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

SECURITY DEFENSE
Business review

N° 153 • 05 Juillet 2016

L'actu de la Menace

➔ Turquie : les faux-semblants….

L'Europe a-t-elle plus à craindre du Brexit ou bien de la Turquie ? C'est la question que devraient se poser les politiques qui sont censés gouverner les peuples européens. Le résultat du référendum sur le maintien ou le départ du Royaume Uni de l'Union Européenne a provoqué une tétanie des dirigeants européens aussi forte que leur incapacité, depuis des années, à gérer les flux de migrants qui traversent sans encombres les frontières européennes ou à se mettre d'accord sur la politique à adopter face au danger islamique: Etat Islamique, Al Qaeda, Aqmi, etc. L'attentat suicide perpétré par 3 hommes armés, le 28 juin à l'aéroport Atatürk d'Istanbul, a fait 41 morts et 240 blessés. Les services turcs et américains l'attribuent à l'Etat Islamique, ce qui en ferait son douzième attentat en Turquie depuis 2015. Cela fait beaucoup pour des attentats non revendiqués par EI, mais non démentis non plus. Cela fait aussi beaucoup pour des avertissements. L'EI a subi ses premiers revers du fait de l'intervention russe au coté de l'armée syrienne régulière et, actuellement, EI bat en retraite aussi bien en Syrie qu'en Irak, certaines de ses troupes se repliant en Libye. Alors que nous l'écrivions dans SDBR depuis 4 ans mais que c'était nié par tous les membres de l'OTAN et occulté par les grands medias, il est aujourd'hui admis que la Turquie a été le meilleur allié de l'EI dans ses exactions contre la Syrie, contre les kurdes et contre les chrétiens: allié logistique, allié politique, allié économique. Lorsque deux F-16 turcs ont abattu un chasseur-bombardier russe Su-24, le 24 novembre 2015 sur la frontière turco-syrienne, nous écrivions que la Turquie avait agi sur le conseil de l'administration américaine pour se venger de la déconvenue de sa politique dans la région; parallèlement, la Turquie envoyait vers l'Europe des hordes de migrants infestées de terroristes islamistes, en accord avec la stratégie de l'EI. Pourtant, l'Europe de Bruxelles niait cette évidence. Pourquoi aujourd'hui l'ami d'hier frapperait-il à répétition la Turquie islamique? Est-ce pour reprendre le cours d'une relation distendue, au moment ou l'EI a un cruel besoin de soutien et de zones de replis? Est-ce pour dédouaner Erdogan et faire en sorte que les dirigeants européens se jettent dans ses bras en lui accordant ce qu'il demande (l'entrée en Europe de 80 millions d'habitants plus les millions d'autres qui deviendront par magie de nationalité turque)? Avec une dictature à visée hégémonique, nul n'est capable de savoir ce qui se passe exactement dans la tête du dictateur, l'Histoire l'a montré. Un fait à retenir: la Turquie d'Erdogan veut reconstituer le grand Empire Ottoman qui, en l'an 1600, réunissait la Turquie, l'Irak, la Syrie, la Jordanie, l'Egypte, la Libye et le Maghreb d'un coté, la Grèce, l'ex-Yougoslavie, la Roumanie et la Hongrie de l'autre coté! Pour sa part, EI veut reconstituer le Califat islamique du VIIème siècle: le Portugal, l'Espagne et toute l'Afrique du Nord, le Moyen-Orient, les Balkans, l'Asie Centrale, l'extrémité sud de la Russie et une partie de l'Inde. Cherchez l'erreur ! AE

SOMMAIRE

AGENDA

➢**27 - 29 Septembre 2016 - Moscou, Russie**
Infosecurity Russia
➢**28 - 30 Septembre 2016, Singapour**
Safety & Security Asia
➢**05 - 08 Octobre 2016 - Monaco**
Assises de la sécurité et des SI
➢**16 - 20 Octobre 2016 - Dubaï, EAU**
GITEX Technology week
➢**25 - 27 Octobre 2016 - Kuala Lumpur**
AVSEC World 2016

Plus d'infos

➔ Ransomware

D'après Kaspersky, le nombre d'utilisateurs ciblés par des attaques de crypto-ransomware a atteint 718 536 (avril 2015 à mars 2016) soit 5,5 fois plus que l'année précédente. Cette augmentation s'explique par la rentabilité de ces menaces pour les cybercriminels.

