable lorsqu'il s'agit d'assurer la sécurité, mais elle comporte aussi des défis. Le secteur des centrales d'alarme agréées s'attend à ce que les tendances suivantes aient l'impact le plus important.

3.1 L'internet des objets (IoT) et les bâtiments intelligents

L'Internet of Things (IoT ou l'internet des objets) consiste à connecter des objets du quotidien à un réseau pour permettre l'échange de données. Les **objets intelligents** jouent un rôle clé à cet égard, en effet, grâce à l'utilisation de capteurs, ces objets sont capables d'assimiler un environnement et se chargent de traiter eux-mêmes déjà une partie de ces signaux. Ils peuvent alors communiquer entre eux grâce à des technologies de réseau intégrées, faire usage de services Internet et communiquer de manière interactive avec les humains.

Les **bâtiments intelligents** constituent une des principales applications de l'IoT, qui s'est rapidement développé ces dernières années. La technologie sous-jacente à ces bâtiments intelligents se compose d'objets connectés qui recourent aux technologies de réseau telles que le wifi et le LPWAN (Low-Power Wide-Area Network tel que LoRa et SigFox) pour se connecter à d'autres objets à l'intérieur et à l'extérieur du bâtiment et pour communiquer avec eux.

À titre d'**exemples** de tels objets IoT, on peut citer les caméras intelligentes, les détecteurs de mouvement connectés et les appareils ménagers intelligents. De plus, il est également possible de connecter des systèmes issus des technologies opérationnelles (TO) telles que la ventilation, le chauffage, l'air conditionné et l'éclairage.

Ces objets et systèmes « intelligents » **partagent des données** avec l'utilisateur et peuvent être **commandés à distance**, par exemple, au moyen d'une application sur smartphone ou tablette ou d'un terminal mural. Par ailleurs, les bâtiments intelligents sont aussi capables d'**automatiser les bâtiments**. Vous pouvez, par exemple, programmer une maison intelligente de façon à allumer automatiquement le chauffage lorsque vous êtes sur le chemin du retour du travail (sur la base de la géolocalisation de votre smartphone).

Les systèmes de **sécurisation et de contrôle d'accès** constituent un **élément majeur des bâtiments intelligents**. En 2015, le marché de ces systèmes représentait environ 1,1 milliard d'euros en Europe occidentale et,



Illustration d'une maison intelligente

selon les prévisions, il devrait grimper à 4,5 milliards d'euros à l'horizon 2020.

Les dispositifs de sécurité connectés se composent notamment de **serrures électroniques**, de **capteurs connectés** (p. ex., capteurs de porte et de fenêtre), de **caméras** et de **détecteurs** (p. ex., mouvement, incendie, monoxyde de carbone, CVC, fuites d'eau). Tous ces éléments sont parfaitement **intégrés** et peuvent être **automatisés** ou **commandés à distance**, ce qui permet aux utilisateurs d'activer/désactiver l'alarme ou d'ouvrir/de fermer les serrures des portes à l'aide de leur smartphone ou de leur tablette. Lorsqu'un événement est détecté, ces systèmes avertissent l'utilisateur et/ou une centrale d'alarme. L'intégration croissante des caméras permet **de plus en plus** de transmettre directement **des photos ou des images vidéo**.

Sur ce marché, on trouve les fournisseurs classiques de systèmes d'alarme, mais aussi de plus en plus d'**acteurs technologiques** (p. ex., Google Nest) et d'**opérateurs de télécommunications** (p. ex., Comcast Xfinity, AT&T Digital Life), principalement dans le segment résidentiel où la demande en caméras de surveillance, alarmes anti-effraction et détecteurs de fumée connectés est particulièrement importante.

L'arrivée de l'IoT et des systèmes de sécurisation et de contrôle d'accès dans les bâtiments intelligents a plusieurs **implications** pour le secteur :

- Comme les systèmes intelligents avertissent l'utilisateur et que l'utilisation de ces systèmes est simple, il est plus facile pour les utilisateurs de **se charger eux-mêmes de la surveillance de leur système**. Certains utilisateurs trouveront cela suffisant, mais cela ne compense évidemment pas les avantages que peuvent apporter les centrales d'alarme en termes de disponibilité permanente et de réaction rapide (obligatoire).
- La **nécessité de filtrer et de vérifier** les alarmes ne va cesser de se renforcer puisque le nombre d'objets à gérer n'arrête pas d'augmenter et que le nombre d'alertes générées est donc plus important. Le secteur mise sur la création de suffisamment de valeur ajoutée pour conserver sa pertinence malgré l'arrivée des systèmes autogérés.
- L'IoT et les bâtiments intelligents créent des **opportunités pour les centrales d'alarme d'élargir leur offre**. Plusieurs entreprises belges et étrangères proposant des services de surveillance pour les alarmes anti-effraction offrent également des services de gestion de l'énergie et de l'eau, par exemple, ou gèrent des processus critiques tels que les installations frigorifiques. Il devient aussi plus facile de fournir des services à distance tels que le contrôle d'accès, et ce sans nécessiter la présence d'une personne sur place.
- Il est essentiel que les différents systèmes, par exemple dans un bâtiment intelligent, puissent communiquer suffisamment entre eux – l'importance de la **standardisation et de l'interopérabilité** ne cesse de croître.
- Le fait que ces systèmes intelligents fassent usage des technologies de réseau a aussi des conséquences. D'une part, les centrales d'alarme ont la possibilité de **contrôler à tout moment le statut de capteurs, détecteurs et autres** pour s'assurer que tout fonctionne encore correctement et que le système n'a pas été saboté. D'autre part, ces systèmes sont **vulnérables aux cyberattaques**.

La presse a relaté récemment la volonté de Philippe De Backer, secrétaire d'État belge à la Protection de la vie privée, d'interdire les caméras IP non sécurisées. En effet, plusieurs sites permettent de consulter les images de caméras IP non sécurisées ou mal sécurisées. Il est donc de plus en plus important d'avoir un niveau d'assurance qualité de pointe pour l'ensemble de la chaîne.

3.2 Informatique cognitive et intelligence artificielle

Entrer dans le détail de la définition de l'informatique cognitive et de l'intelligence artificielle (IA) et des différences entre celles-ci nous éloignerait trop de notre sujet. Grosso modo, tous deux sont des systèmes auto-apprenants qui **font des prédictions et étayent des décisions** reposant sur l'analyse de données et sur des décisions antérieures. Ces technologies sont de plus en plus utilisées à des fins de sécurité, tant par les acteurs privés que publics.

La **police britannique**, par exemple, prédit les délits grâce à l'intelligence artificielle. Un système informatique doté de l'intelligence artificielle prédit le risque que des suspects commettent un délit, ce qui doit aider la police à prendre la décision de prolonger la détention de ces personnes.

Dans le **secteur privé**, les **systèmes de sécurisation de type « smart home » basés sur l'IA** connaissent un développement exponentiel.

Récemment, **Alarm.com** a lancé le dispositif « **Insights Engine** ». Ce système est capable d'identifier le comportement, les schémas d'activité et les données d'appareils et de capteurs connectés (cf. IoT) dans un bâtiment pour se familiariser aux habitudes des utilisateurs. La technologie peut alors agir en tenant compte de ces informations. La première application de cette technologie serait une nouvelle catégorie de notifications intelligentes capables d'informer les utilisateurs des risques en matière de sécurité au sein du bâtiment, sans devoir créer eux-mêmes des règles ou notifications appropriées. La technologie est ainsi à même de se familiariser à l'utilisation de la porte d'entrée d'un bâtiment, par exemple. En semaine, cette technologie constate qu'il y a systématiquement beaucoup d'activité tôt le matin, au moment où les gens se rendent à leur travail ou à l'école. Le week-end, la porte n'est généralement ouverte que plus tard au cours de la journée. Si quelqu'un ouvre la porte d'entrée plus tôt que d'habitude un samedi matin, Insights Engine génère une notification d'« activité inattendue ». La famille est ainsi informée du fait que les enfants sont partis jouer à l'extérieur, par exemple.

