L'actualité de la Menace et de la Protection des Entreprises et des Etats

SECURITY DEFENSE
Business review

N° 196 • 26 Juin 2018

L'actu de la Menace

➔ Djihadisme : une menace endogène !

Le nombre d'attaques djihadistes a plus que doublé en Europe en 2017, a déclaré le 20 juin 2018 l'agence de police Europol, mettant en garde contre «l'acuité du danger» d'actes moins sophistiqués revendiqués par le groupe Etat Islamique (EI) : l'année dernière, 33 attaques « terroristes » ont été comptabilisées par Europol. Parmi ces attentats perpétrés, déjoués ou avortés sur le sol européen, 10 ont entraîné la mort de 62 personnes, a indiqué l'agence de police européenne dans son rapport annuel. En comparaison, 13 attaques avaient été signalées en 2016 et dix d'entre elles avaient été meurtrières, tuant un total de 135 personnes. « Le nombre d'attaques terroristes djihadistes a augmenté en 2017, mais, parallèlement, leur niveau de préparation et d'exécution est devenu moins sophistiqué », souligne le rapport intitulé «Situation et tendances du terrorisme». L'agence de police européenne fait référence aux actes « terroristes » perpétrés par des individus fonçant dans la foule à l'aide d'un véhicule ou poignardant des passants, comme notamment à Londres en 2017 où 13 personnes ont été tuées et 98 autres blessées dans deux attaques de cette nature.

Cependant, les agressions au couteau ou à la voiture bélier n'empêchent pas la préparation d'attentats plus sophistiqués : le chef de la police judiciaire allemande, a fait savoir ce même 20 juin qu'un attentat à la «bombe biologique» à base de ricine, un poison très puissant, avait été déjoué en Allemagne, grâce à l'arrestation la semaine précédente d'un Tunisien de 29 ans à Cologne. Le 11 mai à Paris, un même type d'attentat y avait été déjoué : «Deux jeunes gens d'origine égyptienne» souhaitaient passer à l'acte «soit avec de la ricine, soit avec de l'explosif», avait annoncé le 18 mai Gérard Collomb ministre de l'Intérieur.

Les auteurs des attaques djihadistes, dans l'UE l'année dernière, étaient principalement domiciliés sur le continent, « ce qui signifie qu'ils se sont radicalisés dans leur pays de résidence sans avoir voyagé pour rejoindre un groupe terroriste à l'étranger », rappelle le rapport Europol. Depuis que l'Etat Islamique a perdu du terrain en Syrie et en Irak, « il encourage ses partisans à mener des attaques de manière solitaire dans leurs pays d'origine », affirme Europol. « La menace d'attaques jihadistes au sein de l'UE reste aiguë. L'EI, Al Qaeda et d'autres groupes jihadistes restent une menace majeure et ont l'intention et la capacité de mener des attaques terroristes en Occident », prévient l'agence.

Ce qui est intéressant à observer, c'est qu'Europol appelle un chat un chat, décrit explicitement d'où vient la menace, qui est la cible et quelle est la typologie des agresseurs de l'Occident… Encore un ou deux attentats et les populations allemandes, françaises, belges ou espagnoles imposeront à leurs dirigeants de pratiquer la même fermeté que les Hongrois, les Autrichiens, les Tchèques, les Slovaques, les Polonais ou les Italiens… Alors attendons ! *AE avec Ouest France*

SOMMAIRE

AGENDA

➢**25 - 27 Juillet 2018 - Melbourne, Australie**
Security Expo
➢**04 - 07 Septembre 2018 - Kielce, Pologne**
MSPO
➢**02 - 04 Octobre 2018, Singapour**
Safety & Security Asia
➢**08 - 10 Octobre 2018 - Washington, USA**
AUSA
➢**10 - 12 Octobre 2018 - Monaco**
Assises de la sécurité et des SI

Plus d'infos

➔ CYBER

Fortinet a signé un accord avec INTERPOL pour le partage d'informations sur les menaces. Ce partenariat illustre la coopération entre acteurs publics et privés dans la lutte mondiale contre la cybercriminalité et la protection de la vie privée.

