Mai 2015

Lettre d'information de

Guerrelec

Si vis pacem para bellum... electronicum

N° 50

Le mot du Président

Chers amis,

Voici le 50ème numéro de notre Lettre de Guerrelec. Nous en avons fait un Numéro Spécial à l'occasion du 50ème anniversaire de l'Association des Old Crows (AOC), d'autant que cet évènement vient d'être célébré par un Colloque organisé par notre Association le mercredi 26 novembre 2014 au Fort du Mont Valérien, à Suresnes sur le thème : **« Comment rester maître de l'Ether et du cyberespace »**. *Nous adressons nos remerciements au colonel Jacques Eyhardts, chef de corps du 8ème RT du Mont Valérien qui nous a accueillis dans ses quartiers.*

Après 50 ans des Old Crows et 100 ans de Guerre Electronique, cette journée, destinée à enrichir la réflexion sur la problématique de l'utilisation de l'espace électromagnétique, avait pour ambition de mettre l'accent sur toutes les facettes de ce sujet complexe. Inaugurée par Monsieur Jean-Marie Bockel, sénateur du Haut-Rhin et ancien ministre, et clôturé par Madame Patricia Adam, députée du Finistère, présidente de la Commission de la Défense Nationale et des forces armées, elle a permis d'entendre le point de vue de nombreux conférenciers experts dans divers domaines de la Guerre Electronique. L'évènement a été couronné par un hommage à Jean Turck, pionnier de la Guerre Electronique, né en 1911 qui nous donne un témoignage vivant d'une époque héroïque.

Cette lettre présente la synthèse du Colloque qui a été animé par de nombreuses personnalités devant un public choisi.
Bonne lecture.

IGA Pierre **GRANDCLEMENT**
Président de Guerrelec

Colloque Guerrelec

Synthèse des conférences

50ème anniversaire de l'Association des Old Crows,
Mercredi 26 novembre 2014, Fort du Mont Valérien, Suresnes
« Comment rester maître de l'Ether et du cyberespace »

L'IGA Pierre Grandclément, Président de Guerrelec, et le colonel Jacques Eyharts, chef de corps du 8ème RT, qui nous a accueillis au Fort du Mont Valérien

L'IGA Pierre Grandclément et l'amiral Jean-Pierre Vadet (Guerrelec), entourant le colonel Jacques Eyharts (8ème RT)

Introduction au Colloque

par le sénateur Jean-Marie Bockel [1]

Le sénateur Jean-Marie Bockel durant son intervention

Cyberdéfense et Guerre Electronique sont intimement liées et partagent de nombreuses caractéristiques. Ces domaines d'excellence française sont à la fois une formidable source d'information, mais aussi de vulnérabilité. Ils contribuent largement à la fonction «Connaissance et Anticipation» que le Livre Blanc a érigé en priorité. Avec l'évolution technologique, les systèmes militaires sont devenus fortement dépendants des systèmes d'information qui les constituent intrinsèquement ou les relient aux différents centres de commandement. Or la technologie numérique génère des failles, surtout avec l'utilisation de systèmes d'exploitation issus du domaine civil, qu'il faut circonscrire.

La France doit être au premier rang européen en matière de cyberdéfense. Les moyens montent en puissance dans le cadre de la LPM : moyens humains, technologiques, financiers, et formation :

- c'est la protection des OIV (Opérateurs d'Importance Vitale), environ 250, issus du secteur public et privé ;
- c'est, sous l'impulsion du pacte « Défense Cyber », la montée en puissance du CALID (Centre d'Analyse de la Lutte Informatique Défensive) avec le recrutement de 350 personnels supplémentaires sur la période de la LPM 2014-2019 et le renforcement des effectifs de cyberdéfense du centre DGA/ Maîtrise de l'information, situé à Bruz, pour atteindre environ 400 spécialistes de très haut niveau d'ici 2017, colocalisés avec ceux du centre d'expertise en Guerre Electronique ;
- c'est l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), dont les effectifs devront atteindre 500 en 2015 ;
- c'est, dans le domaine capacitaire, le renforcement de la posture de cyberdéfense : les moyens alloués à l'acquisition et au fonctionnement des équipements dédiés à la cyber-sécurité doivent atteindre 360 M€ sur la période 2014-2019 et les crédits consacrés à la R&D devraient être triplés.

Mais il n'y a pas de souveraineté et de sécurité nationale sans politique industrielle. Les enjeux industriels concernent aussi bien la Guerre Electronique que la cyberdéfense. Il s'agit de développer une véritable politique industrielle à partir des atouts que possèdent nos industriels, que ce soit les grands industriels qui ont déjà commencé à se diversifier dans le domaine de la Cyber ou le réseau de PME qui gravite autour d'eux mais qui sont souvent fragiles. La Guerre Electronique représenterait environ 5 000 emplois hautement qualifiés, non délocalisables. La cyberdéfense devrait concerner bientôt autant d'emplois.

Il est indispensable aussi de développer des coopérations industrielles en Europe - coopérations binationales ou trinationales - pour bien maîtriser ce qu'on décide de partager et pouvoir mettre en place des financements, parfois difficiles à garantir par une seule nation.

Il faut enfin veiller à la bonne exécution de la LPM pour maintenir les programmes d'études amont, pérenniser les industries Cyber et Guerre Electronique, les compétences qu'elles génèrent et maintenir ces domaines d'excellence.

Derrière la dimension Défense il y a également toute une dimension civile et sociétale : enjeux économiques par rapport à l'espionnage massif, enjeux également de préservation de la vie des citoyens qui sont de plus en plus « connectés ». Il s'agit de prendre conscience que ces enjeux sont essentiels pour la liberté de chacun, le devenir de notre société et de notre civilisation. Nous ne sommes plus uniquement sur des enjeux militaires et technologiques, mais également sur des enjeux sociétaux extrêmement importants qui doivent alimenter nos réflexions.

Nota 1 : Le sénateur et ancien ministre Jean-Marie Bockel s'est investi en 2011-2012 dans l'élaboration d'un rapport parlementaire sur la Cyberdéfense qui a été intégralement repris dans le livre blanc 2013 et la Loi de Programmation Militaire (LPM).