Pas plus tard que cette année, **Vivint** a lancé la solution « **Sky** », un assistant intelligent qui se sert de l'intelligence artificielle pour gérer de manière automatique des appareils connectés au sein d'un bâtiment. Sky est par exemple capable d'utiliser les données de capteurs et d'appareils pour détecter la présence ou l'absence d'un utilisateur, ce qui permet de verrouiller automatiquement les portes et d'activer l'alarme. Cette technologie est aussi à même d'assimiler les habitudes quotidiennes des utilisateurs, ce qui permet d'adapter automatiquement les paramètres de sécurité.

La technologie d'**analyse vidéo** constitue une autre application de l'IA dans les systèmes de sécurité. Elle permet d'analyser les images vidéo en temps réel et de détecter les activités anormales susceptibles de présenter un risque pour la sécurité. La technologie d'analyse vidéo enseigne au logiciel de sécurité tout ce qu'il doit considérer comme normal pour lui permettre d'identifier les comportements inhabituels et potentiellement nuisibles ; il



Cas concret : BuddyGuard FLARE

FLARE recourt à l'intelligence artificielle : la technologie permet d'identifier les visages et les sons dangereux et est capable d'avertir les services de secours via une application dédiée en cas d'alerte. Le cas échéant, FLARE permet à la centrale d'alarme de consulter toutes les données audio et vidéo en streaming et en direct.

s'agit là typiquement de détails pouvant échapper à la vigilance d'une personne. L'IA combinée à des caméras peut donc aussi apprendre à faire la différence entre des visiteurs et des intrus. De plus en plus, c'est la **caméra elle-même** qui effectue cette **analyse**.

Par ailleurs, les nouveaux **systèmes de détection audio** basés sur l'IA peuvent identifier et répertorier des bruits suspects afin de repérer et de prévenir d'éventuels cambriolages. Il s'agit d'un renfort efficace aux systèmes de détection visuelle des menaces.

Bon nombre de ces innovations **sont également utilisées dans les systèmes de sécurisation des entreprises**. Effectivement, les technologies telles que la reconnaissance faciale et la détection audio et visuelle des menaces permettent d'améliorer la sécurité des entreprises.

L'intelligence artificielle génère plusieurs possibilités pour le secteur : de travailler de façon **prédictive**, de **filtrer et vérifier mieux encore les alarmes**.

3.3 Drones

Les drones sont des aéronefs sans équipage et sans pilote également appelés « UAV » ou « unmanned aerial vehicles ».

Tant les acteurs publics que privés utilisent de plus en plus le drone. Dans plusieurs pays, les **services d'incendie** et la **police** disposent déjà des drones pour évaluer des situations dangereuses, pour repérer des personnes disparues, instruire rapidement des accidents, etc.

Dans le **secteur privé** aussi, les drones sont utilisés plus fréquemment pour inspecter des installations techniques ou pour appuyer les missions de surveillance. **Alarm.com** a annoncé récemment être en train de mettre au point un **drone de sécurité « smart home »**. Ce drone serait capable de voler tant à l'intérieur qu'à l'extérieur d'un bâtiment lorsque des activités inhabituelles sont observées. Au lieu de patrouiller en permanence, les drones d'Alarm.com ne réagiront et ne décolleront que si un autre dispositif a été activé, par exemple un capteur de mouvement fixé aux luminaires. Grâce aux données des autres appareils « smart home », les drones sauront où se rendre. Ils filmeront ou enverront les images en streaming et en direct sur le téléphone portable d'un utilisateur. En vol, ils utiliseront les caméras et autres capteurs de bord pour faire le tour d'une pièce tout en évitant les obstacles.

Les drones sont généralement équipés de **caméras**. Pour le secteur des centrales d'alarme agréées, ces caméras peuvent donc servir à **vérifier les alarmes** d'une part. D'autre part, les centrales d'alarme peuvent envoyer des drones en cas d'**intervention**, en appui d'autres parties prenantes. Ces drones pourraient par exemple envoyer des **images en streaming et en direct** aux services de secours ou aux entreprises de gardiennage.

Cas concret : police de Dubaï

Avant la fin de l'année 2017, la police de Dubaï envisage de se doter d'une voiture robot autonome pouvant faire office d'unité de surveillance mobile. L'« O-R3 » est équipée d'un drone intégré avec caméra capable également de suivre des personnes hors route.



En Belgique, les possibilités en matière de drones sont encore quelque peu **limitées** par le **cadre juridique** actuel puisque la loi impose de toujours garder en ligne de mire ou un contact visuel avec le drone. Récemment, la **Suisse** a été le premier pays à autoriser une entreprise logistique, Matternet, à faire voler des drones au-dessus de **régions densément peuplées**. Matternet va se doter cette année encore d'un **réseau permanent de drones autonomes**. Ces drones transporteront des échantillons tels que des tests sanguins entre les hôpitaux et les laboratoires.

4. Nette confirmation de la nécessité d'une approche intégrale de la sécurité

Les différentes tendances sociales, économiques et technologiques font qu'il est de plus en plus **difficile** de lutter à la fois contre l'insécurité objective et contre le sentiment subjectif d'insécurité. Il est évident qu'il faut une **approche intégrale de la sécurité** et une **collaboration** intégrée et coordonnée entre les différents intervenants de la sécurité, tant au niveau politique qu'au niveau des parties prenantes privées et publiques. Le secteur souhaite proposer lui-même une **vision claire** pour **contribuer activement** à cette sécurité intégrale.

Partie 3 | Notre vision

La sécurité est un droit fondamental. Le secteur veut donc exploiter les avancées technologiques et faire un usage plus intensif de ses connaissances spécialisées pour contribuer de manière efficace à un environnement plus sûr pour les citoyens, les organisations, les entreprises et les autorités.

Aujourd'hui, le secteur crée de la valeur ajoutée pour différentes parties prenantes en se concentrant sur ses domaines clés que sont le cambriolage et le vol et sur son rôle de filtre des fausses alertes. Le secteur veut **faire un usage plus intensif** de ses connaissances spécialisées, de sa disponibilité permanente et de ses solutions technologiques avancées pour créer encore plus de **valeur ajoutée** pour la **société** et jouer un **rôle actif dans la sécurité intégrale**. Dans sa vision, le secteur a défini les priorités suivantes.



Prévention, protection efficace et assistance en étroite collaboration avec les parties prenantes du secteur

Rôle plus large dans la lutte contre l'insécurité : de la centrale d'alarme à la "centrale d'événements"



Haut niveau d'**assurance qualité** pour l'**ensemble de la chaîne**



Coordination des parties prenantes concernées

Ancrage local dans un **contexte globalisé**



1. Prévention, protection efficace et assistance en étroite collaboration avec les acteurs pertinents

Le secteur entend jouer un rôle majeur à chaque étape de la chaîne de la prévention, de la protection et de l'assistance.

Prévention

Il veut mettre davantage l'accent sur la prévention et passer de la gestion des alertes à la **gestion proactive des situations**. Cet élément de la vision est étayé par la rapidité des évolutions technologiques qui permettent même de travailler de façon prédictive. Pour ce faire, le secteur tient à **travailler en étroite collaboration** avec les acteurs pertinents tels que les assureurs, (les services de prévention de) la police et les services d'incendie.

Plusieurs **zones de police** se servent par exemple des **images de caméras** pour prévenir les problèmes. La police indique également que l'installation d'un dispositif de vidéosurveillance dans un quartier a un effet préventif. Aux Pays-Bas, cette surveillance par caméras axée sur la sécurité et la qualité de vie se fait déjà dans le cadre de partenariats public-privé appelés « Regionale Toezicht Ruimten ».

Les **assureurs** jouent également un rôle crucial à cette étape de la chaîne. Ils attachent de l'importance aux **normes** et aux **labels de qualité** tels

qu'INCERT et BOSEC qui ont un impact en matière de prévention essentiellement. Il est important que ces normes continuent de **s'aligner sur les nouvelles potentialités technologiques**. Par ailleurs, le secteur tient aussi à encourager une **approche intégrée** par une conjonction optimale de mesures de prévention et de protection. Pour ce qui concerne les bâtiments commerciaux et industriels par exemple, les assureurs peuvent imposer des exigences spécifiques. Celles-ci concernent généralement les systèmes d'aspersion automatique d'eau (sprinklers). La gestion des systèmes de sprinklage permettrait au secteur de renforcer un peu plus la sécurité en matière de lutte contre l'incendie.

