N°48
Décembre 2013

Lettre d'information de
Guerrelec

Si vis pacem para bellum... electronicum

Le mot du Président

Chers amis,

A l'occasion de ce dernier numéro 2013 de la Lettre de Guerrelec, j'ai le plaisir de vous annoncer que notre Conseil d'Administration a décidé d'honorer à sa manière le cinquantième anniversaire de la création de l'Association des « Old Crows » en organisant un grand Symposium sur la Guerre Electronique et la Sécurité globale. Cette manifestation aura lieu le 27 novembre prochain au Mont Valérien, siège du Musée des Transmissions (matériels depuis les émetteurs à étincelles du général Gustave Ferrié, en passant par les pigeons voyageurs, jusqu'au Smartphone d'aujourd'hui). Pensez à réserver cette date dès maintenant !

Cet évènement fera suite à une excursion printanière conviviale au Musée du Radar de Douvres-la-Délivrande en Normandie les 13 et 14 juin 2014 dans la logique du 70 ème anniversaire du Débarquement allié. Des sujets de conférences mettront en lumière l'apparition du radar dans la guerre, la naissance de la Guerre Electronique, la situation et la mise en œuvre des contre-mesures le jour du Débarquement ainsi que les leçons de la guerre et les tendances actuelles.

Au programme de cette Lettre, nous découvrons les avancées de l'autoprotection des avions d'armes vues par l'industriel. Puis un article d'actualité nous en dit plus sur la sécurité en profondeur des mobiles, c'est-à-dire la défense en profondeur des mobiles allant de l'identification de balises ennemies à la protection des Smartphones. Egalement quelques évènements comme les essais GE OTAN 2013 ainsi que les 20 ans de la Brigade RENS vous sont livrés en détails.

Enfin, nous serons au fait des dernières avancées du Salon Milipol et de la Convention AOC 2013 aux USA où nous étions représentés par l'un de nos administrateurs au travers d'une conférence.

Pour terminer les Notes de Lecture avec une sélection de livres autour de la Guerre Electronique et de la Guerre de l'Information vous sont offertes pour bien débuter l'année.

Joyeux Noël et Bonne Année 2014 à tous !

IGA Pierre **GRANDCLEMENT**
Président de Guerrelec

Avancées dans l'autoprotection des avions d'armes : détection des missiles et leurrage

Le monde de l'autoprotection des avions d'armes est en constante évolution pour tenir compte à la fois de l'apparition de nouvelles menaces mais aussi pour tirer parti des avancées technologiques. Deux exemples illustrent particulièrement bien ce phénomène : le DDM-NG (Détecteur De Missile de Nouvelle Génération) et le LEA (Leurre Électromagnétique Actif).

DDM-NG

La détection des missiles « silencieux », c'est-à-dire des missiles non-associés à une conduite de tir radar ou laser, est un besoin qui a été exprimé de longue date, puisqu'aucun dispositif au sein des systèmes de contre-mesures existants ne permettait de détecter ce type de menace, obligeant les avions à larguer de manière préventive des séquences de leurres infrarouges, avec tous les inconvénients que cela représente en termes de consommation de leurres et de non-discrétion.

La DGA a très tôt investi dans ce domaine, dès les années 1970, et plus particulièrement dans la technologie infrarouge avec le DDM développé par MBDA France en coopération avec Sagem. Elle s'est montrée dans ce sens