Quelques membres distingués de l'association Guerrelec

Table Ronde N°1 :

Les enjeux de la maîtrise du spectre

Modérateur : Philippe GUILLAUME, ancien directeur de la Guerre Electronique de Thales Communications et Sécurité

Le spectre radioélectrique : une ressource vitale

par Joelle Toledano, Professeur d'économie, membre du conseil d'administration de l'ANFR.

C'est le premier des trois points de vue correspondant à trois usages du spectre radioélectrique choisis pour illustrer les enjeux de la maîtrise du spectre :

Le numérique dévore le monde : une étude de l'INSEE faite en 2009 indiquait que 80 % de l'économie française était concernée par le numérique. Dans les 20% d'activités restantes, considérées comme non touchées par le numérique, l'INSEE avait identifié l'agriculture, la pêche, les services à la personne …

De g. à dr., Philippe Guillaume (Guerrelec), Joelle Toledano (ANFR), le général Dran (DRM), Gérard Labaune (Thales), Robin Marijon (Thales)

Autant de sujets dont nous avons aujourd'hui la preuve qu'ils sont totalement concernés par la numérisation.

Cette numérisation génère donc des échanges d'informations qui sont transportées par des réseaux de communication. En 2012, la moitié du flux d'informations échangées passait par des réseaux de communication sans fil, utilisant le spectre radioélectrique. En 2017, selon CISCO, les 2/3 des informations échangées passeront sur ces réseaux sans fil. Par ailleurs, les échanges d'informations continuent à augmenter de façon considérable. De 2012 à 2017 est prévue une augmentation du trafic de 13 % par an sur les réseaux fixes et de plus de 30 % sur les réseaux sans fil. Durant cette même période, le trafic généré par les ordinateurs individuels, 75 % à ce jour, diminuera pour tomber à moins de 50 %. Le trafic sera donc généré principalement par le M2M (6 milliards d'objets connectés en France en 2020), les Smartphones et autres tablettes.

Parallèlement au développement des communications mobiles qui utilisent des licences exclusives d'accès au spectre, le succès du WIFI résulte de l'ouverture à tous de bandes de fréquences gratuites et harmonisées. Le WIFI a valorisé le haut débit fixe tout en permettant aux opérateurs de réseaux mobiles de réaliser des économies d'investissement substantielles. Ce spectre, dont l'importance croissante a été démontrée, est géré de façon à régler les problèmes d'interférences et de « spectrum crunch ». L'objectif de la gestion du spectre est de maximiser la valeur (économique et sociale) que la société peut retirer de son utilisation par un maximum d'agents tout en minimisant les problèmes d'interférences entre ces agents. La gestion est assurée au niveau international par l'UIT, organisme des Nations Unies, au niveau européen par le CEPT et au niveau national par l'ANFR. Trois modèles de gestion des fréquences coexistent :

- fréquences allouées à des administrations pour des besoins exclusifs (aviation civile, fréquences militaires…)
- fréquences allouées à des sociétés privées pour des services aux particuliers (réseaux mobiles)
- fréquences librement utilisables (sans licence).

Face à la croissance des besoins, il convient de faire évoluer ces modèles en ayant recours au partage dynamique qui présente plusieurs caractéristiques intéressantes :

- il permet un usage plus efficace du spectre d'un point de vue économique
- il est compatible avec la législation française
- il est porteur de solutions techniques innovantes.

Il convient de compléter le partage économique du spectre par la mise à disposition de fréquences libres de droits, partagées par tous selon des critères techniques précis.

Pour en savoir plus : http://www.economie.gouv.fr/files/files/pdf/rapport-gestion-dynamique-2014-06-30pdf.

Le spectre radioélectrique : une source d'informations

par le Général Bruno Dran, Directeur Adjoint de la DRM.

Le général Bruno Dran, Directeur Adjoint de la DRM

L'Éther est une source centenaire de renseignements qui s'est diversifiée au cours du vingtième siècle. Dès 1914, tout était en place : les interceptions, le cassage du chiffre, mais aussi l'élaboration du renseignement de synthèse

pour le commandement ainsi que la collaboration avec les pays alliés. Après les écoutes, l'interception des radars a apporté des informations supplémentaires essentielles de même que la capacité à localiser de façon précise les émetteurs.

On en arrive ainsi à la définition des missions de la DRM qui doit fournir des renseignements de synthèse pour le commandement, du renseignement en soutien des opérations et, de plus en plus, du renseignement aux fins d'actions. Pour cela, la DRM dispose d'un certain nombre de moyens en termes d'interception mais aussi des moyens d'exploitation. Pour chaque opération, elle définit les moyens de renseignement à déployer et en assure le maillage.

Equipement radio de la 1ère Guerre mondiale

Equipement radio de la Seconde Guerre mondiale

Pour l'avenir cinq grandes tendances apparaissent :

- la mutualisation complète des dispositifs d'interception
- longue distance entre les trois grands services à savoir DGSE, DRM et DGSI. Cette mutualisation arrive après le spatial militaire HELIOS qui avait été faite d'emblée ;
- la suppression des barrières entre le renseignement tactique et le renseignement stratégique. A l'avenir, un maillage important entre le renseignement de terrain et le renseignement stratégique est fondamental ;
- l'automatisation de l'exploitation du renseignement afin d'économiser la ressource humaine. Pour cela, il convient de continuer les efforts sur la partie déchiffrement mais aussi sur le développement des outils de type traduction automatique, reconnaissance automatique de langues, reconnaissance de locuteurs.

- la cible ayant été détectée, il est nécessaire d'avoir un moyen de surveillance souvent aérien (drones ou avions) qui permet de ne plus la lâcher. La France n'a pas les moyens de se payer de gros avions spécialisés. Il faut des petits avions avec des charges mixtes, optiques et écoutes, incluant la capacité de localisation.
- les opérations se déroulent de plus en plus en coopération avec de grands alliés. Cette coopération est d'autant plus fructueuse que la France est à même de contribuer au renseignement.

En conclusion, le spectre radioélectrique est bien une source de renseignements et il convient de s'intéresser à la totalité du spectre radioélectrique, ce que peu de pays sont capables de faire à ce jour. La France comme les Etats-Unis en est capable.

L'auditoire : première rangée, de g. à dr., Pierre Grandclément (Atos Bull) Robin Marijon (Thales), Gérard Labaune (Thales), le général Dran (DRM) et Philippe Guillaume (Guerrelec)

Le spectre radioélectrique : une arme redoutable

par Gérard Labaune, Directeur des Activités Durcissement, Instrumentation et Sûreté chez Thales Communications, épaulé par Robin Marijon, auteur d'une thèse sur le durcissement électromagnétique face aux micro-ondes de forte puissance.