Protection efficace

Le secteur cherche à atteindre un **meilleur taux de raccordement** des systèmes d'alarme neufs et existants à une centrale d'alarme afin de pouvoir garantir une protection efficace au client final. Les salles de contrôle optent pour une disponibilité permanente et travaillent selon des procédures et avec des systèmes de back-up en vue d'assurer **un traitement continu de toutes les alarmes entrantes**. Aussi, elles travaillent en étroite collaboration avec les services de police et autres services d'intervention afin de garantir une **action rapide et appropriée**.

Plusieurs **assureurs**, y compris à l'étranger, **approuvent** cette protection efficace. Ils octroient des réductions sur les assurances de bâtiments lorsque ceux-ci sont équipés d'un système d'alarme assorti d'une surveillance ou imposent le raccordement à une centrale d'alarme dans certaines situations. Ces réductions peuvent être plus importantes encore si des détecteurs d'incendie et d'eau sont également raccordés au système.

Assistance

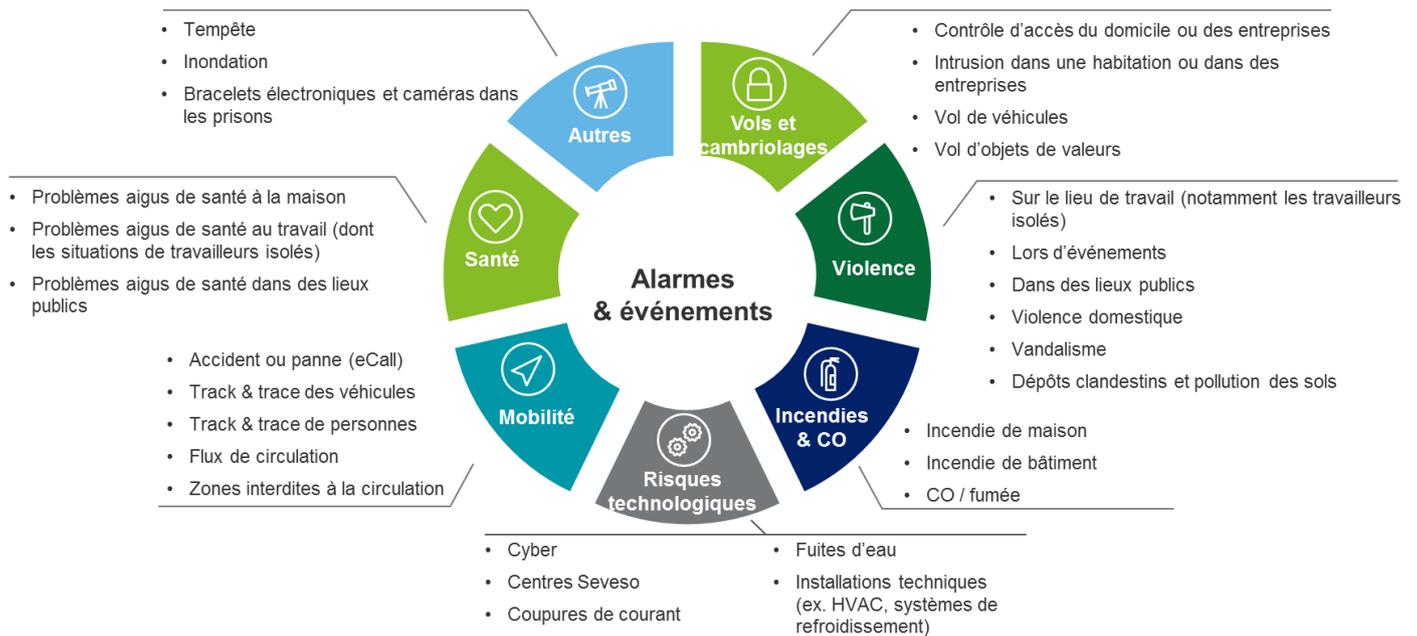
Enfin, le secteur souhaite jouer un rôle majeur en matière d'assistance. D'une part, il peut aider les **services d'intervention** par un échange d'informations (en temps réel) et la fourniture d'accès à distance ; d'autre part, il souhaite continuer à porter **lui-même** assistance aux clients finaux.



2. Rôle plus large dans la lutte contre l'insécurité : de la centrale d'alarme à la centrale « d'événements »

Les évolutions technologiques telles que l'intégration des systèmes d'alarme et des caméras intelligentes ou l'utilisation de capteurs connectés génèrent **plusieurs nouvelles possibilités en termes de surveillance**. Et l'**expertise** accumulée par le secteur en matière de filtrage des fausses alertes, de vidéosurveillance et de services à distance peut aussi représenter une plus-value **pour un groupe plus large de parties prenantes**.

Selon la vision de l'avenir qu'a le secteur, les centrales d'alarme seront des **centrales « d'événements »** qui traiteront un large éventail d'alertes et géreront des **événements**. La **figure** ci-dessous donne un aperçu des alarmes et événements éventuels pour lesquels le secteur peut jouer un rôle important.



La liste des **domaines dans lesquels le secteur souhaite s'investir en priorité** est consultable dans la **Partie 4 | Concrétisation opérationnelle de notre vision**. Il est important de signaler à cet égard que le secteur est constitué d'un **ensemble dynamique d'entreprises différentes** qui se concentreront sur certains **domaines** en fonction du **savoir-faire qui leur est propre**.

3. Coordination des acteurs pertinents

La centrale d'alarme est *le* lieu par excellence où peuvent être **rassemblées en un seul endroit toutes les données pertinentes à propos des événements et alarmes divers**. Ces données peuvent être constituées d'alarmes, mais aussi d'images, de sons, de lieux, etc. La centrale d'alarme est **idéalement placée** pour **analyser** des données et pour, le cas échéant, **mobiliser** les intervenants adéquats. La centrale d'alarme entend améliorer de la sorte **l'efficacité** (ne faire intervenir les parties prenantes qu'en cas de nécessité réelle) et contribuer à une **réaction rapide et adéquate**.

Par ailleurs, la centrale d'alarme peut aussi se servir de ces données pour **aider** les parties prenantes à prendre de meilleures décisions et améliorer ainsi **l'efficacité** de la prévention et des interventions.

Dans son rôle de « **régisser** », le secteur ambitionne une **collaboration** intégrée et optimisée avec les parties prenantes concernées :

- **Intégrée** : avec des rôles et responsabilités clairement définis, des procédures et un échange d'informations structuré et bidirectionnel (par exemple, une bonne communication pendant les interventions, une concertation stratégique et un échange fréquent d'expériences)
- **Optimisée** : une alliance stratégique qui permet à chaque partenaire de se concentrer sur ses compétences fondamentales et d'exploiter autant que possible ses atouts



4. Un niveau d'assurance qualité de pointe pour l'ensemble de la chaîne

Les membres de l'ACA visent un niveau d'assurance qualité de pointe pour l'ensemble de la chaîne afin de faire face comme il se doit aux risques actuels tels que les **cybermenaces** et de garantir un **service efficace**. Cette assurance qualité devrait comprendre trois volets :

- Une **certification moderne** pour l'ensemble de la chaîne qui respecte les normes européennes ;
- La **qualité technique** et l'**interopérabilité** des systèmes ;
- Le respect de la **vie privée**.

D'après la CoESS (Confédération européenne des services de sécurité), la **Belgique** fait figure de **pionnière** pour ce qui est de **décrire et réglementer correctement les activités de surveillance**. D'ailleurs, le secteur belge sert souvent de référence aux autres pays. On doit cela notamment à la **rigueur de la législation** belge en matière de surveillance privée. Une étude comparative de la CoESS datant de 2015 a classé la Belgique dans une catégorie composée d'une poignée de pays européens à la législation « très stricte ». Par exemple, les opérateurs sont obligatoirement triés sur le volet par le SPF Intérieur et les services de sûreté, sont sélectionnés sur la base de critères d'admission très stricts et doivent suivre une formation légale de 70 heures. Outre les exigences imposées par la loi, **le secteur prend lui-même des mesures également** pour garantir la qualité, par exemple une formation interne complémentaire approfondie, des accords de niveau de service stricts et l'obtention de certificats ISO.