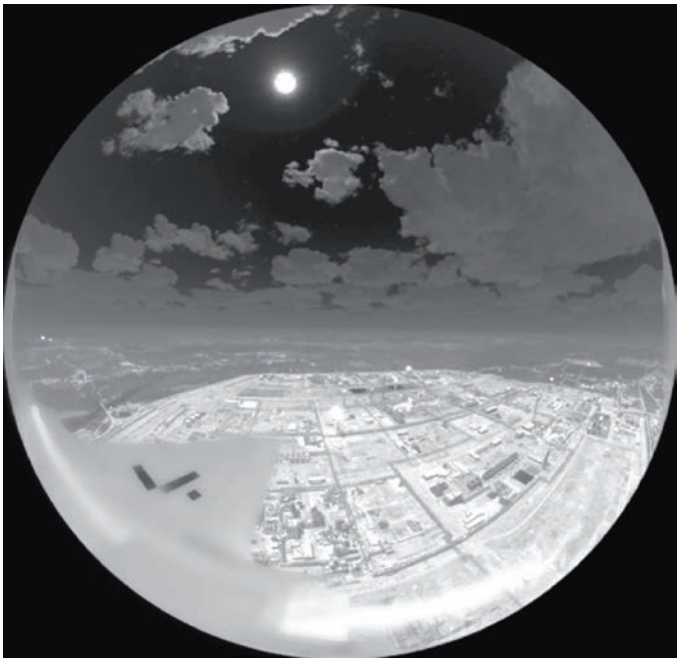
Senseur DDM-NG en haut de dérive Rafale (Photo MBDA)

visionnaire puisque l'on peut constater que les futurs avions d'armes US (F35 et F22) ont finalement rejoint ce choix après quelques hésitations, alors que les Mirage 2000 et Rafale sont déjà équipés de ce type de technologie.

Le DDM-NG, successeur du DDM et développé par MBDA France, profite des dernières avancées technologiques dans les domaines des matrices de détecteurs infrarouges au plan focal, des optiques IR grand champ, des calculateurs embarqués et des algorithmes de traitement, ce qui a permis d'obtenir une couverture de surveillance sphérique autour de l'avion porteur tout en améliorant les performances du DDM.

Le développement s'est déroulé dans un temps très court pour ce type d'équipement (mi 2007 - mi 2012), et il est désormais en cours de livraison pour les Rafale de la quatrième tranche

L'image infrarouge de grande qualité fournie par les senseurs du DDM-NG n'est aujourd'hui utilisée que pour la fonction détection des missiles, mais on peut imaginer qu'elle le sera demain pour d'autres fonctions, à l'instar de ce qui sera effectué sur le F35 (vision périphérique, situation tactique, etc…).



Cazaux vue d'un senseur DDM-NG
(Photo MBDA)

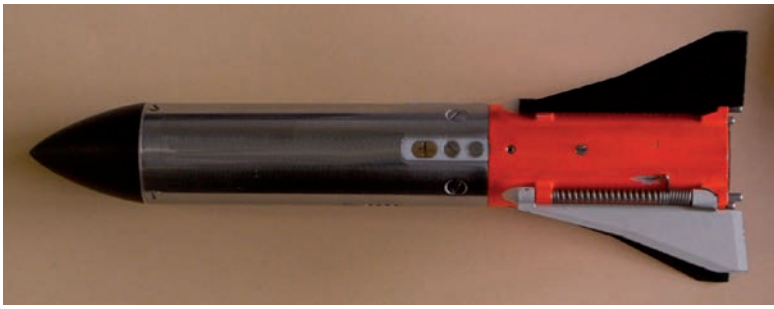
L'utilisation du DDM-NG sur d'autres porteurs est également envisagée (avions de transport, hélicoptères, véhicules…).

Prototype LEA Th-CSF
Matra-Défense années 90
(Photo MBDA)

LEURRE ELECTROMAGNETIQUE ACTIF

Les premières expérimentations de leurres électromagnétiques actifs (également appelés « brouilleurs largués ») ont eu lieu en France au milieu de la décennie 1990, dans le cadre de développements exploratoires conduits par Matra-Défense & Thomson-CSF d'une part et Dassault Électronique, d'autre part, sous l'égide de la DGA. Il s'agissait de doter les avions d'armes de la capacité de leurrer les menaces RF actives, voire semi-actives sophistiquées, en créant un brouillage angulaire.

Bien que les résultats de ces développements exploratoires aient été très concluants, ils n'ont malheureusement pas été suivis à l'époque par une industrialisation de produit.



Prototype LEA Th-CSF Matra-Défense années 90 (Photo MBDA)

Le PEA INCAS de la DGA, en cours d'exécution par MBDA France et Thales, reprend les concepts de l'époque, car le besoin opérationnel existe toujours, mais en profitant des dernières avancées technologiques, en particulier dans les domaines de la technologie DRFM et des composants MMIC.