De g. à dr., le général Dran (DRM) au micro, Joelle Toledano (ANFR), Philippe Guillaume (Guerrelec), Gérard Labaune et Robin Marijon (Thales)

Les armes à énergie dirigée sont des armes qui frappent sans action matérielle. Evidemment, c'est la porte ouverte à tous les fantasmes, aussi bien pour les soldats que pour les ingénieurs, avec pour résultat des projets aussi grandioses que l'IDS de Ronald Reagan. Mais, depuis le 11 septembre 2001, la menace a changé et la question qui se pose est de savoir si les armes à énergie dirigée peuvent aussi apporter des réponses face à ces nouvelles menaces diffuses, nombreuses et évolutives.

Du point de vue technologique, il existe trois moyens pour faire des armes à énergie dirigée : les faisceaux de particules, les micro-ondes et les lasers. Seules les deux dernières technologies sont opérationnelles aujourd'hui.

La technologie micro-ondes a évolué en termes de miniaturisation au niveau des tubes et plus récemment avec l'explosion des architectures de type état solide, lié à l'emploi du nitrure de gallium. Deux points limitent l'efficacité des armes à micro-ondes :

- l'incapacité à focaliser l'énergie dans l'espace ce qui pénalise l'efficacité à grande distance ;
- la moindre vulnérabilité des cibles car les problèmes d'interférences et de susceptibilités ont conduit les concepteurs de circuits électroniques à durcir considérablement leurs composants.

Ces deux points font qu'aujourd'hui l'arme à micro-ondes semble plutôt dédiée pour des applications courtes portées (largement inférieures au kilomètre) et lorsqu'il convient de traiter une zone plutôt qu'une cible.

Deux exemples pour illustrer ces possibilités : l'arrêt d'un véhicule à distance et la neutralisation des mines.

La technologie laser a évolué de façon extraordinaire. Dans les années 1980, le laser ressemblait au tube micro-ondes. C'était un objet extrêmement fragile, volumineux, avec des rendements extrêmement faibles. Est apparue alors la diode laser et la capacité, grâce aux fibres optiques, d'utiliser plusieurs diodes laser en parallèle. Le laser est devenu un objet léger, extrêmement compact et avec des rendements de dix à quinze fois supérieurs à ce qui existait dans les années 1980. Cette technologie a séduit le monde civil, en particulier le monde des télécommunications principalement pour des applications de type câbles sous-marins. Des investissements considérables ont été faits afin de rendre les amplificateurs optiques de plus en plus puissants mais aussi de plus en plus fiables. Ce laser a ensuite été utilisé pour la découpe des matériaux et amélioré en conséquence. Du point de vue militaire, l'arme laser permet de réaliser des opérations d'aveuglement ou de destruction de matériels dans des gammes de distances allant de 100 mètres à 10 kilomètres.

Après de nombreux fantasmes et de nombreuses promesses non tenues, il apparaît aujourd'hui de vraies solutions opérationnelles utilisant soit l'arme laser soit l'arme micro-ondes.

Table Ronde N°2 : Les outils et technologies actuels et en préparation

Modérateur : Jean-Michel RIVIERE, directeur scientifique et du développement, de la société Ineo Defense

Philippe Duluc (Atos Bull), Jean-Marie Rivière (Ineo Défense)

Jean-Marie Rivière (Ineo Défense)

Comment rester maître de l'Éther et du cyberespace ?

Après la maîtrise du spectre, il était important de mettre l'accent sur la connaissance des technologies actuelles et en préparation. La deuxième Table Ronde organise sa réflexion sur des échanges autour de trois thèmes : les programmes d'études amont en Guerre Electronique et en Cyber, les tendances du Chiffre et les avancées technologiques, tout en faisant un état des lieux de l'existant, des perspectives et de la préparation de l'avenir. Ces échanges sont menés par des hauts responsables de l'administration et de grands groupes industriels de Défense et de Sécurité.

Les programmes d'études amont GE et cyber

par l'ICA Eric Bouchardy, directeur adjoint du Service Recherches Technologiques et Technologies de Défense et de Sécurité (SRTS) de la DGA.

L'ensemble des recherches et études du ministère de la Défense servent à préparer la satisfaction des besoins militaires prévisibles. Il sert aussi à constituer, entretenir et développer une base technologique de défense et une expertise technique étatique nécessaire à la réalisation des opérations d'armement et de sécurité. La R&T est un équilibre entre trois objectifs :

- définir puis porter à maturité les technologies indispensables au développement des futurs systèmes dont a besoin le ministère de la Défense et, particulièrement, ceux pour lesquels une autonomie nationale totale, partielle est requise ; ce n'est pas de porter à maturité toutes les technologies mais celle pour laquelle une autonomie française ou européenne est nécessaire ;
- maintenir au juste niveau les compétences industrielles nationales afin de disposer à terme de la capacité de réaliser les programmes futurs,

soit dans un cadre français, soit dans un cadre de coopération ;
- favoriser l'innovation dans les domaines intéressants de la défense et soutenir les PME et PMI.

Pour ce faire, le ministère de la Défense a mis en œuvre, dans le cadre de la LPM en cours, une nouvelle gouvernance globale de la recherche et de technologie dont les principes majeurs de cette nouvelle gouvernance sont d'abord une orientation plus lisible et de niveau politique sur la durée de la LPM.

Un effort financier a été décidé avec un passage, globalement sur la période de la LPM, à 30 millions d'Euros par an de crédits études amont en Cyber sécurité qui seront adressés à la protection de l'information, aux composants de sécurité, aux moyens de lutte informatique et à la résilience des systèmes de défense, (systèmes d'armes et systèmes industriels).


Philippe Duluc (Atos Bull), Cédric Demeure (Thales), Robin Marijon (Thales)

Dans le domaine du renseignement, il s'agit de préparer les futurs programmes de renseignement électromagnétique et image, à la fois sur les composantes spatiales et aéroportées ainsi que sur le traitement de l'information. Les principales études lancées portent à la fois sur les capteurs pour combler le déficit industriello-capacitaire qui avait été constaté ces dernières années, mais aussi sur des travaux d'optimisation des moyens de surveillance, en terme de technologie, de traitement radar et d'exploitation. Les quantités de données fournies par les futurs capteurs, que ce soit MUSIS ou CERES, seront d'un ordre de grandeur bien supérieur aux moyens précédents. Donc énormément de travaux et d'études amont consacrés à l'exploitation, à l'automatisation des traitements, que ce soit dans le traitement de la parole, de l'écrit, de l'image, de l'indexation ou de l'archivage.