Interview de Guy-Philippe Goldstein*

Auteur & Strategic advisor chez ExponCapital (Lux)

♦ **SDBR : En janvier 2012, vous nous expliquiez dans ces colonnes que votre livre, intitulé "Babel Minute Zero" et publié en 2007, annonçait, il y a donc 11 ans, l'émergence d'une nouvelle technologie militaire basée sur le Cyber, avec le risque d'un cyber-chaos international ! Etes-vous devin ?**

Guy-Philippe Goldstein : J'aimerais bien !.... mais je ne suis juste qu'un auteur d'anticipation. Cependant pour parler du futur, il faut souvent utiliser un mot parfois perçu comme grossier dans une certaine culture stratégique: l'imagination. Or, comme le disait Churchill à Harrow en 1941, sans imagination, rien n'est possible. Il ne s'agit pas ici de prédire l'avenir mais de générer des hypothèses en particulier pour identifier des dynamiques individuelles, sociales, politiques… autour des innovations militaires. Cet outil a des précédents étonnants. Les premières guerres aériennes ont été décrites par HG Wells 6 ans avant le premier « bombardement » aérien en 1913. La même année, HG Wells forge le premier l'expression de « bombe atomique » - 32 ans avant Hiroshima. Les descriptions techniques n'étaient pas exactes mais elles mettaient le doigt sur l'importance militaire et diplomatique de ces deux innovations - largement prouvé par la suite. D'ailleurs, c'est à cause d'HG Wells que Churchill ou Szilard se penchent dès les années 20 sur les applications militaires de l'atome. Et sur les questions cyber, Martin Libicki, le grand chercheur de la RAND, écrivait déjà en 1995 que, sur ce qu'il appelait alors le « hacker warfare », les auteurs d'anticipation valaient autant que les analystes « sérieux ».

♦ **Pourquoi ?**

Lorsque l'on parle d'un monde à venir, où il n'y a pas encore de données, on ne pourra jamais que bâtir des conjectures. Autant en générer alors de multiples et des plus diverses possibles dans une première étape, pour ensuite confronter les facteurs sous-jacents. Voilà l'utilité de l'auteur d'anticipation. Quand j'ai commencé à écrire « Babel Minute Zéro », il y a plus de vingt ans, j'avais en tête plusieurs facteurs : 1. Les réseaux Internet allaient dominer notre monde économique ; 2. Par transitivité, les failles informatiques allaient prendre un caractère quasi militaire car c'est l'ensemble de notre univers connecté, de l'industrie à la finance en passant par les transmissions électriques, qui serait relié et donc vulnérable ; 3. Les Etats allaient, bien sûr, se saisir de ces nouvelles armes : leur « métier » étant d'assumer le monopole de la violence légale, ils devaient mettre la main sur ces puissants moyens de coercition. De là pourrait naitre une forme nouvelle de conflit, fondée bien plus fortement sur la dissimulation et la duperie que ce que nous avions connu jusque-là, remettant en cause le principe de désignation de l'adversaire et même de compréhension des lignes rouges réciproques. Ce sont ces deux derniers points qui ont peut-être intéressé mes premiers lecteurs « professionnels », au MIT puis dans l'appareil de sécurité en Israël.

♦ **Quel est votre regard sur l'évolution du risque cyber constatée depuis 2012 ?**

De nombreuses hypothèses formulées en 2012 restent d'actualité et se sont même renforcées. « Babel Minute Zéro» ouvrait sur la possibilité d'escalade dans ce contexte d'introduction de nouvelles armes. La réalité a fini par partiellement donner raison à ces idées. Depuis au moins l'épisode « Stuxnet », et le début des années 2010, il y a à la fois la démonstration des capacités stratégiques de ces armes et une course aux armements, avec des épisodes d'escalades de plus en plus fréquents, en particulier venant de Russie ou d'Iran avec les affaires NotPetya ou Triton. Au niveau de la cybersécurité des entreprises - qui constitue la première ligne de défense, même dans le cadre d'une offensive d'un Etat Nation - on demeure dans le même désarroi qu'en 2012, même si on sent bien que les enjeux ont augmenté de plusieurs crans.