5. Ancrage local dans un contexte globalisé

Même dans un secteur qui s'internationalise, le facteur humain et les affinités locales gardent toute leur importance. Le secteur tient à conserver un ancrage local afin de pouvoir mobiliser des opérateurs possédant les **compétences linguistiques adéquates** et l'**expérience du contexte local** comme la configuration des bâtiments et des lieux publics qui peut fortement varier d'un pays à l'autre.

De plus, il juge l'ancrage local important également pour se coordonner régulièrement avec le **régulateur et les autorités** et contribuer activement à l'élaboration des politiques.

Partie 4 | Concrétisation opérationnelle de notre vision

Afin de remplir son rôle de « centrale d'événements », le secteur tient avant tout à s'investir dans un certain nombre de domaines connexes.

1. Priorisation des domaines

Pour définir ses priorités à court terme, le secteur a pris deux **critères** majeurs en considération :

- En adéquation avec l'objectif/la **raison d'être fondamentale** du secteur, à savoir contribuer à la création d'un environnement sûr pour les citoyens, les organisations, les entreprises et les autorités ;
- Possibilité pour le secteur de créer de la **valeur ajoutée** pour les parties prenantes concernées.

Le secteur souhaite accorder la priorité aux domaines qui sont étroitement liés à sa raison d'être fondamentale et pour lesquels il peut mobiliser ses compétences afin de créer de la valeur ajoutée pour les parties prenantes concernées.

Le secteur pense pouvoir (continuer) à s'engager de manière significative dans les domaines prioritaires suivants :



2. Zoom sur les domaines prioritaires

Le secteur a une vision claire de la concrétisation de ses cinq domaines prioritaires.



2.1 Cambriolage et vol

L'évolution des **progrès technologiques** génère des opportunités pour le secteur de créer encore plus de valeur ajoutée dans ses domaines fondamentaux que sont le cambriolage et le vol.

Grâce à l'**intégration croissante des systèmes d'alarme et des caméras (intelligentes)**, le secteur dispose en effet de meilleurs **moyens de vérification** et d'une mine d'**informations** supplémentaire. Par ailleurs, il devient également possible de travailler de plus en plus de manière **prédictive** et **préventive**. Les caméras intelligentes (reposant sur l'intelligence artificielle) sont déjà capables aujourd'hui de prédire les cambriolages et le vol, ce qui permet de mieux les prévenir.

Outre le traitement des alarmes, le secteur désire s'engager davantage à fournir des **services à distance** tels que le contrôle d'accès à distance et les rondes virtuelles.

Enfin, l'ACA souhaite, avec d'autres parties prenantes, **sensibiliser plus encore** aux avantages d'un raccordement à une centrale d'alarme. L'ACA pourrait à cet effet lancer des campagnes de communication avec d'autres acteurs du secteur de la sécurité.



2.2 Incendie et sécurité des bâtiments

L'année dernière, 78 personnes ont perdu la vie dans l'incendie d'une habitation ; 32 personnes déjà sont décédées au cours de la première moitié de cette année. À titre de comparaison, aux Pays-Bas – pays qui compte 6 millions d'habitants de plus –, seules 14 personnes sont mortes dans un incendie au cours de la même période. Selon le commandant des pompiers Marc Ceyskens, également président de l'organisme faïtier Brandweervereniging Vlaanderen (BVV), **la Belgique est un mauvais élève** par rapport aux Pays-Bas ou à l'Allemagne **en matière d'incendies d'habitations**. C'est pour cette raison que certaines régions en Belgique ont modifié récemment la réglementation relative aux détecteurs de fumée. Toujours selon Marc Ceyskens, beaucoup d'habitations en Belgique ne sont toujours **pas équipées de détecteurs de fumée ou en comptent trop peu**. Souvent, les **détecteurs d'incendie présents ne fonctionnent plus** depuis longtemps. Pourtant, la nouvelle réglementation ne prévoit aucunement l'obligation de raccorder les détecteurs d'incendie à une centrale d'alarme alors que cela permettrait d'assurer un bon suivi des alarmes et du fonctionnement des détecteurs.

En 2014, les services d'incendie ont effectué 18 237 **déplacements sans intervention**. En d'autres termes, les services d'incendie sortent de leur caserne 50 fois par jour pour rien. Les responsables de ces fausses alertes sont notamment des alarmes incendie vétustes ou mal entretenues, des personnes communiquant des informations erronées et des plaisantins. Et la loi concernant la présence de détecteurs d'incendie devenant toujours plus stricte, le nombre d'alertes ne va faire qu'augmenter.

Il est clair que **les différentes parties prenantes peuvent mieux faire** en matière d'incendie. Les membres de l'ACA peuvent vérifier la **sécurité, l'intégrité et la fiabilité des bâtiments** en matière d'incendie, mais aussi de monoxyde de carbone et de fuites d'eau. Ils peuvent surveiller à distance



Cas concret : Deep Sentinel

La start-up Deep Sentinel est en train de redéfinir l'usage des caméras dans les systèmes de sécurisation. Un programme d'intelligence artificielle analyse les images et recherche des schèmes/signaux d'alerte visuels susceptibles de prédire la survenance d'un délit sur une propriété, par exemple une effraction ou le vol d'un véhicule. La start-up fondée par David Selinger, un ancien manager d'Amazon, a déjà attiré 7,4 millions de dollars de financement.

l'infaillibilité et le fonctionnement efficace de divers détecteurs et jouer un rôle de conseil.

En 2016, le secteur a reçu environ 120 000 alertes d'incendie. Moins de 4 % de ces alarmes ont été relayées aux services d'incendie. Dans des situations où la technologie le permet, le secteur peut **vérifier** avec fiabilité les alertes émises par des détecteurs et **réduire** ainsi drastiquement le **nombre de fausses alertes**.

De plus, il peut **fournir un accès à distance** aux services d'incendie lors d'interventions. Et les informations recueillies par les membres de l'ACA peuvent servir à l'**appui des interventions des services d'incendie** et aux **activités d'assistance des assureurs**.

2.3 Criminalité violente, incivilités et dépôts clandestins

Selon une récente étude commandée par la société publique flamande de gestion des déchets, l'OVAM, la Flandre a dépensé un total d'un peu plus de 187 millions d'euros en 2015, soit **29 euros par habitant**, pour lutter contre les débris et les dépôts clandestins. De cette somme, 103 millions d'euros ont été consacrés aux débris, soit une augmentation de pas moins de 42 millions d'euros par rapport à 2013. Ce sont les **communes qui supportent la majeure partie de ces coûts**, soit environ 176 millions d'euros au total ou 94 pour cent du montant total de la facture. Les dépôts clandestins représentent un problème onéreux dans le reste du pays également.

Compte tenu de leur impact social majeur, la **criminalité violente** et les **incivilités** constituent également deux phénomènes importants en matière de sécurité auxquels les services de police et autres autorités concernées consacrent une attention particulière dans le cadre de l'**actuel plan national de sécurité** (2016-2019).

Le secteur peut offrir un **appui au moyen de caméras** pour prévenir ces phénomènes majeurs et y réagir, **tant sur le domaine privé que public**. Grâce à la gestion **proactive** de caméras intelligentes entre autres, il est par exemple possible de réagir plus rapidement aux attroupements et d'améliorer la force de flagrant délit des interventions réactives des autorités contre les dépôts clandestins et la criminalité violente.

Enfin, le secteur peut aussi veiller sur des personnes dans des lieux à risque grâce à la **protection rapprochée virtuelle**. Il peut par exemple assurer un accompagnement à distance lors de l'ouverture et de la fermeture. Dans ce cas, la centrale d'alarme sait à quel moment le travailleur d'une entreprise pénètre dans un certain périmètre et peut observer les images lors de l'ouverture et de la fermeture. En cas de situation étrange ou présence de personnes suspectes, la centrale d'alarme peut envoyer de l'aide ou prévenir la police.