D'autres thèmes sont pris en compte : l'aéronautique de combat, le combat naval, les systèmes terrestres, les hélicoptères et les avions de transport, mais aussi des domaines plus transverses comme les travaux sur l'humain et le NRBC ou encore les communications de réseaux, les systèmes d'information…

Dans la LPM, un effort particulier a été consacré à la recherche et au développement de défense avec 730 millions d'euros par an pour la période.

Les tendances du chiffre

par Philippe Duluc, directeur de la division Sécurité de la société Atos Bull.

L'exposé est articulé en trois thèmes : l'évolution du Chiffre et de la Cryptologie, les grands enjeux d'aujourd'hui dans nos différents systèmes, nos systèmes d'armes… .

Depuis l'Antiquité, nous avons la preuve que des systèmes ont été mis en place et utilisés pour chiffrer des informations et les dissimuler aux yeux des adversaires tout en donnant l'information aux amis. Quelques exemples : la « scytale » (chez les Spartiates, également connue sous le nom de bâton de Plutarque, elle était un bâton de bois utilisé pour lire ou écrire une dépêche chiffrée). Elle est considérée comme le plus ancien dispositif de cryptographie militaire connue. En fait, c'est une transposition manuelle un peu compliquée mais les outils étaient simples : c'était le papier et le crayon associé à des moyens divers et variés, plus ou moins organisés, comme des tableaux de Blaise de Vigenère, (système de chiffrement polyalphabétique, c'est un chiffrement par substitution, mais une même lettre du message clair peut, suivant sa position dans celui-ci, être remplacée par des lettres différentes, contrairement à un système de chiffrement monoalphabétique comme le chiffre de César).

Les armes du décrypteur des cryptologies manuelles étaient la même chose : le crayon, le papier mais avec une gomme en plus. En prenant, un peu de recul, tous ces systèmes de cryptologie manuelle, en service jusqu'à ces derniers temps, étaient finalement décryptables, par nature.

Ensuite, on a eu une évolution technologique en entrant dans le monde des machines électromécaniques. C'était des machines à tambours, à rotors, la plus célèbre d'entre elles étant la machine *Enigma*. Et encore une fois, en prenant du recul, comme ces éléments simulaient de la crypto manuelle, cela finissait par être décrypté. On connaît les succès des cryptologues polonais, français, britanniques et ensuite américains sur *Enigma*.

Après, il y a eu des évolutions très rapides qui allaient de pair avec l'évolution de l'informatique et des réseaux pour s'acheminer directement vers la cryptographie moderne, et cela date de plus de trente ans. La cryptographie moderne, ce sont des machines à chiffre électroniques et, très rapidement, des algorithmes de chiffrement sont devenus mathématiquement prouvés et mathématiquement très forts. Là, nous arrivons à un moment où, contrairement au passé qui a duré des siècles, les systèmes sont indécryptables, ce qui augmente les difficultés des services de renseignement car il n'est plus possible de rentrer dans le contenu des communications cryptées. Cependant,

les données techniques (comme la signalisation, la localisation, « qui appelle qui », dans quel domaine, etc…) permettent de générer des informations de renseignement.

La vulnérabilité des systèmes est donc aujourd'hui sur leurs implémentations, sur la gestion des clés, sur les usages et donc sur les personnes. Ainsi, au-delà des algorithmes sophistiqués, il existe toujours des moyens d'obtenir de l'information en exploitant les failles humaines. Aujourd'hui, la menace consiste à piéger, à pénétrer, à voler des clés…, comme illustré par Monsieur Snowden ou d'autres.

Un des exemples les plus courants, en termes de chiffrement, qui doit être bien présent dans l'esprit, c'est la révolution qui a permis le commerce électronique. C'est la cryptologie asymétrique (l'algorithme a été décrit en 1977 par Ronald Rivest, Adi Shamir et Leonard Adleman. RSA a été breveté par le Massachusetts Institute of Technology en 1983 aux États-Unis). Ceci permet aujourd'hui à des utilisateurs d'Internet qui ne se connaissent pas de sécuriser un échange, de s'authentifier et d'échanger des informations confidentielles.

Les systèmes sont devenus extrêmement complexes, poussés par le besoin de réduire les prix tout en augmentant le nombre de fonctionnalités offertes à l'utilisateur. Cela amène à une utilisation accrue de technologies duales, conduisant à favoriser les attaques et à faciliter la pénétration des malwares. Plus besoin de cryptanalyse : il suffit de voler la clé et déchiffrer le contenu. Et donc, aujourd'hui, tout le jeu des services, des industriels et des militaires est de fiabiliser leurs implémentations et leurs procédures.

En matière de chiffre et de technologie, pour le futur, on parle de lead-data, de cloud computing, de M to M (Machine to Machine), des nanotechnologies… Cette augmentation de la complexité des systèmes va aboutir à une perte de confiance dans la sécurité des données. C'est ce que l'on appelle le Zero Trust Information System qui considère que le système d'information, quel qu'il soit, est perméable et non de confiance. La seule façon de garder la confidentialité des données est de permettre aux utilisateurs de maîtriser leurs clés et leur chiffre pour un chiffrement de bout en bout.

Les tendances technologiques

par Cédric Demeure, directeur de Thales Research & Technology.

Les nouvelles tendances technologiques sont illustrées par des exemples, en termes de micro-informatique et de nanotechnologies, avec des applications dans les domaines de la Guerre Electronique et des Télécommunications. Une première tendance est l'électronique refroidie. En refroidissant à des températures cryogéniques, on peut obtenir des effets de supraconductivité permettant d'obtenir des caractéristiques très intéressantes en termes de performances. Ceci pourra être obtenu à court terme car maintenant sont disponibles des machines à froid de volume réduit pouvant tenir dans une main. En refroidissant l'électronique, nous pouvons obtenir des pertes et des facteurs de bruit très faibles ce qui permet de réaliser par exemple des filtres réjecteurs très efficaces, pour de l'antibrouillage, pour des analyseurs spectraux ou pour faire des capteurs très larges bandes en télécom. Cela permet, par exemple, de recevoir la totalité du signal qui arrive d'un satellite dans un seul capteur.