Gageons que cette fois-ci la réussite complète sera au rendez-vous, avec une mise en production.

Les travaux effectués dans le cadre d'INCAS pourraient éventuellement servir également à un tout autre besoin : le leurrage des missiles IR à capacité de discrimination cinématique, le véhicule du LEA ainsi que les moyens d'éjection pouvant devenir communs aux deux applications.

L'Histoire dira si cette synergie se concrétisera !

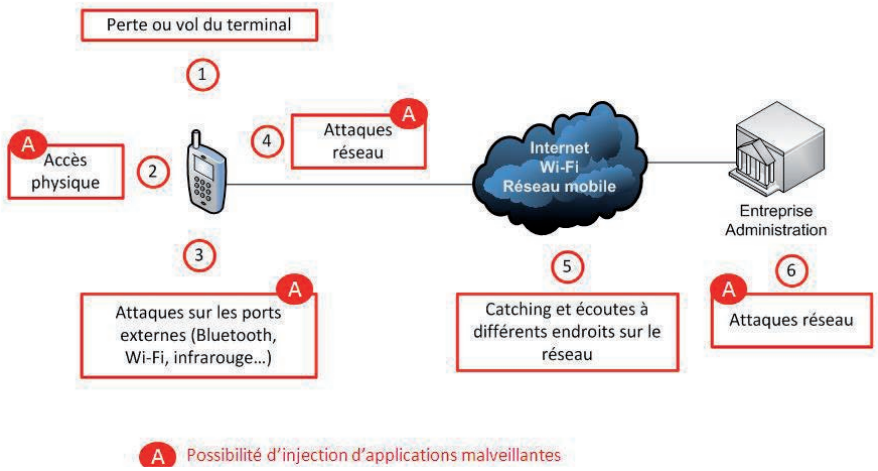
Jean **Tournier**, MBDA

Sécurité en profondeur des mobiles

LA DÉFENSE EN PROFONDEUR DES MOBILES : DE L'IDENTIFICATION DE BALISES ENNEMIES À LA PROTECTION DES SMARTPHONES

L'été et l'automne 2013 auront été riches en divulgation de programmes de recherche d'informations par les Américains et autres puissances étrangères sur les réseaux mobiles, internet télécom en général. Une fois de plus, nous prenons conscience des enjeux pour nos entreprises et nos autorités.

Pour mieux comprendre les menaces qui pèsent sur nos mobiles et Smartphones, une conférence a été proposée aux membres de l'Association Guerrelec le 7 octobre 2013 au Cercle de la Mer. L'article qui suit synthétise les principales menaces et propose des solutions robustes pour s'en prémunir.



1. Perte et vol :

c'est sans doute la principale menace car la plus courante. La personne qui récupère le téléphone peut alors accéder à de nombreuses données si le terminal n'est pas suffisamment protégé. Parmi ces données, il y a non seulement les emails, les contacts et l'agenda mais aussi les historiques d'appels, les historiques de SMS, etc. Il peut aussi y avoir des documents. Pour se protéger, il convient de chiffrer tout le contenu du terminal et proposer une authentification forte de l'utilisateur, par exemple avec l'usage d'une carte à puce tierce.

2. Accès physique :

l'attaquant accède au téléphone physiquement et y injecte un logiciel espion ou peut récupérer des données. Il peut alors à distance récupérer de nombreuses informations ou générer des SMS surtaxés. Si ce type d'attaque peut être complexe, elle peut être orchestrée sur des personnes ciblées. Pour y faire face, des techniques de vérification d'intégrité de contrôle du boot du terminal et de prévention d'installation de logiciels existent.

3. Attaques sur les ports externes :

il s'agit d'atteindre le Smartphone par les accès Bluetooth, Wi-Fi, infrarouge, etc., par exemple, les accès grands publics Wi-Fi dans certains lieux où il est possible d'être attaqué par son propre voisin de table. Face à ces menaces, rien de tel que de fermer/limiter ce type de liens, de renforcer les politiques de sécurité et de vérifier l'intégrité du terminal.