2.4 Travailleurs isolés

Le secteur peut veiller à la sécurité des travailleurs isolés. Ceux-ci **travaillent seuls sans supervision directe** et sont donc vulnérables aux agressions et aux risques de sécurité. Parmi les exemples possibles de travailleurs isolés, citons les techniciens d'opérateurs de télécommunications et de fournisseurs d'énergie, les personnes travaillant seules dans un environnement de production et les travailleurs mobiles tels que les chauffeurs de poids lourds, les commerciaux, les infirmiers à domicile et les médecins généralistes.



Cas concret : ville de Renaix

Une petite ville comme Renaix, qui compte environ 26 000 habitants, dépense approximativement **90 000 euros** par an pour l'enlèvement des graffitis et des dépôts clandestins et la lutte contre le vandalisme. Dans certains quartiers, les bulles à verre sont surveillées par des caméras.

Cas concret : marathon contre les débris

En septembre, plus de mille agents de police, fonctionnaires SAC, assistants de prévention et de sécurité et gardiens de la paix, gardes forestiers et champêtres répartis sur le territoire des cinq provinces flamandes ont pris part à la « Handhavingsweek » (Semaine de la préservation). Une semaine durant, ils se sont rendus sur le terrain pour effectuer des contrôles supplémentaires concernant les dépôts clandestins. Des moyens technologiques tels que des caméras ont été déployés.

Plusieurs pays tels que le Royaume-Uni, l'Allemagne, la France et l'Espagne ont inscrit la protection des travailleurs isolés dans la loi.

Favorisée par les « **new ways of working** », la nécessité de prévoir des solutions pour les travailleurs isolés ne va cesser de croître. La Belgique encourage également le travail flexible et opérationnel, y compris le **télétravail** occasionnel. La question de la responsabilité en cas d'accident d'une personne travaillant à domicile n'est pas encore claire aujourd'hui.



2.5 Circulation et mobilité

Enfin, le secteur entrevoit plusieurs possibilités de mobiliser ses compétences en matière de circulation et de mobilité.

Grâce au contrôle d'accès à distance ou services de portier vidéo, les centrales d'alarme peuvent **fournir, à distance, un accès contrôlé** à un site et/ou autoriser la sortie d'un site. Un opérateur assure l'accompagnement à distance en s'aidant de la vidéo.

Le secteur fournit déjà ce service à plusieurs sites privés, par exemple pour les **livraisons de nuit**, et ce sans nécessiter la présence permanente d'une personne sur place. Le secteur entrevoit aussi pour l'avenir plusieurs avantages à pourvoir ce service **sur le domaine public** afin de fournir un accès contrôlé aux **zones piétonnes**, par exemple pour les livraisons spéciales ou un déménagement, etc.

Aussi, de plus en plus de **caméras** intelligentes sont installées en rue. La **nécessité de procéder à un filtrage et à une vérification par un humain** va donc augmenter. Même si les caméras deviennent plus intelligentes, elles restent sensibles aux facteurs environnementaux et génèrent de **fausses alertes**.

Enfin, le secteur souhaite jouer un rôle dans le système **eCall**. Installé dans les voitures, le système eCall lance automatiquement (ou manuellement au moyen d'un bouton poussoir) un appel d'urgence à une centrale d'alarme en cas d'accident. Aussi, le système communique immédiatement des informations essentielles telles que la localisation exacte et l'heure de l'accident. À partir d'avril 2018, toutes les nouvelles voitures en Europe devront être équipées du système eCall. Le secteur pourrait apporter des **solutions internationales** dans ce domaine.

Partie 5 | En quête d'un win-win

Dans le cadre d'une approche intégrale de la sécurité, le secteur souhaite collaborer activement avec les parties prenantes publiques et privées et leur apporter de la valeur ajoutée.

1. Valeur ajoutée pour la société et les citoyens

Meilleure sécurité publique

En tant qu'acteur actif dans la sécurité intégrale, le secteur pourra contribuer à la sécurité publique et au sentiment de sécurité des citoyens. En effet, le secteur peut apporter un plus en termes d'**expertise spécialisée, de disponibilité permanente, de technologies, de délais de réaction très courts** et d'**informations** dans des domaines tels que l'incendie, la criminalité violente, les dépôts clandestins et la mobilité (voir le chapitre « Concrétisation opérationnelle de la vision »). Grâce à un partenariat intégré et optimisé entre les acteurs privés et publics, il est possible de garantir une meilleure sécurité publique et de mieux répondre à l'évolution des menaces.

Approche intégrée de l'insécurité liée à l'utilisation des bâtiments

Le secteur peut jouer un rôle majeur dans le cadre d'une approche intégrée de l'insécurité dans les bâtiments (**incendie, monoxyde de carbone, fuites d'eau, cambriolage, violence**, etc.). La centrale d'alarme est idéalement placée pour gérer tous ces phénomènes, pour mobiliser les intervenants adéquats et pour les aider, si nécessaire, par des informations en cas d'intervention. De plus, le secteur peut fournir, à distance, un accès aux services de secours et d'intervention. Cela permet une **meilleure prévention** et une **réaction plus rapide et plus ciblée**, ce qui peut limiter les dommages potentiels.

C'est principalement dans les situations où les personnes sont absentes, qu'elles sont en situation de détresse ou qu'elles ne donnent aucune suite/ne sont pas en mesure de donner suite aux alarmes locales ou aux notifications sur leur smartphone, que le secteur peut détecter les incendies, les fuites d'eau, le monoxyde de carbone, les cambriolages ou les vols et réagir adéquatement. Le secteur est disponible 24 heures sur 24 et 7 jours sur 7 et dispose de systèmes de back-up pour assurer ce service à tout moment.

2. Valeur ajoutée pour les parties prenantes publiques

2.1 Valeur ajoutée pour le Service public fédéral Intérieur

La valeur ajoutée que le secteur peut créer pour le SPF Intérieur repose sur les piliers suivants :

- Élaborer ensemble une **politique tournée vers l'avenir** qui permet une collaboration intégrée et coordonnée entre les acteurs de la sécurité et obtenir des **statistiques** pour étayer **l'élaboration de politiques et leur évaluation**



■ Domaine important pour la partie prenante ■ Domaine moins important



■ Domaine important pour la partie prenante ■ Domaine moins important

- Se faire une idée de la **faisabilité** de revoir les politiques en fonction de l'**expérience provenant du terrain**
- Positionnement de tous les acteurs de la sécurité en fonction de leurs **compétences fondamentales** et meilleure coordination entre les différentes parties prenantes pour une **mobilisation des ressources plus efficiente (économiquement)** et une priorité accrue accordée aux missions stratégiques
- Filtrage des fausses alertes et des alarmes non urgentes, vérification efficace et, donc, poursuite de la **réduction du nombre d'interventions superflues** des services d'incendie et de la police
- Accroissement de l'**efficacité** par une détection plus rapide des situations requérant une intervention de la police ou des services d'incendie
- **Limitation du préjudice pour la société** par des interventions plus rapides et plus efficaces des services d'incendie et de la police grâce au partage de données (en temps réel) et la fourniture d'accès à distance
- **Avantage en matière d'innovation** grâce au fonctionnement du marché : stimuler l'innovation en laissant le marché opérer et permettre aux acteurs publics d'accéder aux technologies de pointe (éventuellement importées de l'étranger)

2.2 Valeur ajoutée pour les administrations locales

Le secteur peut aussi créer de la valeur ajoutée pour les administrations locales dans les différents domaines qu'il a identifiés dans sa vision :

- **Efficience économique** par une mobilisation optimale des ressources disponibles
- **Exploitation optimale des caméras existantes** sur le domaine public (sur les plans tant préventif que réactif)
- Prévention et lutte plus efficace contre les infractions et la **criminalité violente dans les lieux à risque** tels que les centres-villes, les quartiers (à problèmes), les rues commerçantes et les centres commerciaux, les gares, les places, les parcs et les domaines récréatifs et les guichets mêmes de l'administration
- Amélioration de la **force de flagrant délit** des interventions réactives des autorités
- Renforcement du **sentiment de sécurité** des entreprises, des visiteurs et des résidents dans les zones piétonnes et les zones (commerçantes) fréquentées, **sans mesures draconiennes** (telles que des blocs de béton) et de manière **économique** (notamment grâce à la possibilité d'instaurer à nouveau une surveillance physique dans ces lieux)
- Limitation du coût des **dépôts clandestins et du vandalisme**