Une grande tendance est l'utilisation de l'optique et des lasers qui ont révolutionné les usages. Il est possible de faire énormément de choses avec les lasers, car les fréquences sont beaucoup plus élevées que les signaux radiofréquence que l'on traite. Ainsi, une bande de 20 GHz qui est énorme dans le domaine RF est une bande étroite dans le domaine optique. Par exemple, des traitements de conversion de fréquence, de filtrage, d'analyse spectrale, d'échantillonnage peuvent être réalisés en optique, dans un volume très réduit.

Une autre grande tendance et de réaliser des algorithmes très compliqués en numérique et, pour cela, il faut numériser. Une alternative à la numérisation classique est d'utiliser des lasers pour une monographie spectrale ce qui est maintenant possible avec des dynamiques assez intéressantes. Ceci permet d'observer toute la bande RF d'un seul coup, offrant la certitude de prendre à 100 % des signaux présents. En termes d'oscillateurs, il est possible de combiner de manière réglable deux lasers fonctionnant à deux fréquences différentes de manière à générer une fréquence intermédiaire variable, permettant ainsi d'obtenir un oscillateur réglable dans toute la bande de fréquence comprise entre 0 et 100 GHz, et ce, avec une grande pureté spectrale. Un autre exemple : un dispositif que nous dénommons « Spectral Hoyle Burning ». C'est un cristal que l'on vient attaquer avec le laser dont la fréquence change, ce qui permet de donner des propriétés de filtrage qui sont directement liées à la fréquence du laser. L'idée est de réaliser un analyseur de spectre avec des performances assez sympathiques comme illustré par cet exemple de réalisation : 22 GHz de bande d'interception avec 400 canaux, et ce, avec l'intérêt d'être à 100% de probabilité d'interception. Un autre exemple donné est un dispositif de filtrage qui permet, dans une application satellite, d'avoir un filtre de très bonne sélectivité avec un facteur de bruit vraiment très faible, ce qui pour le satellite est critique (un gain de 0,1dB de sensibilité dans les télécoms

satellites est très notable). De la même façon, cette technique peut être utilisée pour un récepteur de Guerre Electronique.

Mais il faut toujours une antenne : à des fréquences RF basses, les antennes sont grandes et donc il reste des travaux pour essayer de faire en sorte que ces antennes soient de taille plus réduite. Ces antennes miniatures à large bande, sont basées sur la technologie des « SQUID » (Superconducting QUantum Interference Device). L'idée est d'utiliser une toute petite boucle comportant une jonction Jefferson, l'ensemble étant à une température cryogénique de supraconduction. Le flux magnétique de l'onde RF induit un courant dans la boucle détecté par la jonction. On réalise ainsi une antenne d'une dizaine de microns carrés. Il est possible d'en intégrer 300 000 sur une petite puce. C'est tout petit mais, en revanche, nous avons un capteur d'une sensibilité somptueuse. Vous avez ici, sur un dispositif vraiment minuscule, la possibilité d'avoir une antenne qui puisse être vraiment très intéressante.

Voilà juste quelques exemples pour vous faire rêver.

Table Ronde N°3 : Politiques industrielles face à ces menaces

Modérateur : Jean-François SULZER, responsable des Projets Amont, société Thales Communications & Sécurité

Poursuivant le fil conducteur de la journée, l'Ether et les luttes pour son contrôle, la troisième table ronde s'est penchée avec les points de vue de l'administration, d'une PME et d'un grand groupe, sur les stratégies pour en optimiser l'usage alors que ses ressources sont de plus en plus convoitées et que le risque Cyber s'ajoute aux menaces traditionnelles et pour fournir aux acteurs français civils comme militaires les atouts nécessaires pour tenir leur rang.

Sur des sujets duaux comme celui des télécoms pour les forces de sécurité qui est au coeur de nos discussions, des dispositions se mettent en place. C'est en particulier le cas avec la filière des industries de sécurité (COFIS), installée par le premier ministre fin 2013 et qui a vocation à traiter des applications civiles mais intervenant dans la sécurité de l'état ou des opérateurs.

Jean-François Sulzer (Thales), Yvon Livran (Thales), Jacques Turbert (DGA), Charles d'Aumale (Ercom)

Une plus grande coopération entre acteurs civils et militaires

par Jacques Turbert, responsable des métiers Télécommunications à la direction technique de la DGA.

Dans le domaine de l'utilisation du spectre, la Défense se doit d'être exemplaire et de façon très symbolique transporter un maximum de bits par Hertz alloué. Il faut ensuite être astucieux dans la mise en oeuvre sur le terrain, de façon à éviter les interférences entre cellules voisines ou bien cibler les pinceaux de couverture dans les communications par satellites. A l'inverse, la protection contre les menaces de Guerre Electronique induisent une surconsommation de spectre qu'il faut minimiser, mais aussi savoir justifier.

Pour aller plus loin, l'allocation entre les différents utilisateurs doit se faire de façon dynamique (en d'autres termes ne jamais laisser inutilisées des bandes de fréquence disponibles). Cette approche est parfaitement illustrée par le concept de « radio cognitive » que développe Thales dans un contexte de coopération européenne. De façon tout aussi pragmatique peuvent être mises en place des utilisations temporaires mixtes. Typiquement des licences secondaires peuvent être accordées à des opérateurs civils sur des bandes militaires indispensables mais peu utilisées dans le temps, comme celles de la télémesure pour certains essais.

Reste que pour être efficace, politique publique, négociations internationales et développements industriels doivent être synchronisés. Dans ce domaine, l'Europe, encore dans le flou, part avec un sérieux handicap face aux Etats-Unis qui viennent d'allouer deux fois 10 MHz réservés à la sécurité publique large bande dans la bande des 700 MHz, configuration offrant un parfait compromis entre portée et encombrement des antennes. C'est le challenge qu'il nous reste à relever.

Charles d'Aumale (Ercom) durant sa conférence

Une réflexion d'ensemble combinant Guerre Electronique et cyberdéfense au profit des acteurs civils et militaires

par Charles d'Aumale, directeur commercial de la société ERCOM.

