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

SECURITY DEFENSE
Business review

N° 186 • 23 Janvier 2018

L'actu de la Menace

➔ Asie du Sud-Est : attention danger !

Alors que l'attention des médias internationaux se concentre en priorité sur les États défaillants du monde musulman (Afghanistan, Irak, Libye, Syrie, Yémen), la situation du golfe de Thaïlande échappe souvent à toute analyse. Le site d'informations « Thaïlande-fr » (groupe Siam News Network basé à Hong Kong), a publié une suite d'articles intéressants sur la situation dans le sud du pays. Bien qu'étant un pays à majorité bouddhiste, la Thaïlande souffre de l'une des insurrections musulmanes les plus anciennes et les plus meurtrières d'Asie. A la frontière malaise, trois provinces, Pattani, Yala et Narathiwat, regroupent la majorité des 5% de musulmans de Thaïlande et 4/5 d'entre eux parlent malais. Elles appartenaient anciennement au sultanat de Patani, haut lieu de l'islam en Asie du Sud-Est au XVIIe et XVIIIe siècles.

Les rebelles sécessionnistes, se décrivant comme des islamistes, ont frappé le sud de la Thaïlande depuis plusieurs décennies avec des décapitations, des voitures piégées et des attentats, en une régularité rarement vue à l'extérieur du Moyen-Orient. Depuis 2004, ces attaques répétées ont déjà fait 6800 victimes ! Devant ces faits on peut difficilement, comme le font certains think thank et autres medias, considérer ce foyer de violence comme purement anecdotique, ou justifié par la répression des autorités thaïes. A de très rares exceptions, pour l'instant, le conflit est resté localisé dans le sud et sans grandes conséquences pour le reste de la Thaïlande. La vision manichéenne de soi-disant chercheurs sur la situation en Thaïlande, comme aux Philippines d'ailleurs, n'a pas d'argument sérieux devant les faits : les islamo-malais ont tué au moins 171 enseignants et ont incendié ou fait exploser plus de 300 écoles publiques en 10 ans dans les provinces frontalières du sud… Les écoles étant un fort symbole de l'Etat, les populations musulmanes s'y attaquent « dans le but de faire fuir les populations bouddhistes thaïlandaises de ce qu'ils appellent la terre des musulmans malais »: vous avez dit nettoyage ethnique…? S'attaquer à l'école et aux enseignants est toujours le signe de l'avancée d'un totalitarisme !

En considérant la globalité de la région, qui part de la Thaïlande, descend sur la Malaisie et Singapour, puis remonte sur l'Indonésie jusqu'aux Philippines, on observe un arc qui pourrait bien devenir le prochain terrain de jeu du totalitarisme islamique : Tanzim Qaedat al-Jihad (aussi connu sous le nom d'Al-Qaïda dans l'archipel malais), en Malaisie, est considéré comme un groupe dissident du groupe islamiste sud-asiatique Jemaah Islamiya présent en Indonésie ; le Kumpulan Mujahidin Malaysia (KMM), qui semble en sommeil depuis 2014 mais peut se réveiller à tout moment, est pour la création d'un état islamique pan-régional comprenant le sud de la Thaïlande, l'Indonésie entière et le sud des Philippines ; Darul Islam Sabah en Indonésie semble être devenu la branche locale de l'EI (ISIS - Islamic State of Iraq and Syria) ; Abu Sayyaf, autre branche d'EI, est basée à Jolo (Philippines) au centre de cet arc, comme pour mieux en devenir le coordonnateur… A suivre donc ! AE

SOMMAIRE

> Interview de Charlotte Touzot, Doctorante p.2

> Baromètre Cybersécurité du CESIN p.4

> Les marchés financiers p.5

> Ruptures technologiques & ruptures stratégiques p.6

AGENDA

➢**06 - 11 Février 2018 – Singapour**
Singapore Airshow 2018
➢**06 – 07 Mars 2018 - London, UK**
Counter Terror Expo
➢**06 - 08 Mars 2018 - Abu Dhabi, EAU**
ISNR
➢**06 - 08 Mars 2018 – Monaco**
ROOMn 2018
➢**12 - 14 Mars 2018 - Doha, Qatar**
DIMDEX