Interview de Guy Duplaquet

Chef de la mission de préfiguration du réseau radio du futur
Ministère de l'intérieur

♦ **SDBR : Le salon CCW est l'occasion de faire le point avec vous de la réflexion française sur les réseaux de communication critiques. Où en êtes-vous ?**

GD : Aujourd'hui, en France, en matière de réseau d'appui aux équipes de la sécurité intérieure et de secours aux personnes et aux populations, nous avons une seule technologie, mais, pour des raisons essentiellement historiques, deux réseaux: RUBIS, le premier réseau construit en TETRAPOL, conçu à la fin des années 80, déployé sur une dizaine d'années à partir du début des années 90 et utilisé par la Gendarmerie, utilise la gamme de fréquence 80 MHz, et le réseau INPT (Infrastructure Nationale Partageable des Transmissions), initialement appelé ACROPOL pour la police et ANTARES pour les pompiers et la sécurité civile, également construit en TETRAPOL, mais sur une gamme de fréquence différente de celle de RUBIS. La technologie TETRAPOL est du type 2G (plutôt même 1.5G). Fonctionnellement, son temps d'établissement des communications est inférieur au temps de connexion des communications classiques. Les deux réseaux, RUBIS et INPT, sont interconnectés et sont architecturés autour de la maille départementale. Le réseau RUBIS est entièrement construit sous une architecture interne IP ce qui n'est pas le cas de l'INPT, qui a encore une part très significative en TDM (protocole ancien Time division multiplexing). La migration vers l'IP en cours s'avère complexe..

♦ **Remplacer carrément le type de réseau est-il plus aisé que faire migrer un réseau vers plus de technologie ?**

Faire migrer un réseau revient à déclencher un «big bang» au jour J à l'heure H, avec tous les risques induits. Changer de réseau – fonctionnant sur des fréquences distinctes – permet de faire cohabiter les 2 réseaux le temps nécessaire au rodage du nouveau système. Je tiens à préciser que RUBIS et INPT rendent les services pour lesquels ils ont été conçus (transmission de la voix, communication de groupe, messages courts) et ils ont montré, lors d'événements tragiques récents, une réelle résilience: lors du crash de l'avion de la German Wings, nous avons reconfiguré le réseau pour avoir une bonne couverture de la zone impactée; lors de l'attentat du Bataclan, le réseau parisien a parfaitement supporté la charge – pourtant intense au regard de l'importance de la mobilisation des moyens déployés – et les problèmes rencontrés ont relevé essentiellement de problématiques d'usage des terminaux et non du réseau lui-même.

♦ **Quelles sont les difficultés que vous rencontrez aujourd'hui avec les réseaux RUBIS et INPT?**

Elles sont de plusieurs types. Au plan technologique comme je l'ai dit, TETRAPOL est une technologie proche de la 2G qui n'est pas conçue pour la transmission de données au sens où on l'entend aujourd'hui, même si, en situation de crise, c'est toujours sur la voix qu'on va d'abord compter pour gérer les situations et assurer le commandement. Hors temps de crise toutefois, l'absence de capacité de transmission de données large bande est pénalisante. Sans doute dans le futur, y compris en situation de crise, aurons-nous besoin de transmettre des données, mais ce sont des usages nouveaux qu'on perçoit encore mal. Actuellement, du fait de l'absence de transmission de données sur les réseaux TETRAPOL, nous constatons des usages «détournés» par les personnels des moyens de communications commerciaux pour transmettre des données. Nous tenons compte de cette situation: le ST(SI)²* développe, au travers de Neo, des solutions de sécurisation de l'accès aux systèmes d'information opérationnels au travers des réseaux commerciaux et la direction des systèmes d'information et de communication (DSIC) développe span, une solution d'accès en mobilité au poste de travail nominal d'un agent, mais, tant avec Neo qu'avec span, nous n'aurons toujours que la disponibilité – perçue comme limitée – des moyens commerciaux. Nous sommes actuellement dans une situation où ces moyens commerciaux utilisés présentent un niveau de risque significatif, risques qu'il convient d'adresser. Ceci étant, l'appui pérenne sur les réseaux commerciaux, au moins en débordement/secours – mais, potentiellement, en fonction d'arbitrages éventuels à venir, sur un périmètre plus important qui reste à définir – fait d'ores et déjà l'objet de travaux amont, au travers de réflexions sur la mise en œuvre d'un opérateur virtuel étatique (projet M3I, conduit par la DSIC).