L'actualité récente montre l'extrême dynamisme du secteur des mobiles, en particulier de la data mobile et des attaques dans le domaine. Pour combler la soif de bande passante, les états continuent à vendre des licences à des prix impressionnants. Les Etats-Unis ont ainsi récolté plus de 40 $ milliards début 2015 pour 65 MHz de largeur de bande pour des usages 4G. Leur prix de réserve était de 10 $ milliards pour couvrir les frais du réseau FirstNet (réseau ad hoc 4G pour la sécurité civile) et pour dédommager les armées et autres utilisateurs fédéraux. Parallèlement, l'ARCEP a initié le processus de mise en vente de licences autour de 700MHz.

Cette frénésie de bande passante vient de la très forte croissance des abonnements de Smartphones. On estime qu'il y aura plus de 3 milliards d'abonnés data mobiles en 2015. Principalement grand public, ces appareils sont de plus en plus connectés aux systèmes d'informations des entreprises. On considère ainsi qu'environ la moitié des employés dans le monde utilisent des applications grand public pour partager des documents. Autant dire que les directions informatiques ont perdu le contrôle. Les mobiles sont donc devenus une source très importante d'information, d'où des attaques à tous les niveaux. Cela peut se faire en volant le terminal, en l'attaquant sur différents ports, en y insérant à distance ou au contact des logiciels malveillants, en interceptant les communications, en attaquant les points d'accès distants des organisations. Les exemples sont nombreux dont un qui a fait date début 2014 sur une conversation entre deux diplomates américains sur l'Ukraine. L'enregistrement a été diffusé sur YouTube où l'on y entend quelques mots doux sur l'Union Européenne…

Face à cela, de nombreux acteurs se sont positionnés. Certains sur des marchés de masse de type Mobile Device Management et d'autres sur des solutions de téléphone mobile hautement sécurisée. Les industriels français sont présents sur ce créneau avec des acteurs comme Thales, Atos Bull, Ercom, Pradeo, etc. Parallèlement, l'Etat s'est mis en ordre de marche pour renforcer les compétences et dispositifs en cybersécurité. Deux grands plans d'actions sont en cours de déploiement. Le premier sous la responsabilité du Ministère de la Défense, avec le Pacte Cyberdéfense. Le deuxième sous le leadership de l'ANSSI dans le cadre du programme gouvernemental sur la nouvelle France industrielle. Dans les deux plans, il y a très clairement une implication du tissu industriel français, aussi bien grands groupes que PME. Au niveau des PME, des initiatives de coopération sont enclenchées par exemple à travers Hexatrust qui regroupe une vingtaine d'éditeurs français en cybersécurité.

La dynamique insufflée pour les pouvoirs publics et par les entreprises, utilisateurs ou industriels, montre la prise de conscience de la nation en matière de cybersécurité. Les cadres sont désormais fixés. Il s'agit désormais de dérouler en continuant les actions initiées et en les renforçant.

Une démarche industrielle globale et novatrice porteuse d'une ambition pour la France

par Yvon Livran, responsable de la réglementation du Spectre Electromagnétique chez Thales, président de la commission Fréquences du GIFAS.

L'explosion des besoins liés aux applications civiles est une évidence, mais les besoins ne cessent de croître également dans le domaine militaire, se focalisant naturellement sur les fréquences réellement utilisables. S'y ajoutent de nouvelles utilisations, comme les robots ou les drones.

Il s'en suit un besoin évident de partage du spectre et, pour le faire efficacement, de bien en contrôler l'usage. Le partage de la bande 800 MHz il y a quelques années et celui qui doit intervenir en 2015 pour la bande 700 MHz montrent bien les limites de ce processus. Depuis 30 ans les méthodes dynamiques se sont développées avec pour objectif, en un lieu et à un instant donné, d'utiliser toutes les bandes libres. L'exemple typique de cette optimisation est l'autorisation conditionnelle donnée à du WIFI d'émettre en l'absence de signal radar opérant dans la même bande. Le risque devient alors de voir les situations s'inverser, l'utilisateur secondaire devenant dans les faits prioritaire… Le partage des bandes entre utilisateurs s'avère néanmoins possible et on le voit bien pour les applications civiles de sécurité.

Ce partage induit toutefois une nouvelle vulnérabilité : si une application est visée par un brouillage, toutes les applications utilisant la même bande seront touchées, sans oublier que tout partage implique de faire respecter les engagements de toutes les parties.

En guise de conclusion, pour renforcer l'émergence de nouveaux services, la France doit s'engager résolument vers le partage électronique de fréquences et, à cette fin, développer des compétences en matière de contrôle du spectre dans un paysage où la gestion du spectre va devenir dynamique. Et pour reprendre un proverbe d'un philosophe intergalactique, Monsieur Spot : « Plus on partage, plus on possède », voilà le miracle !

Discours de clôture

par Madame Patricia Adam

Pierre Grandclément, Patricia Adam (Présidente de la Commission de la Défense Nationale et des forces armées)

Les enjeux de la maîtrise de l'Ether ont plusieurs aspects :

volet budgétaire, dimension politique et deux domaines, Guerre Electronique et renseignement.

D'abord la Guerre Electronique, qu'elle soit défensive ou offensive, est une arme de supériorité, puisqu'elle permet de priver l'adversaire de l'usage du spectre électromagnétique. Elle permet d'observer dans un environnement très encombré aujourd'hui, ce qui est invisible, mais en cas d'agression, elle permet aussi de détecter et de contrer sans délai une menace. Sur son aspect défensif, la Guerre Electronique assure à nos armées et à nos services de sécurité en général leur supériorité.

La recherche et l'exploitation du renseignement devenant une priorité dans les développements récents de la lutte antiterroriste, les moyens dévolus à la Guerre Electronique constituent désormais des priorités dans la loi de programmation militaire.

Néanmoins, les techniques de Guerre Electronique devenant aussi potentiellement autant de risques pour les libertés publiques, le législateur doit intervenir dans des délais de plus en plus courts pour trouver l'équilibre entre sécurité et liberté.

L'Éther et le cyberespace sont devenus des espaces conflictuels. Ils sont devenus des champs de bataille qu'il est impératif de maîtriser, au même titre que les espaces terrestres, maritimes ou aérospatiaux. Il ne s'agit pas de perdre la supériorité là où se gagne la décision ultime. De même que le contrôle de la mer ou de l'espace aérien suppose la maîtrise des ports et des aéroports, le contrôle de l'Éther ou du cyberespace implique la protection des réseaux, de leurs interfaces informatiques, récepteurs, terminaux et autres moyens impliqués dans les échanges de données au sens large.