Plus d'infos

➔ Cyber risques

Une étude Pradeo montre que 60% des applications mobiles (provenant de Google Play par exemple) divulguent les données de leurs utilisateurs. Les flottes mobiles des entreprises, uniquement protégées contre les malwares, ne sont plus à l'abri et vont devenir une cible privilégiée en 2018…

Interview de Charlotte Touzot*

Doctorante (OMIJ-CRIDEAU**) et ATER*** en Droit public, Université de Limoges

♦ **SDBR : Vos travaux de recherche touchent aux « activités militaires et à l'environnement » : quel est le champ couvert par ce titre ?**

Charlotte Touzot : Il s'agit de l'ensemble des activités militaires qui s'exercent en temps de guerre comme en temps de paix, tels que les entraînements, les manœuvres, les activités de maintien de la paix, ou encore toutes les activités qui entrent dans le champ de la Défense nationale. J'ai effectué au cours de mon Doctorat plusieurs séjours de recherches, en Suisse, en Turquie et au Liban, où j'ai passé 7 mois et où je continue à me rendre régulièrement. À cette occasion, j'ai travaillé sur l'intégration de l'environnement au sein des Forces armées libanaises (LAF), notamment au sein de la Marine nationale libanaise, ainsi que sur les missions de dépollution et de déminage effectuées au Sud Liban par les Forces intermédiaires des Nations Unies pour le Liban (FINUL). Mes recherches portent principalement sur la manière dont les activités militaires peuvent et/ou doivent intégrer les enjeux environnementaux au sein de leur fonctionnement. On note à ce titre une environnementalisation progressive de ces activités, notamment due à la mise en œuvre du concept de développement durable au sein des différentes institutions publiques. C'est, par exemple, le cas de la gestion du patrimoine militaire, tant au niveau des infrastructures que de la domanialité militaire, mais aussi des opérations de dépollution et de démantèlement des sites et matériels militaires. On peut également constater que les Armées ne se sont pas contentées d'adapter leurs activités aux enjeux environnementaux, elles en ont fait une nouvelle activité dont le champ s'étend de plus en plus. Une première illustration de ce recyclage de l'Armée est l'assistance militaire en cas de catastrophes (naturelles, industrielles et technologiques), qui est quasi-systématique. La seconde illustration réside dans l'existence d'activités militaires de protection de l'environnement, reliées à la mission de surveillance du territoire (lutte contre les pollutions, lutte contre les trafics, etc.). En d'autres termes, les militaires peuvent potentiellement protéger l'environnement à travers leurs activités et leurs missions, soit directement, soit indirectement. Ceci n'a par ailleurs pas vocation à dénaturer le cœur de métier, mais a vocation au contraire à l'adapter aux nouveaux enjeux et aux nouvelles menaces, comme le changement climatique.

♦ **Comment protéger l'environnement quand des milliers de mines anti-personnel sont utilisés dans les conflits asymétriques récents ?**

La protection de l'environnement en temps de conflits armés est délicate. L'environnement constitue à la fois le théâtre des conflits, souvent un objectif militaire (en permettant aux belligérants de se mettre à couvert), une ressource pour la conduite des hostilités, et parfois la cause du conflit (ressources naturelles). Malgré l'existence d'un encadrement juridique et d'une reconnaissance de plus en plus générale et profonde de la nécessité de protéger l'environnement, la protection de l'environnement reste secondaire en cas de guerre. Les mines anti-personnel sont un fléau non seulement pour la sécurité humaine, mais aussi pour la sécurité environnementale et sanitaire. Le recours à de telles armes est d'autant plus regrettable que les dommages s'étendent dans le temps et ne permettent pas une réhabilitation post-conflit du territoire adéquate. Prenons l'exemple du conflit qui a opposé Israël au Hezbollah en 2006, dans lequel pas moins de 7 millions de bombes, roquettes, mines antipersonnel et obus ont été lancés par Israël sur le sol libanais en seulement 34 jours de durée du conflit. L'armée israélienne a utilisé des conteneurs à sous-munitions envoyés par bombardier ou lance-roquettes, le but étant de balayer la zone. Il s'agit là de moyens de saturation du champ de bataille, utilisés lors du retrait des troupes israéliennes. C'est dans ce contexte que se pose la question de la sécurisation du territoire qui a été le théâtre des opérations, et qui passe alors par une longue phase de déminage et de désarmement. Mais les dommages environnementaux ne sont pas uniquement causés par l'utilisation de mines anti-personnel mais également par les autres types d'armes et de munitions (notamment chimiques), par l'abandon de matériels militaires (déchets militaires) et par l'utilisation des ressources naturelles au cours des hostilités mais aussi en préparation de celles-ci. La meilleure protection de l'environnement dans de telles circonstances est offerte par le droit des conflits armés et par le droit international de l'environnement, lorsque les conventions de protection de l'environnement prévoient la circonstance de conflits. Encore faut-il que le droit soit respecté par les belligérants… En définitive, la protection de l'environnement ne peut véritablement être effective qu'en temps de paix, en raison de son caractère à la fois universel et intrinsèquement pacifique.