Là-dessus, il y a désormais de nouvelles menaces et peut-être une lueur d'espoir. D'un côté, les Russes ont fait la démonstration d'une approche intelligente en retournant aux concepts de l'infoguerre, qu'ils ont redéveloppé avec cet ADN propre aux services de renseignements des régimes autocratiques – celui de polices politiques au service de l'Etat Central. En manipulant Internet et les réseaux sociaux à l'insu de l'Occident et en attisant les vulnérabilités sociales sur le terreau de pays occidentaux encore marqués par la Grande Récession, ils ont réussi à atteindre leur but politique, en particulier au cœur des Etats-Unis. Cela a un coup bien plus faible que s'ils avaient essayé d'intimider l'Europe en doublant le nombre de divisions blindées ! (...)

** Guy-Philippe Goldstein est aussi Intervenant à l'Ecole de Guerre Economique et Contributeur au journal académique de l'INSS (Tel-Aviv). Il a publié "Babel Minute Zéro" (Denoël, 2007), "Sept jours avant la Nuit" (Gallimard, 2017) et nous annonce "La Cyberpuissance au XXIe siècle" (Ed du Rocher, 2019)*

Suite de l'interview...

(...) Nous avons été peut-être obnubilés par une vision trop matérielle des infrastructures critiques - électricité, transports, eau, télécoms, système financier, etc. - et avons oublié les infrastructures « critiques » propres aux démocraties : le système électoral et les élus, les membres du système judiciaire (y compris avocats, jury, etc..) - et surtout les médias de masse. Bref : nous nous sommes focalisés sur les actifs tangibles mais pas intangibles - qui sont pourtant aujourd'hui une part considérable de la valeur économique (ex : marque, réputation, propriété intellectuelle..). Et plus qu'économique, en vérité. En 2014, Obama a publiquement volé au secours de Sony Picture Entertainment attaqué par la Corée du Nord. Pourquoi ? Parce qu'il symbolisait la liberté de parole, un studio de cinéma étant devenu de facto une infrastructure critique à défendre. Un studio de cinéma ! La lueur d'espoir, ce sont les approches nouvelles qui se développent dans la cybersécurité et qui pourraient rebattre les cartes. Les technologies ou approches avancées de déception** sont en particulier capable de renverser l'avantage perçu jusqu'ici à l'attaque et, cette fois, donner l'avantage à la défense. On l'a vu d'ailleurs en parti dans l'affaire des MacronLeaks, où les fausses informations, mélangées peut-être à des vraies, ont décrédibilisé les attaquants. Des startups se sont montées autour de ces approches. Si elles font la preuve de leur efficacité, elles pourraient très profondément changer la donne - y compris d'ailleurs au niveau diplomatique.

♦ Quels sont les plus grands risques encourus par un pays aujourd'hui ?