2.3 Valeur ajoutée pour la police

Une **collaboration** avec la police **basée sur la chaîne de sécurité** et assortie d'un respect mutuel des responsabilités des partenaires impliqués peut comporter plusieurs avantages :

- **Poursuite de la réduction du nombre d'interventions superflues** grâce au filtrage des fausses alertes et alarmes non urgentes et à une vérification efficace



- Possibilité de se **centrer sur ses missions fondamentales** (p. ex., proposer une alternative à la surveillance pendant les vacances et en cas d'absence)
- **Interventions plus efficaces** grâce au partage d'informations (p. ex., les images vidéo) ou à la détection plus précoce des délits
- **Accès à des technologies de pointe** telles que des drones et des centres mobiles sans engendrer des coûts d'investissement élevés (en collaboration avec le secteur du gardiennage)

2.4 Valeur ajoutée pour les services d'incendie

Le raccordement des détecteurs d'incendie et de fuites d'eau à une centrale d'alarme présente plusieurs avantages pour les services d'incendie :

- Amélioration des **dossiers d'intervention** grâce au partage d'informations techniques à jour en matière de détection d'incendie et d'informations sur le bâtiment
- **Interventions plus efficaces** grâce au partage de données en temps réel telles que les images vidéo, la localisation du ou des foyers d'incendie, la présence d'habitants/d'utilisateurs, etc. ou la détection plus précoce des situations d'urgence
- Contribuer aux **objectifs stratégiques** (réduction du nombre de victimes) et investir ensemble dans des systèmes appropriés de détection d'incendie

3. Valeur ajoutée pour les parties prenantes privées

3.1 Valeur ajoutée pour les assureurs

Grâce à une meilleure prévention et à une détection plus rapide des incendies, du monoxyde de carbone, des fuites d'eau, des cambriolages et des vols et à une réaction plus rapide et ciblée, le secteur peut **réduire le nombre de demandes d'indemnisation et limiter leur ampleur**.

De plus, les membres de l'ACA peuvent aussi recueillir et partager des **statistiques** et des **informations** pour :

- faciliter l'**expertise** effectuée par les assureurs ;
- réduire le nombre de **demandes d'indemnisation non fondées** ;
- améliorer la **prévention** et alimenter la **future standardisation**.

3.2 Valeur ajoutée pour les installateurs

À l'instar des membres de l'ACA, les installateurs sont confrontés à la rapidité des évolutions technologiques. Leur **rôle est en train d'évoluer** en raison notamment de l'abandon des réseaux analogiques en faveur des réseaux numériques (basés sur l'IP), de l'arrivée des appareils IoT, de l'intégration des systèmes d'alarme et des caméras (intelligentes) et des demandes extensives des clients.

Le secteur peut créer de la valeur ajoutée pour les installateurs en s'accordant en matière d'**utilisation des nouvelles technologies** et d'**application des nouveaux modèles économiques**. Le secteur peut aider les installateurs à suivre les évolutions technologiques et à satisfaire la demande des clients. En effet, le rôle de la centrale d'alarme devient encore plus important dans un environnement de sécurité où la caméra occupe une place centrale.

Les deux secteurs peuvent partager leurs ressources pour sensibiliser les citoyens à la valeur ajoutée que représentent les systèmes d'alarme connectés.



■ Domaine important pour la partie prenante ■ Domaine moins important



■ Domaine important pour la partie prenante ■ Domaine moins important



■ Domaine important pour la partie prenante ■ Domaine moins important

3.3 Valeur ajoutée pour les entreprises

Le secteur peut également créer de la valeur ajoutée pour les entreprises dans différents domaines :

- **Approche intégrée de l'insécurité** liée à l'utilisation des **bâtiments**, y compris une meilleure prévention, une détection plus sûre et une réaction plus rapide et ciblée
- Les membres de l'ACA peuvent permettre aux **syndics** et aux **gestionnaires de bâtiments** spécifiquement de se centrer sur leurs **missions fondamentales**.
- **Économies d'échelle** grâce à une centrale d'alarme globale pour les **zones d'activité économique**
- **Back-up pour les centrales d'alarme internes** : les grandes entreprises actives dans certains secteurs tels que l'industrie chimique et le secteur pharmaceutique disposent de leur propre service d'incendie qui assure également la permanence de la centrale d'alarme interne. Lorsque ce service d'incendie est en intervention, la centrale d'alarme se retrouve donc exempte de personnel. Dans ces situations, le secteur peut alors jouer un rôle de back-up.
- **Sécurité accrue pour les travailleurs isolés et le personnel confronté à des situations à risque** : le secteur peut veiller sur la sécurité du personnel pour limiter les incidents et la responsabilité potentielle, réduire la rotation du personnel et éviter toute dégradation de l'image. La sécurité est un thème cher au cœur des syndicats également. Le secteur est idéalement placé pour créer de la valeur ajoutée à cet égard.
- **Efficiency économique par l'augmentation des services à distance**, notamment grâce à la possibilité d'instaurer à nouveau une surveillance physique (pour les livraisons de nuit, par exemple)

4. Valeur ajoutée pour le secteur

Le fait de repenser la sécurité intégrale et le positionnement de tous les acteurs de la sécurité en fonction de leurs compétences fondamentales crée la possibilité pour le secteur de **se développer** et de **continuer à investir dans les ressources humaines, l'innovation et les technologies**.

Enfin, l'implication à bon escient des membres de l'ACA dans la politique de sécurité intégrale est aussi une **reconnaissance** du partenaire fiable et compétent qu'est le secteur.



■ Domaine important pour la partie prenante ■ Domaine moins important

Partie 6 | Notre engagement

Le secteur souhaite s'engager afin de concrétiser sa vision et de créer effectivement de la valeur ajoutée pour les différentes parties prenantes pertinentes.

Le secteur a identifié les chantiers importants suivants.

1. Être un partenaire à part entière dans la sécurité intégrale

L'ACA représente aujourd'hui plus de 95 % des raccordements en Belgique. Pour pouvoir intervenir en qualité de partenaire à part entière dans la sécurité intégrale, le secteur souhaite mettre en place une **représentation permanente** assortie d'une capacité suffisante de dialogue et d'action.

Le secteur entend établir un **dialogue** permanent avec les autres **fédérations du secteur privé** dans la chaîne prévention-intervention-assistance et l'association belge représentant le secteur de la sécurité électronique (ALIA Security), et **jeter des ponts** entre celles-ci. Il aspire à parvenir à un win-win avec ces parties. Cela peut se traduire par des positionnements plus largement partagés vis-à-vis des responsables politiques et par un nombre accru de projets pilotes réussis.

En parallèle, le secteur veut se rapprocher davantage du **SPF Intérieur** afin d'être un **partenaire à part entière** dans la contribution à l'élaboration des **politiques**. La principale priorité du secteur est de **concrétiser** ensemble la **nouvelle loi-cadre** approuvée à l'été 2017.

L'ACA peut aussi devenir plus active au sein de la Confédération européenne des services de sécurité (**CoESS**), la **fédération sectorielle européenne**, et essayer de positionner davantage la Belgique comme une pionnière en matière de « centrales d'alarme de l'avenir ».

De plus, le secteur souhaite **collaborer plus étroitement** avec les **administrations locales** et les **acteurs privés et publics de la sécurité**. Il veut déployer des moyens pour mettre sur pied, en qualité de fédération sectorielle, des **projets pilotes** au niveau des zones de police locale, des zones d'incendie et des administrations locales lorsque cela est pertinent, et ce en collaboration avec des entreprises privées de gardiennage.

Enfin, le secteur veut investir plus dans la **communication** vis-à-vis du grand public à propos du raccordement aux centrales d'alarme.

2. Être à la pointe de l'innovation

L'ACA veut continuer à investir du temps et des moyens au niveau de la fédération sectorielle en matière d'**évolutions technologiques** et dans les domaines d'application de celles-ci. Le secteur souhaite **suivre** de près les évolutions technologiques, identifier les **applications pertinentes à l'étranger** et publier/**communiquer** les enseignements au grand public.