** Thèse : « Activités militaires et Environnement », sous la direction de Jessica Makowiak. (Soutenance prévue au Printemps 2018)*

*** Observatoire des mutations institutionnelles et juridiques-Centre de recherches interdisciplinaires en droit de l'environnement, de l'aménagement et de l'urbanisme.*

**** ATER : attachée temporaire d'enseignement et de recherches.*

Suite de l'interview...

♦ **Que fait la FINUL au sud Liban ? Est-ce que son action pour l'environnement est transposable ailleurs ?**

La FINUL* est basée au Sud du Liban depuis 1978. Sa mission principale est de s'assurer qu'il n'y ait pas de reprise des hostilités. À ce titre, la force intérimaire apporte son soutien aux forces libanaises (lors d'opérations militaires conjointes et coordonnées, mais également en organisant des entraînements et des formations), ainsi qu'auprès de la population. La FINUL veille à ce que la zone ne soit pas utilisée à des fins militaires autres que celles poursuivies par les Nations Unies. La zone de la FINUL couvre 1000 km^2. La « Blue Line » quant à elle s'étend sur 120 km de long. C'est une ligne qui a été matérialisée par les Nations Unies et qui est considérée comme une ligne de retrait, et non comme une frontière à proprement parler entre le Liban et Israël. Le marquage de cette ligne est toutefois réalisé aussi dans la perspective éventuelle d'établir à terme une frontière entre les deux territoires. La « Blue Line » est matérialisée par 268 bidons bleus. Les Forces intérimaires ont donc pour mission de dépolluer et déminer la zone. Actuellement, la FINUL n'opère que du déminage opérationnel, autrement dit au profit des troupes. C'est la différence avec le déminage humanitaire qui lui vise à libérer une zone pour une activité autre que militaire. À l'heure actuelle, 326 points ont été déminés sur la ligne. Cependant, en l'absence d'accord entre les autorités libanaises et les autorités israéliennes, la Blue Line est discontinue sur 40 km. Il s'agit de zones dites réservées (où on ne trouve donc pas de bidons bleus). La zone Sud-Liban est extrêmement polluée. Elle compte quelques 380 000 mines ainsi que de nombreux déchets de guerre. Israël a donné les plans de situation des champs de mines (IDF minefield reports), qui demeurent cependant difficiles à lire : les plans sont anciens et les mines bougent… Le déminage effectué par la FINUL ne s'opère uniquement que sur la Blue Line à l'heure actuelle. Il n'y a pas de déminage humanitaire du fait de la souveraineté des États et il n'y a plus aujourd'hui d'accord entre les Nations Unies et le gouvernement libanais pour faire du déminage en dehors de la Ligne bleue, et ce depuis 2011. Le déminage et la dépollution de la région Sud-Liban ont donc pour finalité première de permettre le marquage d'une ligne de démarcation et de remettre en état la zone à la suite du conflit intervenu en juillet 2006. Pour le dire autrement, il s'agit de la réhabilitation post-conflit du territoire, dont la première étape est précisément le déminage. Les missions de maintien de la paix exercées par les Casques bleus ne revêtent pas un caractère général et ne peuvent de ce fait pas être transposées à l'identique d'un terrain à un autre. Néanmoins, l'intégration des préoccupations environnementales au sein des Nations Unies et plus particulièrement au sein du Conseil de sécurité laisse penser que l'ensemble des missions doivent à la fois limiter leurs impacts sur l'environnement et répondre à une démarche de préservation de l'environnement. C'est d'ailleurs en ce sens que chaque base militaire compte une «cellule environnement», qui a pour mission de veiller à la rationalisation des ressources (eau, énergie, carburants, déchets).