4. Attaques via le réseau :

la plupart des terminaux professionnels ont un accès plus ou moins sécurisé à leur mail mais également un accès direct à l'internet. C'est comme si un PC de bureau était connecté d'un côté au système de l'organisation de façon spécifique (via le LAN) et d'un autre côté à un accès internet grand public. Une telle situation permet de nombreuses attaques et transforme le Smartphone en potentiel cheval de Troie. Pour éviter une telle situation, il faut que les accès internet des Smartphones passent par l'entreprise / administration. Cela permet de bénéficier des systèmes déjà installés dans les systèmes d'information. Il est aussi important de disposer d'un pare-feu local et de contrôler l'installation d'applications.

5. « Catching » et écoutes sur les réseaux : le « catching » repère les identifiants de la SIM et du terminal ; les écoutes peuvent se faire à tous les niveaux du réseau : sur la partie radio, dans le cœur de réseau, sur les passerelles internationales, sur les transmissions internet. Face aux écoutes, il convient de chiffrer les transmissions en maîtrisant les clés de chiffrement. Face au « catching », il existe des systèmes d'identification des attaquants et quelques conseils de bon aloi tels que ne pas allumer son mobile dans un aéroport étranger, voire avoir un téléphone de secours.

6. Attaques réseaux :

les attaques peuvent enfin être ciblées sur l'accès de l'organisation pour s'introduire dans le système d'information. La parade repose sur l'authentification forte des utilisateurs et sur le respect des règles de pare-feu informatique ainsi que le contrôle d'intégrité des communications.

7. Injection d'applications malveillantes :

comme on peut le voir sur le schéma, les applications malveillantes peuvent être installées à différents endroits de la chaîne de transmission. Pour éviter cette menace, il faut respecter les différentes recommandations décrites ci-dessus.

Charles **d'Aumale,** ERCOM,
Directeur Vente et Marketing,
produits de sécurité

Les « NEMO trials » ou les essais OTAN 2013

Organisés chaque année, les essais GE OTAN 2013 reconnus sous le nom de « NEMO trials » (NATO ElectroMagnetic Operations) se sont déroulés en France du lundi 30 septembre au 4 octobre, aux abords de Toulon.

Ces essais s'inscrivent dans le cadre du groupe capacitaire OTAN AWWCG1 (Above surface Warfare Working Capability Group n°1, c'est-à-dire lutte au-dessus de la surface et tout ce qui est lutte antinavire ou antiaérienne en général) comprenant le volet GE navale, lui-même anciennement appelé MCG8 (Maritime Capability Group n°8) dédié, à l'époque, à notre domaine électronique. Chaque année, un état membre organise les essais GE selon un planning défini au fil des années.

Après la Turquie en 2011, le Danemark et l'Allemagne en 2012, la France était le pays hôte et organisateur des essais 2013, les derniers essais organisés par la France remontant à 2002.

S'inscrivant dans un volet capacitaire, la représentation française à l'OTAN à l'AWWCG1 est assurée par l'IPETA Stéphane Drouy, architecte ECM radar à DGA/Ingénierie Projet et le LV Charles-Philippe Récamier, Officier Programme GE à l'EMM. L'organisation de ces essais, sous l'autorité de l'UM NAV et de l'EMM, a été confiée à l'IETA Anne-Laure Fourrier chef du groupe « Evaluation Guerre Electronique » au sein de DGA/Techniques Navales et le capitaine de frégate Patrick Legros, commandant du CSGE qui, grâce à leur ténacité, leurs capacité d'adaptation, une patience à toutes épreuves associée à une bonne humeur stoïque en toutes circonstances, ont relevé le défi brillamment. On retiendra par exemple l'incendie lors de la Main Planification Conference à Toulon ou encore la juxtaposition calendaire du grand rassemblement de voiliers aux essais eux-mêmes, entraînant son cortège de reconfigurations et d'aménagements en tous genres…

Après une année de préparation réunissant les interlocuteurs des nations comme les différentes entités françaises de la DGA et notamment DGA IP, DGA EM et DGA MI, ou encore l'EMM, ALFAN, sans oublier la participation d'industriels comme TSA, TCS, NAVICO France et Lacroix et tout particulièrement DGA TN et le CSGE, les essais se sont déroulés de manière optimale du 30 septembre au 4 octobre 2013 aux abords de l'île du Levant et du site du SESDA au sud de la presqu'île de St-Mandrier.