Ils sont d'ordre psychologique avant toute chose. C'est d'une part un manque de résilience – l'impossibilité d'agir dans la solidarité et la confiance collective. Peut-être au niveau national et certainement au niveau du tissu industriel des pays. Des exercices d'alerte pourraient être organisés de manière fréquente afin de préparer a minima les populations clés à réagir de manière rapide, efficace et coordonnée. Mais il est clair aussi que des facteurs non cyber, tels que le renforcement des inégalités, la destruction des classes moyennes et le délitement du tissu social, ont potentiellement un effet négatif sur notre capacité de résilience cyber, établie d'abord au niveau humain. Le deuxième risque, c'est celui du manque d'imagination. A nouveau, l'exemple de l'attaque russe contre les systèmes médias et politiques occidentaux est symptomatique. Nous avions là un angle mort intellectuel. Les Russes, eux, ont innové et gagné la première manche. Ils ont d'ailleurs tenté d'autres choses. On a ainsi appris que le « CyberCaliphate », qui s'en était également pris à TV5 Monde, avait lancé en février 2015 une campagne d'intimidation contre les femmes de soldats américains au Moyen-Orient. Il s'agit là de dégrader une force combattante en allant chercher un de ses points faibles sur un champ de bataille non immédiatement apparent : celui du couple. Les dimensions du champ de bataille sont démultipliées avec le cyber entre de multiples fronts, connectés entre eux via l'utilisateur. On sent bien l'explosion d'un champ d'affrontement en vérité bien plus large. Enfin, en termes de menace directe, il est clair que nous sommes désormais engagés dans un conflit entre les démocraties libérales et les régimes autocratiques. Il va y avoir des à-coups. Le premier sera la communication publique (si c'est le cas !) de l'enquête de Robert Mueller et ses conclusions vis-à-vis de l'intrusion de puissances étrangères. Dans ce cas, le monde occidental pourrait se retrouver sur la ligne de « cyber front » très, très rapidement.

♦ Y a-t-il des grands pays cyber-armés et des pays cyber-cibles ?

Tout le monde est une cible et, parfois, c'est en étant une cible que l'on se renforce, au contact de l'adversité. C'est le cas par exemple d'Israël ou de l'Estonie. Donc il y a une certaine « chance » en réalité à être une cible, pour peu que l'on priorise le talent national sur l'atténuation de ce risque. Je proposerais plutôt une catégorisation en termes de capacité défensive, capacité offensive et pas de capacité réelle. Il y a de grands pays au niveau des capacités défensives : si on se focalise sur le tissu social et économique, plusieurs classements vont mettre en avant les pays nordiques (scandinaves et baltes), la Suisse, parfois Israël, ou même la France, en raison de ses efforts règlementaires et institutionnels. L'accent est mis sur la capacité «civile» de réaction à une attaque, qui est aussi un reflet de son investissement dans le capital humain. Mais il ne faudrait pas non plus oublier le marché incomparable que constitue la cybersécurité civile américaine. En regard, il y a des grands pays au niveau des capacités offensives. On pourrait facilement y mettre beaucoup de pays qui ont, ou qui ont eu, des velléités de capacité de forces stratégiques. Les armes cyber y jouent désormais un rôle de premier plan. On y trouve à la fois des puissances occidentales (les Etats-Unis, les grandes puissances européennes, Israël), les grandes puissances dites «révisionnistes» et même des ex-états « voyous » ou proches. Hors de ces deux groupes, des états qui vont être dépendants des grandes puissances, sauf à développer sur place leur propre capacité (et les rattrapages ne sont jamais impossibles dans cet univers du talent nomade). A l'intersection de ces deux groupes : les vraies cyber-puissances d'aujourd'hui.

Interview réalisée par Alain Establier

*** techniques avancées de leurre/tromperie qui font croire a l'assaillant qu' il est parvenu a ses fins*

EUROSATORY 2018

Avec 1802 exposants de 63 pays, 39 pavillons nationaux, 71 conférences et 57 056 visiteurs professionnels, Eurosatory s'affirme incontestablement comme le salon international de référence dans les domaines de la Défense et de la Sécurité Terrestres et Aéroterrestres. Ce n'est donc pas un hasard si 641 journalistes de tous les continents couvraient l'événement. L'édition 2018 a mis en avant une évolution du niveau des visiteurs ainsi qu'une internationalisation et une professionnalisation du salon. Nous avons noté la présence de tous les grands industriels européens, une forte représentation des Américains et des Israéliens. Dommage que les Russes, 2ème exportateur mondial de produits de défense, soient toujours interdits de salons en France, alors qu'on pouvait constater une présence massive des Turcs… Rappelons que le secteur de la Défense représente en France un marché annuel de 18 milliards d'euros (ce qui le place au 3ème rang des secteurs industriels français), qu'il nourrit 165 000 emplois, dont 20 000 emplois hautement qualifiés, 5000 diplômés par an et 4500 en contrat d'apprentissage.