♦ **Finalement, quelles voies de progrès proposer dans la gestion de l'environnement post-conflit ?**

La gestion de l'environnement post-conflit s'accompagne de bon nombre de mesures, qui varient selon l'intensité du conflit. Il faut tout d'abord évaluer les dommages environnementaux avant de chercher à les réparer. Il existe pour ce faire différents outils, comme les études d'impacts ou encore les interventions d'urgence. Il faut également rechercher à restaurer les services environnementaux, ce qui nécessite au préalable un minimum d'organisation administrative et politique. Le volet environnemental de la réhabilitation post-conflit est intimement lié aux volets humanitaire et sanitaire, et ne peut être ni pensé ni mis en œuvre en dehors de ces derniers. La gestion de l'environnement post-conflit répond parfaitement à la logique humanitaire de la responsabilité de protéger et de son triptyque « prévention-réaction-reconstruction ». C'est en ce sens que la remise en état de l'environnement à la suite d'un conflit doit s'orienter : en prévention, afin d'empêcher la survenance d'un nouveau conflit lié aux déséquilibres environnementaux ; en réaction, afin de limiter l'étendue des dommages écologiques et sanitaires (par exemple la contamination des cours d'eau) ; en reconstruction, afin d'assurer une stabilité écologique et une sécurité environnementale sur le long terme. On pourrait alors proposer le développement d'une véritable mission « environnement » dans le cadre des missions de maintien de la paix, à l'instar de ce qu'avait proposé Irina Bokova, ancienne directrice de l'UNESCO, concernant la protection du patrimoine (qui comprend également le patrimoine naturel). Cela ferait également écho à l'assistance militaire en cas de catastrophes naturelles et répondrait aux mêmes logiques et exigences. Une telle mission devrait s'opérer de manière intégrée entre les enjeux environnementaux, sanitaires, sociaux, économiques et sécuritaires, mais aussi de manière mutualisée entre les humanitaires et les militaires, et ce malgré les nombreuses limites institutionnelles et politiques (liées aux motifs de l'intervention). La complémentarité des acteurs humanitaires et militaires, en matière de réhabilitation post-conflit, serait indéniablement une chance pour la préservation de l'environnement qu'il faudrait exploiter.

Propos recueillis par Alain Establier

** FINUL : http://www.un.org/fr/peacekeeping/missions/unifil*

3ème Baromètre annuel de la Cybersécurité du CESIN

Pour la 3ème année consécutive, le CESIN* (Club « très fermé » des Experts de la Sécurité de l'Information et du Numérique) vient de publier son baromètre annuel avec OpinionWay, enquête menée exclusivement auprès de ses membres, dont 41% ont accepté de répondre aux questions posées. Moins de la moitié, parmi les RSSI des plus grandes entreprises et organisations françaises membres du CESIN, à se sentir concernés par l'état de l'art et la perception de la cybersécurité et de ses enjeux, voila qui est curieux… Les 142 répondants ont néanmoins souligné l'impact de la transformation numérique des entreprises et la réalité de la cybermenace.

➔ L'évolution des cyber-attaques

Pratiquement toutes les entreprises ayant répondu au sondage affirment avoir été attaquées une ou plusieurs fois depuis un an (92 %) : une sur deux constate une augmentation de 48 % du nombre d'attaques et, pour le quart d'entre elles, des impacts sur le business ont été ressentis : arrêt de la production, indisponibilité significative du site internet, perte de chiffre d'affaire... Le ransomware demeure l'attaque cyber la plus fréquente (73 % des entreprises ont fait face à une ou plusieurs demandes de rançons), 38 % ont subi une fraude externe, 30 % un vol d'information, 25% ont été touchées par des attaques en déni de service et 16 % par une défiguration de site web. A noter que les attaques WannaCry et NotPetya ne sont pas citées dans l'étude car, si ces attaques ont en effet généré énormément d'activités de prévention pour l'ensemble des RSSI, très peu d'entreprises membres du CESIN auraient été effectivement touchées (ou alors ce sont celles qui ont refusé de répondre au sondage ?). Un point à souligner, plus d'un sondé sur deux a été touché par le social engineering et les vulnérabilités résiduelles permanentes.