Les centrales d'alarme privées peuvent aussi servir d'« **environnement de test** » pour des projets pilotes.

3. Tendre vers la standardisation, l'interopérabilité des systèmes et la cybersécurité

L'interopérabilité des différents systèmes et la standardisation constituent un défi spécifique en matière de technologies et de fonctionnement en chaîne. Avec la Confédération européenne des services de sécurité (CoESS), l'ACA souhaite coordonner et stimuler l'**harmonisation des normes** en Belgique (par exemple, vis-à-vis des fournisseurs et des installateurs, des centres d'information et de communication [CIC] de la police, etc.).

De plus, elle veut s'investir pour apporter une réponse adéquate aux **cybermenaces** et garantir le respect de la **vie privée**.

Partie 7 | Pistes de réflexion pour l'avenir

Pour jeter les bases des étapes ultérieures, le secteur a élaboré des suggestions concernant la collaboration avec les différentes parties prenantes et a identifié des actions concrètes.

1. Collaboration avec les parties prenantes publiques

1.1 Collaboration avec le Service public fédéral Intérieur

Le secteur est désireux d'engager un dialogue avec les directions générales « Sécurité et prévention » et « Sécurité civile » du SPF Intérieur et d'évoluer vers une **concertation structurelle** étayée par des **statistiques** objectives et, éventuellement, des **indicateurs clés de performance**.

Voici les actions concrètes qu'il entrevoit.

| Domaine(s) | Sécurité civile | ACA |
|---|--|--|
| <ul style="list-style-type: none"> • Incendie et sécurité des bâtiments | <ul style="list-style-type: none"> • Amorcer une concertation avec la BVV, la FRCSPB et les corps de sapeurs-pompiers • Faire remonter l'information lorsqu'une alarme transmise concernait un incendie réel • Mieux sensibiliser à la sécurité incendie et évoluer vers une législation plus stricte | <ul style="list-style-type: none"> • S'engager à vérifier (lorsque la technologie le permet) • Impliquer le SPF Intérieur dans les projets pilotes • Communiquer plus avant avec les autorités et les services d'incendie à propos des avantages d'une approche intégrée, y compris le raccordement à une centrale d'alarme • Recueillir des statistiques pour étayer l'élaboration des politiques et l'évaluation |

| Domaine(s) | Sécurité et prévention | ACA |
|--|---|--|
| <ul style="list-style-type: none"> • Cambrilage et vol • Criminalité violente, incivilités et dépôts clandestins • Travailleurs isolés • Circulation et mobilité | <ul style="list-style-type: none"> • En collaboration avec l'ACA, concrétiser la nouvelle loi-cadre, y compris le volet « vidéosurveillance » sur le domaine public – passer de groupes de travail ponctuels à une collaboration plus large et plus structurelle • Fournir un appui pour accélérer les projets pilotes du secteur avec d'autres parties prenantes | <ul style="list-style-type: none"> • Devenir un partenaire stratégique fiable pour la mise en œuvre et l'évaluation de la future politique en matière de sécurité et de prévention • Impliquer le SPF Intérieur dans les projets pilotes • Recueillir des statistiques pour étayer l'élaboration des politiques et l'évaluation • Communiquer à propos de la valeur ajoutée que représente le raccordement à une centrale d'alarme |

1.2 Collaboration avec les administrations locales

Le secteur a la volonté de mettre sur pied des **partenariats public-privé** avec des administrations locales qui seront précédés par un nombre limité de **projets pilotes** mûrement choisis en collaboration avec d'autres parties prenantes.

Pour le vol et les cambriolages en particulier, le secteur entrevoit des possibilités de déployer à plus grande échelle le concept néerlandais « **Keurmerk Veilig Wonen** » (label d'habitation sécurisée) et le certificat « **Prévention cambriolage** » dans certaines zones de police belges, et ce en collaboration avec la police et les administrations locales.

Voici les actions concrètes qu'il entrevoit.

| Domaine(s) | Administrations locales | ACA |
|--|---|---|
| <ul style="list-style-type: none"> • Criminalité violente, incivilités et dépôts clandestins • Circulation et mobilité | <ul style="list-style-type: none"> • En collaboration avec le secteur et la zone de police, mettre sur pied des projets pilotes dans les domaines suivants : <ul style="list-style-type: none"> • Appui de la vidéosurveillance pour la prévention et la réaction à la criminalité violente, aux incivilités et aux dépôts clandestins • Contrôle d'accès à distance pour les zones piétonnes et les zones (commerçantes) fréquentées • Appui de la vidéosurveillance en matière de mobilité et de contrôle d'accès | <ul style="list-style-type: none"> • Collaborer avec la police, les communes, les citoyens et les entreprises pour résoudre de manière efficace et structurée les problèmes communs • Être un interlocuteur à l'écoute des doléances des citoyens (y compris en matière de respect de la vie privée) |
| <ul style="list-style-type: none"> • Cambriolage et vol | <ul style="list-style-type: none"> • Impliquer le secteur dans des projets tels que le certificat « Prévention cambriolage » | <ul style="list-style-type: none"> • Soutenir les campagnes de prévention et de communication de la police |

1.3 Collaboration avec la police

Concernant les modalités concrètes de la collaboration avec la police, le secteur entrevoit des possibilités d'appliquer le concept des « **Regionale Toezicht Ruimten** » **mis en place à Eindhoven et Nimègue (RTR-NL)** à la Belgique.

Les RTR-NL sont un partenariat public-privé axé sur la sécurité et la qualité de vie, le tout appuyé par la vidéosurveillance. Concrètement, ce concept se traduirait de la manière suivante en Belgique :

- **Surveillance proactive**, y compris sur le **domaine public**, par les membres de l'ACA **sous la houlette de la police**
- Une **collaboration basée sur la chaîne de sécurité** assortie d'un respect mutuel des responsabilités des partenaires impliqués
- À l'heure actuelle, celle-ci devrait encore se faire dans le cadre des infrastructures de la police. À terme, il peut toutefois être intéressant d'utiliser les **infrastructures du secteur privé** pour des motifs d'économies d'échelle.

De plus, le secteur souhaite travailler sur l'**échange d'informations** avec la police. En effet, le secteur peut disposer de données susceptibles d'aider la

police lors d'interventions, par exemple les notifications de localisation SIG, les coordonnées de contact, la situation, les issues de secours, etc.

Le secteur a identifié les actions suivantes.

| Domaine(s) | Police | ACA |
|--|---|---|
| <ul style="list-style-type: none"> • Criminalité violente, incivilités et dépôts clandestins • Travailleurs isolés • Circulation et mobilité | <ul style="list-style-type: none"> • En collaboration avec les administrations locales et les zones de police, mettre sur pied des projets pilotes dans les domaines suivants : <ul style="list-style-type: none"> • Appui de la vidéosurveillance pour la prévention et la réaction à la criminalité violente, aux incivilités et aux dépôts clandestins • Contrôle d'accès à distance pour les zones piétonnes et les zones (commerçantes) fréquentées • Appui de la vidéosurveillance en matière de mobilité | <ul style="list-style-type: none"> • En collaboration avec la police, développer davantage une vision basée sur des constatations faites sur le terrain pour ce qui concerne le cadre légal requis (échange de données, partenariat public-privé, respect de la vie privée, etc.) • Organiser la concertation avec les représentants de quartier (y compris les RIQ) pour mieux comprendre les attentes et les difficultés et renforcer l'implication/élargir éventuellement le rôle des RIQ |
| <ul style="list-style-type: none"> • Cambrassage et vol | <ul style="list-style-type: none"> • Impliquer le secteur dans des projets tels que le certificat « Prévention cambriolage » • Faire remonter l'information lorsqu'une alarme transmise concernait réellement une effraction ou un vol • Donner la priorité aux alarmes vérifiées (éventuellement moyennant des conditions telles que la vérification vidéo) | <ul style="list-style-type: none"> • Soutenir les campagnes de prévention et de communication de la police • Tendre vers un échange électronique des données |

1.4 Collaboration avec les services d'incendie

Le secteur est désireux d'évoluer vers un modèle de **concertation** avec les services d'incendie et de conclure des **accords concrets** quant à la collaboration.