♦ **A quoi faites-vous allusion en parlant d'usages « détournés » ?**

Les forces de police et de gendarmerie sont des utilisateurs comme les autres et la nouvelle génération utilisera ses appareils professionnels comme elle utilise déjà son Smartphone. C'est un état de fait qui constitue un élément de la réflexion à conduire sur la radio de demain: le monde de la radio doit donc s'adapter à ces évolutions, qui sont irrémédiables. Une partie du «détournement» d'usage des réseaux commerciaux vient de l'écart fonctionnel très important qui existe entre les terminaux actuellement utilisés sur INPT et RUBIS, et le Smartphone qui est le moyen – privé ou professionnel – standard de communication des personnels. Cet écart fonctionnel est tellement important qu'il génère une réaction de rejet de la part de certains utilisateurs. Lorsque les industriels justifient la migration vers la 4G ou la 5G, uniquement en faisant valoir le besoin de large bande, je pense qu'ils omettent le moteur de l'utilisation des terminaux, qui existerait même s'il n'y avait que la voix qui devait être transportée; il faut tenir compte de la facilité d'usage et de l'ergonomie, appréciées des utilisateurs.

Suite de l'interview page 3

**ST(SI)² : Service des technologies et des systèmes d'information de la sécurité intérieure. Lors de cette interview, Guy Duplaquet était accompagné du colonel Gonzague Montmorency, chef du bureau de la prospective radio au ST(SI)².*

Interview de Guy Duplaquet

Chef de la mission de préfiguration du réseau radio du futur Ministère de l'intérieur

♦ **Quelle est donc la stratégie française dans ce domaine ?**

Notre stratégie est de sauter une génération et d'engager la construction d'un réseau appuyé pour l'instant sur les technologies LTE 4G au standard 3GPP. Plusieurs éléments sont déjà calés. Tout d'abord, il s'agit au plan technique de s'aligner inconditionnellement sur la normalisation internationale. L'objectif est de concevoir un réseau pouvant profiter d'un écosystème de partenaires extrêmement riche et diversifié, apte à évoluer dans le temps, éventuellement en substituant des composants ou en changeant de fournisseur, sans avoir à réinventer l'ensemble du dispositif.

♦ **Construire un nouveau réseau national ne prendra t-il pas trop de temps ?**

C'est une opération longue, comme on l'a vu avec RUBIS et INPT où il a fallu entre dix et quinze ans pour avoir une couverture significative. La durée de vie des systèmes est aussi un paramètre important. Les plans d'Airbus D&S, principal fournisseur de l'INPT et de Rubis, affichent un arrêt de la commercialisation et de la maintenance des équipements TETRAPOL (non IP) TDM à l'horizon 2020 et un arrêt de la maintenance des équipements IP à l'horizon 2030. Donc c'est aussi un moteur pour nous. 2020 étant beaucoup trop court, nous avons décidé de mettre en place une formation des personnels , un plan de migration partiel et une noria d'équipements provenant des plaques régionales migrées afin de maintenir les plaques en TDM. Nous envisageons de déployer les premiers pilotes industriels en 2021, puis d'équiper une métropole test en 2023 avant un éventuel déploiement parisien. C'est donc une opération lourde, estimée à ce stade à environ un milliard d'euros sur quinze ans, qui ne s'improvise pas...

♦ **Est-ce plus cher que le coût de RUBIS et INPT ?**

Le coût cumulé depuis 20 ans de RUBIS et INPT est d'environ 2,5 milliards d'euros et le coût actuel de maintenance de ces deux réseaux est d'environ 60 millions par an. Avec le projet d'un nouveau réseau nous avons donc un objectif de réduction importante, à terme, des coûts globaux.