SESDA

Parmi les nations participantes on compte pour les unités l'Allemagne avec une frégate de type Brandebourg, le « Mecklenburg-Vorpommern » et la Turquie avec la MEKO 200 « Oruçreis » et pour la partie française, la FAA « Cassard » de type éponyme et la participation de la frégate Horizon « Forbin » remplaçant au pied levé le « Chevalier Paul » retenu à la dernière minute pour raisons opérationnelles, sans oublier le pétrolier ravitailleur « Meuse » pour le soutien logistique.

Cassard

Mecklenburg-Vorpommern

Incendie à Toulon – avril 2013

Tall Ship Regatta

SESDA

Ile du Levant

Pour les moyens d'essais, les essais sont l'occasion de réunir tout l'arsenal de l'OTAN en matière de simulateurs, émulateurs, brouilleurs en tous genres avec des moyens allemands, italiens, norvégiens, turcs et britanniques ou encore des moyens de l'OTAN sans oublier la participation de pays associés comme la Suède.

Pour les senseurs et pods déployés on compte pour les différentes parties :

- Mesure de SER (surface équivalent radar) : des moyens français (BHR-NG), suédois (ARKEN) ou encore allemands (MARSIG et MEMPHIS) ;
- Mesures de SIR (signature infra-rouge) : des moyens français (BMIR), turcs (GREMLIN), italiens et allemands, pour ces derniers ayant en particulier un simulateur d'autodirecteur IR ;
- Emulateurs électromagnétiques comme pour les moyens français, SIRENE, MUSE et SEFP et OTAN avec le TRACSVAN
- Brouilleurs : des moyens OTAN (TRACSVAN), britanniques avec SIREN, un démonstrateur du leurre actif décalé qui a pu être mis en œuvre grâce au soutien du bâtiment de soutien affrété « Rebel », norvégien (EKKOII) et pour les moyens français (BULGAR, BAGUERA) ainsi qu'un brouilleur de GPS pour évaluer l'impact de cette action sur nos unités.

Bulgar

- Radars LPI (Low Probability Intercept) : installés sur les deux sites d'essais et fournis par la société NAVICO France et la participation d'un étraco du Commando Hubert équipé également d'un LPI.
- Simulateurs d'autodirecteurs : avec la contribution allemande du pod ROMEO, italienne avec CESARE depuis la côte et celle, française, du BAD portée par le Falcon de la société AVDEF.

Falcon AVDEF

- Mesure d'Imagerie radar avec le moyen norvégien PICOSAR, monté à bord d'un hélicoptère de la société « Global Heli Service » affrété pour l'occasion.

Au bilan 50 créneaux d'essais sur 51 prévus et près de 400 passes cumulées sur toutes les unités présentes ont fait de ces essais GE OTAN, comme en ont témoigné les différents participants lors du dernier rassemblement capacitaire de l'AWWCG1 à Bruxelles la semaine suivant les essais, une performance rare en termes de mise à disposition de moyens, d'expérimentations technico-opérationnelles dont les résultats permettront d'améliorer encore nos capacité et nos savoir-faire de détection, d'identification et de protection de nos unités.

Cet article est une nouvelle occasion pour remercier au nom de la communauté GE tous ceux qui ont œuvré à la réussite de ce grand rendez-vous, en particulier Anne-Laure Fourrier et Patrick Legros.

Souhaitons bon vent à l'Italie pour l'organisation des essais GE OTAN2014 !

LV Charles-Philippe **Récamier,**
Etat-major de la marine - Bureau Expertise
Officier de programmes Guerre Électronique navale

La Brigade RENS : vingt ans d'engagements opérationnels

Le 21 septembre dernier la Brigade de Renseignement a fêté ses vingt ans par une prise d'armes, puis deux journées portes ouvertes au camp d'Oberhoffen à d'Haguenau en Alsace. Une JPO constitue alors un moment privilégié pour découvrir ses matériels majeurs.