Sur le plan opérationnel, le secteur veut travailler sur l'**échange d'informations** avec les services d'incendie. En effet, le secteur peut partager des données telles que des informations techniques relatives à la détection incendie et des informations sur les bâtiments.

| Domaine(s) | Services d'incendie | ACA |
|---|--|---|
| <ul style="list-style-type: none"> • Incendie et sécurité des bâtiments | <ul style="list-style-type: none"> • Mise sur pied d'un projet pilote concret avec une zone d'incendie ou un nombre limité de zones d'incendie pour la vérification des alarmes d'incendie et l'échange d'informations | <ul style="list-style-type: none"> • Devenir un partenaire stratégique fiable pour la mise en œuvre de la future politique en matière de sécurité et de prévention • Mettre la centrale d'alarme à disposition en tant qu'environnement de test |

2. Collaboration avec les parties prenantes privées

2.1 Collaboration avec les assureurs

Le secteur veut engager un **dialogue structuré** avec les assureurs et **échanger des informations** à propos de l'impact de la gestion des alarmes sur la prévention et l'intervention et en appui au traitement des sinistres. L'ACA entrevoit également des possibilités de mettre sur pied des **projets pilotes** avec les assureurs en matière de nouvelles technologies.

Concrètement, le secteur entrevoit les actions suivantes.

| Domaine(s) | Assureurs | ACA |
|---|--|--|
| <ul style="list-style-type: none"> • Cambrilage et vol • Incendie et sécurité des bâtiments • Travailleurs isolés | <ul style="list-style-type: none"> • Encourager le raccordement à une centrale d'alarme (conseil, obligation et/ou réduction de prime en fonction de la situation) | <ul style="list-style-type: none"> • Recueillir de meilleures statistiques pouvant permettre aux assureurs de calculer les risques • Être un interlocuteur pour les certifications INCERT et BOSEC et contribuer à l'élaboration d'une approche adéquate pour ce qui concerne la cybersécurité des systèmes anti-effraction basés sur l'IP |

2.2 Collaboration avec les installateurs

La collaboration avec les installateurs peut se faire en majeure partie au travers du modèle de coopération existant avec l'association belge représentant le secteur de la sécurité électronique (ALIA Security), tant en matière d'effraction et de vol que d'incendie et de sécurité des bâtiments. Une meilleure coordination et une **collaboration plus étroite** sont possibles pour ce qui concerne le recours aux **nouvelles technologies et aux nouveaux modèles économiques**.

2.3 Collaboration avec les entreprises

Concernant la problématique des **travailleurs isolés** et de la **protection rapprochée virtuelle** en particulier, le secteur entend consulter les représentants des secteurs à haut risque afin d'assurer une meilleure traduction des besoins en solutions efficaces.

Le secteur identifiera un secteur d'essai afin de lancer un **projet pilote** conjoint. Son souhait est de parvenir à une **réglementation** et à des **garanties** suffisantes en termes de **qualité** pour les travailleurs isolés et la protection rapprochée virtuelle.

Le secteur veut aussi continuer à collaborer étroitement avec les **entreprises de gardiennage** afin de proposer des **solutions globales** sur le marché.

3. Conclusion

Différentes tendances sociales, économiques et technologiques font qu'il est de plus en plus **difficile** de lutter à la fois contre l'insécurité objective et contre le sentiment subjectif d'insécurité. Il est évident qu'il faut une **approche intégrale de la sécurité** et une **collaboration** intégrée et coordonnée entre les différents acteurs de la sécurité. Tant au niveau de la politique qu'au niveau des parties prenantes privées et publiques.

L'Association des centrales d'alarme (ACA), l'organisme professionnel des centrales d'alarme agréées, a la volonté de mobiliser son **savoir-faire unique** et d'exploiter les **avancées technologiques** pour **contribuer activement** à la **sécurité intégrale**.

En effet, la centrale de l'avenir est une « **centrale d'événements** » qui traitera un **large éventail d'alertes** et sera capable de gérer **proactivement des événements et des situations**. La centrale d'alarme est *le* lieu par excellence où peuvent être **concentrées** en un seul endroit toutes les données pertinentes – alarmes, mais aussi images, sons et lieux. Les membres de l'ACA sont donc idéalement placés pour analyser ces données, **mobiliser les intervenants adéquats** et **aider ceux-ci à prendre de meilleures décisions**.

L'ACA veut s'investir en priorité dans des domaines dans lesquels elle peut créer un **win-win** avec d'autres acteurs en matière de sécurité intégrale, à savoir :

- Cambriolage et vol
- Incendie et sécurité des bâtiments
- Criminalité violente, incivilités et dépôts clandestins
- Contrôle d'accès à distance sur le domaine public
- Mobilité

Le secteur veut s'**engager** à être un partenaire à part entière et chercher à se **rapprocher** d'autres intervenants de la sécurité intégrale. L'ACA veut être à la pointe de l'**innovation** à cet égard et contribuer activement à l'**élaboration et à l'évaluation** des **politiques**. Afin de créer une vision reposant suffisamment sur des réalités de terrain, le secteur veut mettre sur pied des **projets pilotes** au niveau des administrations locales, des zones de police et des zones d'incendie. L'ACA invite les parties prenantes à entamer un **dialogue**.

Annexe

Sources

Entretiens

- ALIA Security (Olivier Demoulin)
- Assuralia (Bernard Desmedt)
- Zone d'incendie Centrum (Sam Gydé)
- APEG (Jan Cappelle)
- CoESS (Danny Vandormael)
- Connexcenter (Johan Chenot et Ludovic De Crem)
- Police fédérale (Eddy De Raedt)
- SPF Intérieur (Philip Willekens)
- SPF Intérieur (Bert Hoffer)
- G4S Secure Monitoring (Filip Driesens et Mark Bormans)
- Police locale de Sint-Niklaas (Alain Collier)
- Oktopus (Gaëtan Lejeune et Pieter Debersaques)
- Securitas (Peter Henderickx)
- Seris Monitoring (Didier Herremans et Peter Verpoort)
- SMC (Gino Ghilardi)
- Union des villes et communes flamandes (Tom De Schepper)
- Verisure (Ralph Gijbels)
- Verisure (Steffen Berghman)
- Agence flamande Soins et Santé (Ilse Goossens)

Étude exploratoire de la littérature

- Sites web SPF Intérieur, Vigilis et Belgium.be
- Site web Incert
- Centre fédéral de connaissances pour la sécurité civile (2015) – Statistiques 2014 des services d'incendie belges
- Technavio (2016) – Smart Home M2M Market in Western Europe 2016-2020
- CoESS (2015) – The new security Company : integration of services and technology responding to changes in customer demand, demography and technology
- UGent thèse de master (2016) – Het vertrouwen in ANPR onderzocht: een analyse van de bijdrage van ANPR tot de criminaliteitsbestrijding in het kader van technology-led policing
- De Standaard (09/2017) – De grote levensvragen | Twaalf stellingen waar u het (niet) mee eens bent
- Nieuwsblad (08/2017) – Brandweer kan het niet langer aanzien : in België dubbel zoveel doden in branden als in Nederland
- Beveiliging Nieuws (08/2017) – Belgische staatssecretaris wil verbod onveilige IP-camera's
- Businesswire (05/2017) – Investors Bet That Deep Sentinel's Advanced Artificial Intelligence Can Protect American Homes by Predicting Crime
- Wingmag Pro (05/2017) – Britse politie voorspelt misdaad met Artificial Intelligence
- POM Technologies (04/2017) – A Look at Future Tech : How Artificial Intelligence and System Automation Could Impact Security
- The Verge (06/2017) – Police in Dubai have recruited a self-driving robo-car that can 'scan for undesirables'
- Tech Crunch (01/2017) – Alarm.com is building drones to monitor your home inside and out

- The Verge (09/2017) – The first autonomous drone delivery network will fly above Switzerland starting next month
- HLN (12/2016) – Stad hoest jaarlijks 90.000 euro op door vandalisme en graffiti
- Knack (04/2017) – Zwerfvuil en sluikestorten kost Vlaming jaarlijks 29 euro
- VRT (09/2017) – Eerste flitsmarathon tegen zwerfvuil