♦ **Comment allez-vous gérer les urgences critiques, nombreuses en ce moment, entre 2016 et 2021 ?**

A très court terme, nous allons mettre en place quelques réseaux tactiques LTE (en bande 700MHz) et un service de mobilité critique pour le GIGN, le RAID et la BRI. Le projet, piloté par les équipes du ST(SI)^2, a fait l'objet d'un appel à candidature publié le 15 juin dernier, ce qui amène les différents industriels à se positionner. Le déploiement est prévu mi-2017. Même si ce marché ne vise pas à la construction du grand réseau à couverture nationale cible du programme RRF, cet appel à candidature va nous permettre de poser des briques significatives du réseau du Futur. Ces premières briques vont nous permettre de disposer d'un vrai Retex des utilisateurs et de pouvoir observer comment ils s'emparent des nouvelles fonctionnalités. Au travers de ces briques, nous voulons répondre aux besoins opérationnels des forces d'intervention mais nous voulons aussi en profiter pour apprendre autour de la technologie LTE, identifier les satisfactions, les difficultés opérationnelles et tester les services d'itinérance (multi-roaming) sur les réseaux commerciaux, indispensables lorsqu'on se trouve hors couverture. En parallèle, nous allons travailler sur la gouvernance et l'organisation du réseau du Futur, sur le statut juridique et le financement (service à compétence nationale, régie directe du ministère de l'intérieur, établissement public, etc...), et continuer à réfléchir au plan technique (quelle articulation avec les réseaux commerciaux ?). Nous comptons avoir posé les différents scénarios pour un arbitrage au printemps 2017, confirmés à l'horizon de l'automne 2017 (du fait des échéances politiques).

♦ **La France est-elle en avance ou en retard sur ce sujet ?**

Nous ne sommes certainement pas en retard ! Bien sûr, la Corée du Sud dispose d'ores et déjà de son réseau LTE, le Royaume-Uni a notifié son marché et les États-Unis ont lancé leur propre consultation, en avance sur nous. De très nombreux autres pays, comme l'Allemagne, viennent cependant tout juste de déployer leur réseau national Tetra/TEDS (2G/3G) et n'envisagent pas, à court terme, de s'engager dans une nouvelle modernisation. Un domaine où nous avons une petite avance en termes de maturité de la réflexion, me semble-t-il, est le fait d'envisager de travailler avec certains opérateurs d'infrastructures: transport (ADP, SNCF, RATP etc.), énergie (EDF, etc.). Ces opérateurs ont des besoins de liaisons radios et leurs missions intègrent un important volet sécurité et de secours. Nous avons de fait, de manière récurrente, des besoins d'interopérabilité lors d'interventions. Cependant les équipements, pour les emprises géographiques correspondantes, sont potentiellement très onéreux et leur installation sous le contrôle de l'État poserait certainement des problèmes de responsabilité. Le principe de l'accord envisagé serait d'apporter nos fréquences sur leurs emprises géographiques, pour leur faciliter l'implantation de leur réseau et, en échange, d'accueillir nos agents en situation de crise et de nous laisser préempter en tant que de besoin leurs ressources.

♦ **Est-ce que les industriels français vous suivent dans cette préparation de la radio du Futur ?**

De notre point de vue, il est important que les industriels français travaillent aussi sur les groupes de normalisation et de standardisation, et qu'ils participent donc à la réflexion autour des réseaux du Futur: nous avons tout intérêt à ce que l'écosystème sur lequel nous allons nous appuyer soit riche, dynamique et diversifié en compétences (équipementiers, intégrateurs, opérateurs...).

Interview réalisée par Alain Establier

EUROSATORY, la suite

Le salon Eurosatory a été l'occasion de rendre visite au pavillon israélien, toujours très fourni en exposants. Derrière les grands du secteur (Rafael, Elbit Systems) ont éclos des PME présentant souvent des innovations techniques.

➔ Rafael

Le missilier présentait son système de protection air-sol à courte portée Iron Dome, mis en service opérationnel en 2011 pour contrer les attaques de rockets et les tirs de mortiers du Hezbollah et des Palestiniens sur les villes et les sites sensibles israéliens. Iron Dome a été initié pour devenir autonome vis-à-vis du protecteur américain et de son système Patriot construit par Raytheon. Le système est discriminant et permet de choisir la menace à éliminer (rocket, obus), en fonction des trajectoires prévisionnelles analysées d'une salve par exemple. Le système aurait permis d'intercepter 1500 rockets depuis 2011, avec un taux de réussite de 90%. www.rafael.co.il