➔ THALES : accélérateur de la transformation digitale de ses marchés

Le groupe Thales couvre quasiment l'ensemble des besoins opérationnels des Armées, de la préparation au combat à la protection du pays et de la force, tant au plan tactique que stratégique. Cette année, la grande nouveauté a été la présentation d'une solution globale d'infrastructure de Cloud privé dédiée aux forces armées, pour une efficacité accrue dans la conduite des opérations : « **Nexium Defence Cloud** ». Les solutions de Cloud déjà utilisées pour des applications civiles ne sont pas adaptées aux besoins des forces armées, car elles exigent une bande passante illimitée dont les forces ne disposent pas sur le terrain. Le Cloud de défense Thales est une solution souveraine qui peut fonctionner dans un contexte contraint leur offrant une totale autonomie sur les théâtres d'opérations : c'est une solution globale et résiliente pour permettre aux forces de rester connectées en permanence, depuis n'importe quel terminal ; elle offre un accès privatif aux données, adapté aux contraintes spécifiques des infrastructures militaires, du centre de commandement au théâtre d'opérations et elle bénéficie de l'expertise de Thales en matière de cybersécurité.
Autre nouveauté présentée, la jumelle « **Sophie Ultima** », équipement léger, ultraperformant et «quatre-en-un», prêt pour le combat collaboratif et la réalité augmentée afin de garantir la supériorité tactique des forces armées de jour comme de nuit. Elle apporte au fantassin un avantage tactique de nuit, en permettant l'identification de la cible à une distance à laquelle les jumelles concurrentes ne pourront que la reconnaître, et de jour, grâce à la combinaison des performances inégalées d'une jumelle de jour avec la capacité de détection de l'imagerie thermique pouvant détecter la chaleur corporelle à des distances supérieures à 1 km. Thales a vendu 15 000 jumelles de la gamme Sophie dans 55 pays. www.thalesgroup.com

➔ NEXTER : systémier intégrateur français de la défense terrestre

Nexter était présent sous la bannière du Groupe KNDS (KMW + NEXTER Defense Systems). Fournisseur de référence de l'armée de Terre française, Nexter est très engagé dans le programme Scorpion. On pouvait voir le « Jaguar », exposé pour la première fois, aux côtés de son binôme dans le programme EBMR « Griffon » et du « Leclerc » rénové. Le dernier né de la gamme Scorpion, le VBMR Léger baptisé « **SERVAL** » lors de ce salon, faisait l'objet d'une animation holographique en taille réelle. Les autres systèmes et produits du groupe étaient également présentés : le VBCI APC [Transport de troupe], la famille CAESAR, avec les versions 6x6 et 8x8, le système d'artillerie 105LG1, les robots Nerva et Optio.
OPTIO est une nouvelle gamme de robots tactiques polyvalents destinés à mener différentes missions sans exposer de personnels débarqués : ouverture d'itinéraires, reconnaissance et observation, logistique ou appui feu. Les travaux de Nexter visent à accroître la pertinence opérationnelle de ces systèmes robotisés, en poursuivant 3 axes de développement complémentaires : polyvalence et modularité, afin de doter ces systèmes robotisés de la capacité d'adaptation qui rendra les Forces plus réactives à l'évolution des menaces ; intégration de robots et de drones dans les véhicules de combat, vers la constitution de systèmes composites (Habités - Non Habités) ; développement d'une autonomie supervisée pour permettre à l'opérateur de se concentrer sur le cœur de la mission tactique. Sur Eurosatory, Nexter exposait une variante armée de la gamme OPTIO combinant la plateforme téléguidée «THeMIS» de Milrem et un tourelleau 20 mm téléopéré de Nexter.
Pilier important de Nexter, troisième acteur européen dans son domaine, **le pôle munitionnaire** composé des sociétés Mecar, Simmel Difesa et Nexter Munitions, exposait sa gamme complète de munitions, du 20 mm au 155 mm, répondant aux besoins des trois milieux : naval, terrestre et aérien.
La tourelle de 40mm téléopérée équipée du canon de CTA International (société commune entre Nexter et BAE), l'ARX25 et le P20 illustraient l'offre du groupe en matière d'armes et tourelles.
www.nexter-group.fr