➔ L'efficacité des solutions techniques

Les entreprises implantent en moyenne une douzaine de solutions techniques. Globalement, les solutions de protection disponibles sur le marché sont jugées de plus en plus efficaces (cela tend à augmenter), mais elles resteraient perfectibles et ne seraient pas totalement adaptées, dans 22 % des cas, aux besoins de l'entreprise et, dans 34 % des cas, à la fréquence actuelle des attaques. Au-delà de l'antivirus, des tunnels VPN, mécanismes de filtrage web et solutions antiSPAM, on note une forte montée des souscriptions aux cyber-assurances : 55 % des sondés y ont déjà souscrit ou sont en train de le faire (les conséquences de potentielles non-conformités au RGPD** n'y sont sans doute pas étrangères).

➔ La transformation numérique influence le niveau d'exposition au risque

Pour le Cloud, déjà très répandu dans les entreprises puisque 87 % des sondées y stockent des données notamment sous la forme hybride public/privé, la problématique de la confidentialité des données représente l'enjeu principal en matière de cybersécurité et 94 % estiment que la sécurisation des données hébergées dans le Cloud nécessite des outils spécifiques. Les pratiques des salariés mettent aussi à mal la cybersécurité, notamment le Shadow IT, mais aussi l'utilisation de terminaux multiples et l'usage personnel de ces derniers fournis par l'entreprise. Concernant l'internet des objets, les failles de sécurité de l'IoT semblent le premier défi à relever en entreprise : 73 % des RSSI sondés pensent que les salariés sont plutôt bien sensibilisés aux risques mais peu proactifs, donc 62 % des entreprises auraient mis en place des procédures de vérification du respect des recommandations par les salariés.
Concernant le RGPD, 89% des RSSI sondés considèrent qu'il grève les budgets et ajoute une charge de travail, et la majorité déclare ne pas avoir achevé leur chantier de mise en conformité avec le RGPD et ne pas être sûre de pouvoir le finaliser pour la date butoir du 25 mai 2018. Le RGPD est cependant bien perçu par les entreprises, 83 % d'entre elles le considérant comme un réel moyen de renforcer la protection des données, la mise en conformité ayant déjà permis de refonder la gouvernance de la cybersécurité dans une entreprise sur deux. AE

** CESIN : www.cesin.fr*
*** RGPD : Règlement Général (européen) sur la Protection des Données*

Les marchés financiers

Les taux longs se sont légèrement tendus depuis le début d'année, mais les opérateurs manquent de conviction pour amplifier le mouvement, face à des banques centrales toujours acheteuses d'obligations (y compris aux Etats-Unis où les titres échus sont réinvestis à hauteur du montant mensuel des échéances diminué de 20 milliards de dollars) et à des taux d'inflation encore faibles (surtout dans la Zone Euro et au Japon), même si les risques de déflation sont maintenant écartés. Le statu quo sur la politique monétaire devrait prévaloir à l'issue du premier Conseil de Politique Monétaire 2018 de la BCE (25 janvier) puis du premier Federal Open Market Committee (31 janvier). C'est dans la communication que les opérateurs chercheront des raisons d'amplifier la hausse des taux, mais ils risquent de rester sur leur faim : la BCE a besoin de chiffres d'inflation plus élevés, qu'elle n'aura vraisemblablement pas avant mars, et il est probable que le dernier FOMC présidé par Janet Yellen restera aussi prudent que les précédents. Les réunions monétaires de mars devraient être plus décisives pour les marchés obligataires !