➔ Netline Communications Technologies

Considérant qu'un minidrone peut présenter une menace similaire à un IED (engin explosif improvisé), en utilisant les mêmes types de technologies, la société Netline a développé un système de capteurs pour identifier l'approche d'un drone et le neutraliser, sous 3 formes: un modèle pour véhicule, un modèle facilement transportable et un modèle portable par l'homme, le tout pour des utilisations différentes ou complémentaires afin de sécuriser un périmètre (ex. une prison, une usine), une frontière ou un rassemblement de personnes. Utilisable par tous les temps, nuit et jour, il utilise la gamme de fréquence 20MHz / 6GHz pour neutraliser le drone. www.netlinetech.com

➔ Bluebird Aero Systems

Depuis plusieurs années, Bluebird Aero Systems produit pour le ministère israélien de la Défense et a commencé à développer des minidrones volants, pouvant voler 4 heures à 3600 pieds dans un rayon de 80kms (utilisés entre autres en Bolivie et en Australie). Depuis 4 ans, Bluebird a voulu développer un drone tactique, plus endurant et pouvant voler plus loin, à mi-chemin entre le minidrone et le drone MALE: le Thunder B. Avec 24h d'autonomie, grâce à la gestion informatisée de son carburant, il évolue à 2000 mètres d'altitude dans un rayon de 100 à 150 kms. Il embarque tous les équipements nécessaires à son intégration à un système de C4i, pour des missions de renseignement, de surveillance ou d'acquisition de cible (voire plus…).

➔ General Robotics

Cette start-up présentait pour la 1ère fois un fantastique petit robot terrestre, pour les forces spéciales ou les forces de sécurité, destiné à neutraliser des adversaires en milieu urbain. D'un poids de 12kgs, extrêmement manœuvrable, pouvant monter et descendre des obstacles comme des escaliers, il a une autonomie de 2 à 5 heures suivant l'utilisation. Il est équipé de 8 caméras digitales lui permettant une vision circulaire, dispose de capteurs de lumière et de température, d'un module GPS et peut faire de l'acquisition de cible «point & shoot». Il peut être équipé d'un Glock 26, pistolet de 9mm à 14 coups. Idéal pour neutraliser des tireurs embusqués… www.glrobotics.com

➔ Rada Electronic Industries

Cette PME de 100 collaborateurs, implantée sur 2 sites en Israël, produit et développe toute une gamme de radars de détection de tirs hostiles: des radars terrestres statiques ou déployables, des radars manœuvrables embarqués dans des véhicules légers ou blindés et des radars pour les frégates. Les radars sont opérationnels entre -40°C et +55°C; ils couvrent, selon les modèles, la zone des 2km (tir de rocket) à 12km (tir de mortier). Rada a aussi toute une gamme de détection aérienne allant de 3,5km à 100km selon les objets volants (du minidrone à l'avion de transport lourd) et selon les modèles de la gamme. www.rada.com

Les marchés financiers

Retour au calme sur les marchés après deux journées d'autant plus noires que les marchés avaient bizarrement joué le «remain» durant les 4 jours précédant le scrutin; le calme semble donc revenu sur les marchés. La baisse de la livre et celle des actions bancaires (pas seulement celles de la City) n'ont cependant été que très partiellement corrigées, ce qui est d'ailleurs assez intuitif et rappelle que l'un des enjeux principaux des négociations tournera autour du rôle de la City. Le «Brexit» va être le fil rouge des marchés cet été. Les actifs britanniques seront confrontés à la défiance durable des investisseurs mais bénéficieront, si besoin est, du soutien de la Banque d'Angleterre. Dans le reste de l'Union Européenne, le front uni présenté par les dirigeants de l'UE 27 est rassurant pour les marchés, mais les brèches qui ne manqueront pas de s'ouvrir au fil des semaines devraient générer de la volatilité. A noter enfin que le risque de hausse des taux directeurs américains paraît s'éloigner. Même si c'est pour de mauvaises raisons (la Fed considère que la croissance américaine est trop faible et vulnérable aux conséquences du «Brexit»), cela enlève un facteur d'inquiétude aux marchés boursiers.