Nous célébrons cette année les 50 ans de la dissuasion nucléaire. La Guerre Electronique concourt à la crédibilité de la dissuasion, notamment en assurant la capacité de pénétration. Les besoins générés par la dissuasion ont entraîné le développement de technologies militaires nouvelles au profit des forces conventionnelles. La France a pu ainsi acquérir toute seule une panoplie de moyens de Guerre Electronique aujourd'hui reconnus dans le monde entier en se dotant progressivement d'une filière industrielle, dominée par un champion de rang mondial, et d'un tissu de PME de très haute technologie extrêmement performantes, le tout sous la surveillance de la DGA.

Le 3ème Forum de l'Innovation organisé par la DGA vient d'avoir lieu. Les domaines de l'électronique, de l'électromagnétisme, de l'optronique, des systèmes d'information, de la cybersécurité et des matériaux sont autant de thèmes d'intérêt pour la DGA qui pour la conception d'équipements de Guerre Electronique. La préparation de l'avenir est une mission essentielle de la DGA. Comme il y a cinquante ans, le besoin militaire tire la technologie au profit d'applications duales dans un domaine de souveraineté pour lequel les coopérations, même avec nos meilleurs partenaires européens, sont difficiles à mettre en oeuvre.

La DGA a un rôle extrêmement important à jouer pour développer et entretenir la base industrielle et technologique nécessaire à la préservation de notre capacité de Guerre Electronique. Il est nécessaire de financer des programmes d'étude amont pour accompagner la croissance d'une filière toujours fragile. Le ministre de la défense est attentif à préserver ces crédits, qu'il s'agisse de PEA ou des dispositifs Astrid et Rapid[1] qui commencent à orienter véritablement l'innovation de défense dans les PME, avec des expériences particulièrement riches et prometteuses. Les USA ne partagent pas leurs technologies dans ce domaine depuis son apparition. Leur constance dans le financement de son développement mérite d'être notée.

S'agissant du renseignement stratégique, la France est actuellement le seul pays européen à développer une capacité de recueil du renseignement d'origine électromagnétique complète, en particulier intégrant une composante spatiale. Le programme CERES est bien engagé avec une livraison de trois satellites en 2020, En l'occurrence, cela concourt à la crédibilité de la dissuasion, mais aussi de nos engagements conventionnels.

La vulnérabilité des réseaux de communications civils face à la menace terroriste doit aussi être mentionnée. Ce risque, bien qu'identifié par les Opérateurs d'Importance Vitale, n'est pas encore suffisamment pris en compte.

Il faut enfin souligner les difficultés qui s'opposent à une coopération européenne dans des domaines aussi sensibles et aussi stratégiques. La Guerre Electronique est indubitablement un domaine de souveraineté dont on peut éventuellement partager les résultats - mais pas la technologie. En revanche, la coopération entre forces armées, que ce soit en interarmées ou en interalliés, est une réalité dont l'Association Guerrelec elle-même porte témoignage et que je voudrais ici remercier au nom de la représentation nationale.

Les échecs ayant conduit aux évènements du 11 septembre montrent que la technique, si elle est indispensable, n'est pas suffisante. La Guerre Electronique, c'est aussi une affaire d'Hommes, car l'intelligence humaine tend le plus souvent à se jouer de la technique.

1 Astrid et Rapid : programmes d'études amont DGA

Hommage à Monsieur Jean Turck, 103 ans, pionnier de la Guerre Electronique française

Guerrelec a souhaité rendre hommage à Jean Turck, pionnier de la Guerre Electronique, né en 1911.

Pierre Grandclément, notre Président, l'a reçu lors du Colloque du 26 novembre 2014 célébrant les 50 ans des Old Crows.

Il a rappelé les 100 ans de la Guerre Electronique et le fait que Jean Turck a été pendant son service militaire en 1931, radio-opérateur militaire à la Tour Eiffel, avant d'être recruté par l'ingénieur de l'aéronautique Maurice Hurel. Il a participé aux premières inventions de la radiocommande (télécommande en modulation de fréquence) pour guider les bombes Hurel-Turck, et les drones. C'était déjà, à l'époque, une lutte stratégique…

Pierre Grandclément, Patricia Adam, Jean Turck (pionnier de la GE)

Pendant la Seconde Guerre mondiale, sa société qui était dans la zone occupée, déménage dans le sud de la France, en zone libre. Puis, en 1943, pour éviter de travailler pour les forces nazies, Jean Turck rejoint Alger où il invente un système de brouillage des bombes volantes allemandes qui réduira à néant leur efficacité. Jean Turck précise : « Ce sont des bombes qui ont été volées, construites sur des brevets qui ont été fournis par Vichy ».

Dans les années 1950, il développe sur crédits militaires, dans son laboratoire privé, des instruments infrarouges de télémesure et de détection. Il est à l'origine des engins antichars, comme les SS-11.

La télécommande des missiles « Milan » est un de ses enfants. Il en réalise des centaines, malgré une insuffisance de personnel. Alors, il s'associe à une société française bien connue, la SAT (Société Anonyme de Télécommunications). Rapidement, une équipe de 2 000 personnes se met en place pour développer des matériels infrarouges et des télémesures…

Ces produits ont été industrialisés pour en faire une véritable industrie. En 1970, dans le cadre d'une politique industrielle bien comprise du ministère des armées, les laboratoires Turck sont rachetés par la SAT devenue SAGEM et SAFRAN et où Jean Turck reste conseiller scientifique au conseil d'administration.

Pierre Grandclément, en présence de Madame Patricia Adam, députée et présidente de la Commission de la Défense nationale à l'Assemblée nationale, a remercié Jean Turck de sa présence, l'a cité comme exemple pour les jeunes générations d'ingénieurs et l'a fait membre d'honneur de l'association Guerrelec.