EUROSATORY 2018, suite

➔ Safran Electronics & Defense : leader de la navigation inertielle

L'utilisation croissante de technologies numériques sur le champ de bataille nécessite d'améliorer constamment les capacités d'orientation, de positionnement et de pointage de précision des véhicules et des plateformes. Safran Electronics & Defense actualise son offre de centrales de navigation inertielle pour les applications terrestres avec la **nouvelle gamme «Geonyx»**, désormais la centrale de navigation la plus compacte, la plus robuste et la plus fiable sur le marché. La navigation inertielle permet de déterminer le mouvement grâce à des capteurs d'accélération (accéléromètres) et de rotation (gyroscopes). Elle fournit une estimation de la position, de la vitesse et de l'attitude tout au long du parcours d'un véhicule (avions, missiles, navires, sous-marins, véhicules terrestres). Elle fonctionne sans point de repère extérieur, hormis le point de départ. Il n'y a donc pas de dépendance à un système de navigation par satellites comme le GPS, par exemple. Pour les véhicules terrestres et plateformes d'artillerie, Safran dispose d'une gamme complète de systèmes de navigation inertielle qui équipent plus de 50 véhicules et plateformes dans le monde: les centrales de haute précision Sigma 30, les unités tactiques Epsilon. La dernière-née, « Geonyx », est une centrale de navigation et de pointage inertiel de haute précision, avec une tenue aux chocs extrêmes, qui recèle un concentré de toutes les avancées technologiques de Safran dans les centrales inertielles : elle met à profit les meilleures caractéristiques de Sigma 30 en termes de performance, de robustesse dans des conditions difficiles (Sigma 30 est sur le canon Caesar de Nexter), de polyvalence, de simplicité d'utilisation et d'extrême précision. Grâce à son gyroscope à résonateur hémisphérique, le HRG Crystal, innovant et déjà éprouvé, la gamme «Geonyx» constitue une avancée majeure en termes d'efficacité opérationnelle, d'intégration du produit et de coûts de possession.
www.safran-group.com

➔ CNIM, Bertin et Exensor

Eurosatory a été l'occasion pour le groupe CNIM et ses filiales, Bertin Technologies, Bertin IT et Exensor, de présenter l'ensemble de leurs systèmes et équipements pour la Projection et la Protection des Forces Armées sur terre, et de cybersécurité (www.cnim.com):