Les Leaders du secteur Security & Defense

Nom	Pays	Cours au 31/12/15	Cours au 17/06/16	Cours au 30/06/16	▲/▼	Depuis le 01/01/16
Rheinmetall	DE	61,48	54,52	53,07	▼	-14%
Siemens	DE	94,60	92,29	90,92	▼	-4%
ThyssenKrupp	DE	18,34	18,5	17,94	▼	-2%
Airbus Group	FR	62	50,83	52,4	▲	-15%
Alcatel-Lucent	FR	3,57	3,49	3,47	▼	-3%
Atos	FR	77,45	77,94	74,04	▼	-4%
Dassault Aviation	FR	1146	931,5	904,95	▼	-21%
Safran	FR	63,37	56,93	60,69	▲	-4%
Thales	FR	69,1	72,26	75,67	▲	10%
CNHI / ex Fiat Industrial	IT	6,34	6,54	7,09	▲	12%
Finmeccanica / Leonardo	IT	12,9	11,56	8,86	▼	-31%
Hitachi Ltd	JP	691,5	457	423,9	▼	**-39%**
Mitsubishi Electric	JP	1282	1260	1208	▼	-6%
Panasonic	JP	1240	898,2	881	▼	-29%
Sony	JP	3002	2899	2988	▲	0%
Assa Abloy	SW	178	162	170,4	▲	-4%
Axis AB	SW	343,4	331,6	338,9	▲	-1%
Saab Group	SW	260,8	260,5	260,6	▲	0%

Nom	Pays	Cours au 31/12/15	Cours au 17/06/16	Cours au 30/06/16	▲/▼	Depuis le 01/01/16
Volvo Corp.	SW	79,1	88,7	82,65	▼	4%
Babcock Int Group	UK	1016	980	893,5	▼	-12%
Bae Systems	UK	499,6	478,3	512	▲	2%
Qinetiq Group	UK	268,88	233,9	219,7	▼	-18%
Ultra Electronics	UK	1976	1674	1692	▲	-14%
Boeing	US	144,59	129,82	126,99	▼	-12%
Cisco Systems	US	26,95	28,95	28,26	▼	5%
Elbit Systems	US	88,33	89,69	89,83	▲	2%
General Dynamics	US	136,64	138,99	135,63	▼	-1%
Honeywell International	US	103,57	115,92	114,46	▼	11%
Kratos	US	4,1	4,05	3,94	▼	-4%
L3 Communications	US	119,51	143,7	143,32	▼	20%
LEIDOS / ex SAIC	US	56,26	46,85	46,8	▼	-17%
Lockheed Martin	US	217,15	237,56	244,08	▲	12%
Northrop Grumman	US	188,81	214,32	217,24	▲	15%
Raytheon	US	123,86	134,66	135,07	▲	9%
Tyco International	US	31,68	42,99	41,7	▼	**32%**
United Technologies	US	96,07	101,2	100,47	▲	5%

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

Kratos Defense & Security

Flottant : 445.700.000 actions soit 76059 % du total des actions
Cours au 31/12/2015 : 4.10 USD
Cours au 03/06/2016 : 4.05 USD
Cours au 17/06/2016 : 3.94 USD
Variation par rapport au 01/01/2015 : - 4 %
Dividende 2016 : 0 USD soit un rendement de 0 %
Actualités : Kratos a annoncé avoir reçu un contrat de 9,4M USD pour la maintenance des systèmes de formation à l'avionique des hélicoptères d'un allié majeur des Etats-Unis. Kratos a récemment reçu 10M de commandes pour des produits spécialisés à l'appui d'un programme de système de communication aéroporté et 3,6M pour la conception, l'ingénierie, le déploiement et l'intégration de systèmes de sécurité spécialisés pour 2 grandes sociétés de transport de personnes américaines.

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 : 950 € HT (TVA 20%: 1140 € TTC)
Abonnement semestriel : 600 € HT (TVA 20% 720 € TTC)
ISSN 2107-7312

Prochain Numéro: **Mardi 19 Juillet 2016**

4 questions à Eric Davalo

Directeur Stratégie, portefeuille de solutions et ingénierie de Secure Land Communications*, Airbus Defence and Space

➔ SDBR: Votre produit « Tactilon Cell » est-il un produit militarisé ou civil ?