Les Leaders du secteur Security & Defense

Nom	Pays	Cours au 31/12/17	Cours au 04/01/18	Cours au 18/01/18	▲/▼	Depuis le 01/01/18
Rheinmetall	*DE*	*108,1*	*109,65*	*111,25*	▲	*3%*
Siemens	*DE*	*116,15*	*119,54*	*123,06*	▲	*6%*
ThyssenKrupp	*DE*	*24,02*	*25,26*	*25,06*	▼	*4%*
Nokia Corp,	*FIN*	*3,89*	*4,01*	*3,97*	▲	*2%*
Airbus Group	*FR*	*83,81*	*84,44*	*91,38*	▲	*9%*
Atos	*FR*	*121,25*	*124,25*	*126,95*	▲	*5%*
Dassault Aviation	*FR*	*1292*	*1310*	*1362*	▲	*5%*
Safran	*FR*	*86,36*	*87,74*	*90,92*	▲	*5%*
Thales	*FR*	*89,84*	*91,02*	*91,1*	▲	*1%*
CNHI / ex Fiat Industrial	*IT*	*11,2*	*13,58*	*12,18*	▼	*9%*
Finmeccanica Leonardo	*IT*	*9,9*	*10,16*	*11,23*	▲	*13%*
Hitachi Ltd	*JP*	*877,9*	*890,5*	*917,8*	▲	*5%*
Mitsubishi Electric	*JP*	*1871*	*1945*	*2126*	▲	*14%*
Panasonic	*JP*	*1649*	*1691*	*1678*	▼	*2%*
Sony	*JP*	*5083*	*5279*	*5449*	▲	*7%*
Assa Abloy	*SW*	*171*	*171,85*	*177,9*	▲	*4%*
Axis AB	*SW*	*339,9*	*340*	*344*	▲	*1%*
Saab Group	*SW*	*398,5*	*404,3*	*402,3*	▼	*1%*

Nom	Pays	Cours au 31/12/17	Cours au 04/01/18	Cours au 18/01/18	▲/▼	Depuis le 01/01/18
Volvo Corp.	*SW*	*153,6*	*158,6*	*163,2*	▲	*6%*
Babcock Int Group	*UK*	*704,5*	*713,8*	*743,4*	▲	*6%*
Bae Systems	*UK*	*571,5*	*574,2*	*584,2*	▲	*2%*
Qinetiq Group	*UK*	*231,5*	*237*	*216,2*	▼	**-7%**
Ultra Electronics	*UK*	*1346*	*1390*	*1492*	▲	*11%*
Boeing	*US*	*294,91*	*297,8*	*348,21*	▲	**18%**
Cisco Systems	*US*	*38,3*	*39,17*	*41,22*	▲	*8%*
Elbit Systems	*US*	*133,29*	*134,51*	*141,61*	▲	*6%*
General Dynamics	*US*	*203,45*	*201,74*	*208,83*	▲	*3%*
Honeywell International	*US*	*153,36*	*152,44*	*159,19*	▲	*4%*
Johnson Controls (Tyco)	*US*	*38,11*	*38,96*	*38,95*	▲	*2%*
Kratos	*US*	*10,59*	*10,95*	*11,17*	▲	*5%*
L3 Communications	*US*	*197,85*	*199,24*	*212,93*	▲	*8%*
LEIDOS / ex SAIC	*US*	*64,57*	*63,92*	*66,79*	▲	*3%*
Lockheed Martin	*US*	*321,05*	*321,21*	*334,75*	▲	*4%*
Northrop Grumman	*US*	*306,91*	*306,65*	*317,42*	▲	*3%*
Raytheon	*US*	*187,85*	*188,3*	*197,47*	▲	*5%*
United Technologies	*US*	*127,57*	*130,04*	*134,86*	▲	*6%*

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

Lockheed Martin

Flottant : 286 480 000 actions soit 99.91% du total des actions
Cours au 31/12/2017 : 321.05 USD
Cours au 04/01/2018 : 321.21 USD
Cours au 18/01/2018 : 334.75 USD
Variation par rapport au 01/01/2018 : + 4 %
Dividende 2017 : 7.46 USD soit un rendement de 2.32 %
Actualités : L'Armée de l'Air française a accueilli le premier C-130J Super Hercules au sein de la 62e escadre de transport sur la base aérienne 123 Orléans-Bricy, sur un total acheté de quatre : deux avions de transport d'armements tactiques C-130J-30 et deux ravitailleurs aériens KC-130J, dont les livraisons se feront en 2019. La France utilise des C-130H depuis 1987 et ces nouveaux C-130J seront intégrés à la flotte existante d'avions Hercules. La France est le dix-septième pays à choisir le C-130J pour ses opérations de transport aérien.