- Une version modernisée des **Ponts Flottants Motorisés (PFM)** pour l'Armée française, solution de franchissement adaptée aux nouveaux besoins de projection des Forces en territoire extérieur.
- SaphyRAD MS : un radiamètre militaire multisondes innovant pour les environnements difficiles et les situations d'urgence, conçu pour être utilisé par les forces armées ou des équipes HAZMAT.
- L'élargissement de la **gamme optronique de Bertin** : CamSight, une famille de modules caméras compacts et légers pour une vision améliorée de jour comme de nuit, et PeriSight Zoom, un nouveau système optronique de caméra dédié aux véhicules militaires, pour une vision fiable jour et nuit de longue portée.
- Les solutions éprouvées de réseaux de capteurs déposés au sol de la société Exensor, leader mondial dans le domaine de la surveillance, société suédoise acquise par Bertin Technologies en juillet 2017. La plateforme **Flexnet Sensor** est un outil polyvalent qui peut être utilisé dans une grande variété d'applications grâce à une gamme variée de capteurs au sol sans surveillance - UGS (Unattended Ground Sensors). Bertin et Exensor sont fiers d'annoncer le succès de leur première collaboration, permettant l'intégration de la technologie optronique de Bertin au sein d'un capteur Exensor : CamSight, caméra OEM (Original Equipment Manufacturer) développée à partir de la technologie optronique commune de FusionSight, monoculaire de vision diurne et nocturne, et de PeriSight, système de vision périmétrique. CamSight inclut une technologie d'imagerie thermique non refroidie et sans obturateur, offrant un étalonnage en usine unique sans besoin de contrôle d'étalonnage périodique. CamSight a été intégrée à la caméra Scout d'Exensor, caméra sans fil intelligente avec détection de mouvement intégrée, faisant partie de la plateforme Flexnet UGS développée par Exensor et fournie à des clients militaires et civils dans le monde entier.
- **Crypto Crossing** : une solution de passerelle email hautement sécurisée conçue par Bertin IT.

AE

Les marchés financiers

Au risque d'être contredit lorsque les entreprises annonceront cet été leurs résultats semestriels (qui devraient rester globalement bons sur la lancée de l'accélération de la croissance fin 2017), les facteurs politiques et géopolitiques pourraient être à l'origine de la plupart des mouvements de marché dans les prochains mois. Après l'alerte italienne (apaisée pour l'instant, mais les questions économiques resurgiront au plus tard lors des discussions budgétaires), l'Europe est confrontée à d'autres dossiers délicats : gouvernement minoritaire en Espagne, fortes tensions entre la chancelière allemande et le CSU. Sauf surprise, le sommet européen de fin de semaine ne devrait pas déboucher sur des annonces propres à « réenchanter » l'Europe ou la Zone Euro et devrait constater que les avancées sur le Brexit restent largement insuffisantes ! L'escalade dans les mesures, ou les menaces de mesures protectionnistes, entre les USA et la Chine va aussi être suivie de près par les marchés, qui s'accommodent facilement des mesures fiscales de l'administration Trump mais moins des foucades présidentielles. Sans oublier le fil rouge habituel des tensions au Proche-Orient ! De quoi passer l'été, l'œil braqué sur les fils info !

Les Leaders du secteur Security & Defense

Nom	Pays	Cours au 31/12/17	Cours au 31/05/18	Cours au 20/06/18	▲/▼	Depuis le 01/01/18
Rheinmetall	*DE*	*108,1*	*109,1*	*104,35*	▼	*-3%*
Siemens	*DE*	*116,15*	*111,50*	*116,50*	▲	*0%*
ThyssenKrupp	*DE*	*24,02*	*22,57*	*22,27*	▼	*-7%*
Nokia Corp,	*FIN*	*3,89*	*4,95*	*5,11*	▲	**31%**
Airbus Group	*FR*	*83,81*	*97,31*	*100,52*	▲	*20%*
Atos	*FR*	*121,25*	*116,2*	*121,45*	▲	*0%*
Dassault Aviation	*FR*	*1292*	*1661*	*1661*	▲	*29%*
Safran	*FR*	*86,36*	*102,15*	*100,15*	▼	*16%*
Thales	*FR*	*89,84*	*108,9*	*108,75*	▼	*21%*
CNHI / ex Fiat Industrial	*IT*	*11,2*	*10,02*	*9,31*	▼	*-17%*
Finmeccanica Leonardo	*IT*	*9,9*	*8,72*	*8,88*	▲	*-10%*
Hitachi Ltd	*JP*	*877,9*	*796,6*	*786,1*	▼	*-10%*
Mitsubishi Electric	*JP*	*1871*	*1545*	*1459*	▼	**-22%**
Panasonic	*JP*	*1649*	*1489*	*1526*	▲	*-7%*
Sony	*JP*	*5083*	*5160*	*5404*	▲	*6%*
Assa Abloy	*SW*	*171*	*189,6*	*189,9*	▲	*11%*
Axis AB	*SW*	*339,9*	*330*	*331*	▲	*-3%*
Saab Group	*SW*	*398,5*	*364,2*	*369,7*	▲	*-7%*