ED : C'est en fait une bulle tactique Broadband, complètement intégrée, sur laquelle nous avons tous les éléments radio et réseau nécessaires pour fonctionner en autonomie mais aussi les applications sécurisées d'échanges de vidéo, de données et de voix intégrant les fonctions de prise d'alternat. C'est un produit extrêmement compact qui peut être transporté par une seule personne, de faible consommation énergétique, et qui peut servir pour des interventions critiques, que ce soit dans le domaine de la Défense ou de la Sécurité Publique. Nous ne sommes pas sur le champ de bataille pour autant et ce produit, basé sur les technologies radio 3GPP commerciales, n'est pas destiné à des environnements de guerre électronique. Tactilon Cell intègre aussi les dernières versions des standards 3GPP qui offrent certaines des fonctions nécessaires pour les communications sécurisées, comme une gestion de la Qualité de Service adaptée et un premier niveau de communication de groupe vocale.

➔ Serait-ce le début prévisible d'une évolution du militaire vers des produits du quotidien ?

Nous pensons qu'une partie du marché va évoluer pour bénéficier des avancées du 3GPP dans les technologies mobiles commerciales et dans les fonctions spécifiques destinées aux communications critiques. Au sein d'Airbus Defence and Space, nous avons déjà intégré du Wimax pour les besoins logistiques de l'armée française et nous avons adapté du LTE en bande de fréquence 400 MHz pour l'armée allemande. Tactilon Cell utilise du LTE sur des bandes de fréquences pour lesquelles des solutions commerciales existent et intègre des communications de groupe sécurisées basées sur la première version du standard 3GPP dans ce domaine. Cette démarche est suivie par nos clients Défense et Sécurité qui vont sur des bulles tactiques, faciles à faire évoluer et à remplacer au rythme des évolutions technologiques commerciales et de l'ajout des fonctions 3GPP spécifiques nécessaires aux communications sécurisées. Ces solutions demandent, pour des utilisateurs comme la Défense, des investissements beaucoup moins importants que des solutions comme la SDR (Software Defined Radio) utilisée sur les champs de bataille. Ces solutions amènent des innovations technologiques rapides car les technologies, radios et réseaux, commerciales qu'elles utilisent sont standardisés au 3GPP et donc leurs développements bénéficient des financements en R&D énormes qui sont rendus possible par la taille du marché commercial «standard» qu'elles adressent en priorité.

➔ N'y a-t-il pas là une contradiction avec les quelques 80 millions que l'Etat français vient de débloquer pour continuer à faire vivre les réseaux tactiques actuels ?

Les technologies de communication radio mobile existantes, que ce soit les réseaux tactiques militaires ou les systèmes de communications sécurisées TETRAPOL ou TETRA, remplissent parfaitement leur mission et sont les seules options disponibles aujourd'hui pour assurer les communications critiques indispensables dans leur champ d'utilisation. La mise en œuvre des technologies Broadband issues du 3GPP permet de les compléter en offrant un plus grand débit et donc l'accès à des applications multimédia, mais elles ne disposent pas de nombre de fonctions critiques indispensables. Le 3GPP propose une feuille de route pour intégrer ces dernières, mais l'émergence d'un écosystème à même de remplacer en partie les technologies existantes va prendre du temps. Il est donc important que les systèmes existants continuent à évoluer et soient maintenus en condition opérationnelle pour au moins les dix années à venir. En parallèle, nos clients mènent des expérimentations, soit en utilisant des services d'opérateurs mobiles, soit avec des bulles tactiques, afin de se préparer à une potentielle migration à l'horizon 2025.

➔ L'arrivée des opérateurs sur ce secteur va-t-elle changer le marché ?

Les opérateurs fournissent depuis longtemps des services de communication aux forces de sécurité pour ce qui est du transfert de données. Nous travaillons déjà avec eux et les solutions que nous avons livrées en Finlande ou en Belgique (Blue Light Mobile) pour du transfert de données passent sur des réseaux d'opérateurs mobiles, en y apportant plus de sécurité, de capacité et de résilience. Ainsi ASTRID** possèdent ses propres cartes SIM et contrôle de bout en bout la sécurité de ses communications de données. Nous pensons que ce type de schéma va se multiplier, mais selon des options qui ne sont pas encore figées. Pour Airbus Defence and Space, ces solutions complètent les systèmes de communications critiques dédiés basés sur les technologies TETRAPOL et TETRA. Nous apportons les applications et terminaux métiers, l'intégration et la sécurisation de la solution de bout en bout.

Interview réalisée par Alain Establier

** Secure Land Communications : http://www.securelandcommunications.com*
*** CCW: https://criticalcommunicationsworld.com*
*** ASTRID : https://fr.wikipedia.org/wiki/A.S.T.R.I.D*