Jean Turck

Jean TURCK, né en 1911

- 1931 : Service militaire à la tour Eiffel comme radio opérateur
- 1933 : Création d'une station radiologique
- 1938 : Invention de radiocommande pour bombe sans pilote
- 1943 : Traversée de la Méditerranée
- 1943 : Brouillage des bombes volantes allemandes Henschel
- 1946 : Commutateur d'appareil photo pour avion de reconnaissance
- 1946 : Développement de télémesures diverses
- 1946 : Télécommande d'engins (Milan, Hot, etc..)
- 1950 : Autodirecteur Matra 530
- 1955 : Faisceaux infrarouges à 10 microns laser
- 1956 : Développement de capteurs d'infrarouge
- 1970 : Cession des laboratoires Turck à la SAT

par Pierre-Alain Antoine

LA FRANCE ESPIONNE LE MONDE (1914-1919), LES EXPLOITS DES BRISEURS DE CODES

Auteur : Jean-Claude Delhez
Editeur : Economica
ISBN : 978-2-7178-6694-0
Pages : 29
Prix : 29 Euros

Les briseurs de codes français étaient bien les meilleurs pendant la Première Guerre mondiale, et ce, dès 1914. Les écoutes françaises, regroupant les ministères de la Guerre, de l'Intérieur et des Affaires étrangères, en accord avec la ROOM 40 de la Royal Navy à Londres, ont déjoué les codes allemands, autrichiens ainsi qu'espagnols, pays neutres mais aussi, « just to be sure », des autres belligérants, y compris ceux qui combattaient de notre côté.

L'auteur, après avoir dépouillé des milliers de documents d'archives dont certains n'avaient jamais été ouverts, nous prouve notre savoir-faire en la matière bien avant Bletchley Park lors du deuxième conflit mondial.

Un livre qui a de droit sa place sur la table de chevet de tous les membres de notre Association.

MÉMOIRE DU CHEF DES SERVICES SECRETS DE LA GRANDE GUERRE

Auteur : Charles Dupont, présenté et annoté par Olivier Lahaie
Editeur : Histoires et collections
ISBN : 978-2-35250-358-3
Pages : 295
Prix : 22 Euros

Polytechnicien, artilleur, Charles Dupont, natif de Nancy, est affecté au service de renseignement après l'affaire Dreyfus. Il accomplit plusieurs missions en Allemagne avant de prendre la tête du 2ème bureau (renseignements) de l'état-major général en août 1913 et la tête du 2ème bureau du Grand quartier général en août 1914.Il sera maintenu dans ses fonctions jusqu'en 1917. Il prend la tête de la mission militaire à Varsovie en 1922. Visionnaire, le général Dupont dénonce dans ses mémoires écrites en 1926, la montée des périls en Allemagne, prévoyant l'Anschluss et même la crise de Dantzig qui débouchera sur la Seconde Guerre mondiale.

Ce document, inédit à ce jour, constitue un témoignage exceptionnel sur le renseignement français avant et pendant la Grande Guerre, mais aussi sur la personnalité des grands chefs militaires : Joffre, Nivelle, Pétain et leurs relations avec les milieux politiques de l'époque.

A lire absolument.

COLD WAR WARRIORS, WARPLANES ON THE BRINK OF GLOBAL CONFLICT

Auteurs : Different writers
Editeur : FlyPast, a Key Publishing publication
ISBN : 978-1-910-415078-14
Pages : 98 pages format hebdomadaire
Prix : £ 5,99

Key Publishing est un éditeur britannique spécialisé en aéronautique. Il publie des numéros spéciaux sur des sujets tels que les B-52 ou les C-135 ou les moyens ELINT britanniques pendant la Guerre Froide. Cette fois-ci, ce numéro spécial traite d'avions tels que le F-100 « Super-Sabre » ou le BAC Lightning mais aussi du MiG-25 « Foxbat », du U-2 ou des avions de brouillage électronique tels les EB-66 « Destroyer », stationnés sur la base de Toul-Rosières avant de « sévir » au-dessus du ciel vietnamien depuis la base de Takhli en Thaïlande.

C'est ce type de revues qui enrichit la connaissance des personnes écrivant sur la Guerre Electronique…

LE BÂTON DE PLUTARQUE

Auteur : **Yves Sente, scénariste, André Juillard, dessinateur**
Editeur : Blake et Mortimer
ISBN : 978-2-8709-7193-2
Pages : 64
Prix : 15,95 Euros

Une fois n'est pas coutume, voici une BD. Pour la première fois à ma connaissance, des héros de BD connus, évoquent la Guerre Electronique et cela mérite d'être dit. Dans cet ouvrage où les héros sont les célèbres Blake et Mortimer, cet épisode se situe avant le début de leurs aventures.

Nos héros nous parlent de la machine Enigma, de Bletchley Park (tellement bien dessiné que j'ai eu la confirmation du dessinateur qu'il avait effectivement visité l'endroit), du PC enterré ou « War Cabinet » de Sir Winston Churchill où l'on découvre les WAAF et les WRENS, femmes auxiliaires de la RAF et de la Navy, mais aussi l'ambiance qui y régnait.

Les auteurs citent le « Carré de Polybe » et la « Scytale » ou Bâton de Plutarque, tous deux de vieux systèmes de cryptologie dans un scénario que les auteurs devraient venir nous commenter lors d'une prochaine conférence de notre Association.

Un épisode de relaxation dans le domaine de la Guerre Electronique.

IN MEMORIAM

Nous avons appris avec tristesse la disparition le 23 avril 2015 du colonel (ER) **Alain STERCZYNSKI**, expert de la Guerre Electronique, à l'âge de 67 ans. Il était un adhérent Guerrelec de la première heure.

Il a été successivement officier mécanicien, spécialiste du ROEM, de 1976 à 2000 à Furth im Wald (Allemagne) et il fut un pilier de la GE Armée de l'air au BGE FATAC, EMAA Trans-GE, EMAA/BSA-AV-GE, chef du Bureau ROEM de la sous-direction technique de la DRM, puis chez Ineo Defense ELG.

Il avait notamment écrit sur le Renseignement d'Origine Electromagnétique dans le livre *Les Avions de Renseignement Electronique, 50 ans d'activités secrètes racontées par les acteurs*, publié par l'Association Guerrelec aux Editions Lavauzelle, 2009.

Association Guerrelec AOC French La Fayette Chapter. Directeur de la publication : Pierre Grandclément, Rédacteur en chef : Pierre-Alain Antoine.

Réalisation et impression : GT PRINT : 01 34 52 18 88 IMPRIM'VERT

Ont collaboré à cette édition : Pierre-Alain Antoine, Patrick Demoulin, Pierre Grandclément, Philippe Guillaume, Jean-François Sulzer et Jean-Pierre Vadet.