Nom	Pays	Cours au 31/12/17	Cours au 31/05/18	Cours au 20/06/18	▲/▼	Depuis le 01/01/18
Volvo Corp.	*SW*	*153,6*	*151,75*	*144,9*	▼	*-6%*
Babcock Int Group	*UK*	*704,5*	*833*	*832*	▼	*18%*
Bae Systems	*UK*	*571,5*	*639,4*	*635*	▼	*11%*
Qinetiq Group	*UK*	*231,5*	*264,3*	*268,4*	▲	*16%*
Ultra Electronics	*UK*	*1346*	*1613*	*1649*	▲	*23%*
Boeing	*US*	*294,91*	*354,6*	*344,06*	▼	*17%*
Cisco Systems	*US*	*38,3*	*43,09*	*43,88*	▲	*15%*
Elbit Systems	*US*	*133,29*	*119,37*	*120,19*	▲	*-10%*
General Dynamics	*US*	*203,45*	*203,72*	*191,25*	▼	*-6%*
Honeywell International	*US*	*153,36*	*149,15*	*146,27*	▼	*-5%*
Johnson Controls (Tyco)	*US*	*38,11*	*33,91*	*34,66*	▲	*-9%*
Kratos	*US*	*10,59*	*11,37*	*11,42*	▲	*8%*
L3 Communications	*US*	*197,85*	*199,04*	*194,6*	▼	*-2%*
LEIDOS / ex SAIC	*US*	*64,57*	*60,58*	*59,59*	▼	*-8%*
Lockheed Martin	*US*	*321,05*	*317,74*	*303,53*	▼	*-5%*
Northrop Grumman	*US*	*306,91*	*329,99*	*313,51*	▼	*2%*
Raytheon	*US*	*187,85*	*211,43*	*197,18*	▼	*5%*
United Technologies	*US*	*127,57*	*125,05*	*125,49*	▲	*-2%*

DE: Frankfurt, FR: Paris, IT: Milano, UK: London, SW: Stockholm, US: NYSE, JP: Tokyo

QinetiQ Group
Flottant : 563 600 000 actions soit 99.36 %du total des actions
Cours au 31/12/2017 : 231.50 GBP
Cours au 31/05/2018 : 264.30 GBP
Cours au 20/06/2018 : 268.40 GBP
Variation par rapport au 01/01/2018 : + 16 %
Dividende 2017 : 4 GBP soit un rendement de 1.73 %
Actualités : La police de la Vallée de la Tamise a utilisé la technologie X-Net de QinetiQ, pour pouvoir stopper les véhicules, dans le cadre du plan de sécurité plus large visant à protéger le mariage royal du prince Harry et de Meghan Markle à la chapelle St George de Windsor. X-Net est une solution portable et non létale, capable d'arrêter des véhicules utilisés pour des attaques terroristes allant des petites voitures à des camions de 10 tonnes, en s'enroulant autour des roues et de l'axe du véhicule tout en perforant les pneus, empêchant ainsi toute manœuvre supplémentaire.

Infos utiles

➔Une publication bimensuelle
➔Rédacteur en chef : Alain Establier
➔Société Editrice : SDBR Conseil, SAS domiciliée
4 Rue du Calvaire, 92210 Saint-Cloud, France
520 236 662 RCS Nanterre
E-mail : admin@securitydefensebusinessreview.com
Web: **www.securitydefensebusinessreview.com**

➔Abonnements: +33 (0) 9 77 19 76 40
Abonnement annuel : 980 € HT (TVA 20%: 1176 € TTC)
Abonnement semestriel : 600 € HT (TVA 20% 720 € TTC)
ISSN 2107-7312

Prochain Numéro: Mardi 10 Juillet 2018