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 06 Février 2018

Ruptures technologiques & ruptures stratégiques

Le SGDSN (secrétariat général de la défense et de la sécurité nationale) a produit en 2017 un recueil, à vocation pédagogique, reflétant le point de vue de chercheurs sur un certain nombre de thématiques relatives aux Armées et à la Défense. Nous en avons extrait quelques unes*.

➔ Les missiles et vecteurs hypervéloces

La France possède des compétences dans le domaine des missiles de croisière, en particulier pour le développement de sa composante nucléaire aéroportée, et conduit des études sur la propulsion hypersonique. Un armement est dit hypersonique lorsqu'il se déplace à une vitesse supérieure à Mach 5. Sur le plan militaire, l'apparition d'armements hypersoniques marque une rupture : leur vitesse disqualifie les capacités actuelles d'interception des défenses adverses ; ces armements offrent une capacité extrêmement réactive à des portées très supérieures à celle des systèmes actuels (hors missiles balistiques) ; ces armements peuvent faire peser, à tout moment et à toute distance, une menace instantanée de frappe conventionnelle ou nucléaire. A l'horizon 2030, des armements hypersoniques figureront dans les arsenaux de plusieurs puissances, la France envisagerait d'en disposer à partir de 2035. C'est à souhaiter.

➔ La révolution de l'impression 3D

L'impression 3D fait référence à un processus de fabrication dit additif (en anglais « AM » pour Additive Manufacturing) qui consiste en la mise en forme d'une pièce par ajout de matière (contrairement à l'usinage qui procède par enlèvement de matière) : polymères thermodurcissables ou thermoplastiques, bois (papier), métaux (titane, chrome-cobalt), matériaux céramiques industriels. Malgré des annonces à sensation, cette technologie est encore à son stade émergent mais l'industrie s'y intéressant va sûrement accélérer le développement de cette technologie. Il est déjà possible d'identifier quatre impacts potentiels de cette technologie sur les enjeux de défense et de sécurité : une remise en cause des équilibres industriels actuels dans une gamme d'activités allant de la chimie et la biologie à la santé, en passant par les industries traditionnelles ; la mise à disposition de la Défense de nouveaux moyens logistiques, notamment dans le domaine de la cartographie du champ de bataille, de la maintenance et de la médecine de guerre ; l'apparition d'un risque nouveau de prolifération d'armes de destruction massive en contournant les contrôles d'acquisitions de matériels sensibles (indépendamment de la fabrication domestique d'armes de poing / affaire Cody Wilson**) ; l'émergence de modes opératoires nouveaux pour les terroristes, la 3D leur permettant à terme de créer facilement eux-mêmes des objets dont l'acquisition est aujourd'hui complexe…

➔ Le champ de bataille « 3.0 »

Les robots et les systèmes autonomes sont déjà présents dans les armées. Ils présentent des capacités souvent supérieures aux capacités humaines et sont capables de précision inaccessible en contrôle manuel : en 2030, téléopérés ou entièrement autonomes, les robots agiront dans les champs d'affrontement physiques et le cyberespace. L'apparition dans les unités opérationnelles d'armes à énergie dirigée pourrait bien être aussi l'amorce de la prochaine révolution militaire : propagation à la vitesse de la lumière d'un faisceau d'ondes électromagnétiques (laser ou micro-ondes). Les avantages en sont multiples: fulgurance du tir, puissance modulable selon le besoin, très grande précision du fait de la directivité du faisceau, économique a priori. Ces armes seront en outre particulièrement adaptées aux combats urbains, qui pourraient se multiplier au milieu de ce siècle lorsque les deux tiers des habitants de la planète résideront dans des zones urbaines…
« Si vis pacem, para bellum » (Si tu veux la paix, prépare la guerre)…AE

Source : Chocs futurs, publié par le SGDSN
** *https://fr.wikipedia.org/wiki/Cody_Wilson*