Créée le 1er septembre 1993, la nouvelle brigade prend le nom de BRGE – Brigade de Renseignement et de Guerre Electronique). Son organisation et son équipement sont inspirées par les leçons de la guerre du Golfe de 1991 et très vite elle doit face au contexte post-guerre froide, celui de la multiplication des opérations extérieures. En 1998, la BRGE est redésignée Brigade de Renseignement. Au cours de 20 dernières années, elle a été de toutes les crises (Balkans, Afrique, Moyen-Orient, Afghanistan), sur tout le spectre des engagements (action humanitaire, missions d'interposition, engagements de haute intensité et même territoire national). Des détachements de la BR sont aujourd'hui au Mali. Dès sa création, elle participe aux concepts nouveaux de numérisation du champ de bataille et de maîtrise de l'information de théâtre.

Le renseignement multicapteurs constitue le cœur de sa doctrine, au niveau de la brigade tout entière ou au sein d'unités modulaires plus légères. Dans cette force à forte densité technologique, chaque régiment est unique dans sa spécialité. Elle regroupe deux régiments de Guerre Electronique (les 44 et 54ème Régiments de Transmissions, avec respectivement 810 et 860 militaires), le 2ème Régiment de Hussards spécialisé dans le renseignement humain (770 personnels), le 28ème Groupement Topographique (avec un effectif de 310 militaires), et le 61ème Régiment d'Artillerie, régiment image de l'armée de Terre. Installé à Chaumont, ce régiment est équipé de drones tactiques (Drac d'EADS, et de SDTI Sperwer de Sagem) et de stations d'interprétation du renseignement multicapteurs SLI / SAIM (Thales). Implanté à Mutzig, le 44ème RT se consacre au renseignement d'origine électromagnétique de niveau stratégique, tandis que le 54 à Haguenau assure l'appui électronique d'une force au contact. La BR se complète d'un Centre de formation initiale des militaires du rang. En opérations, la BR se place au service de l'ensemble des forces déployées.

Innovante dans ses technologies, la BR l'est aussi au plan de l'organisation de ses dispositifs de déploiement. C'est à travers la BR que l'armée de Terre inaugure l'emploi des drones en France, à travers les systèmes du 61ème RA. Pour les OPEX, elle met en place des bataillons multicapteurs, des patrouilles légères d'appui électronique sur blindés PVP, et les équipes légères de Guerre Électronique. En toutes circonstances, elle fait appel à des savoir-faire très pointus au niveau de ses personnels : interprétation d'image, insertion auprès des populations, connaissance des langues étrangères.

La JPO de Haguenau a permis de redécouvrir l'épopée de la Guerre Electronique française, soit plus d'un siècle d'Histoire : la Tour Eiffel transformée en 1914 en station d'écoute, les centres GE de la guerre froide, ou encore le calculateur principal de la chaîne d'interception VHF Elodée qui a été déployée de 1980 à 1995 au 54ème RT. La discrétion naturelle de la BR n'a pas empêché l'exposition de matériels de nouvelle génération, tel que le tout nouveau véhicule CATIZ de Thales France (CApacité Terrestre d'Interception de Zone). Rattachés au 54ème RT, les CATIZ sont destinés à l'appui des unités au contact ou à l'escorte de dispositifs. Ils opèrent sur toute la gamme des fréquences radio. Pour sa part, le 2ème Régiment de Hussards a perçu les nouvelles jumelles infrarouges multifonctions JIM LR (Long Range) de Sagem qui équipe les patrouilles de recherche sur blindés VBL.

Sous le commandement du général Frédéric Hingray, la BR compte 3 600 hommes et femmes. La performance technologique, l'adapatabilité de ses matériels à la diversité des situations, l'intéropérabilité interalliée et la flexibilité de son organisation sont clairement au centre de ses préoccupations opérationnelles.

Philippe **Wodka-Gallien**

Station d'écoute EMILIE (Ensemble Mobiles d'Interception, de Localisation et d'Indentification des Emissions) du 44ème RT dédié à l'écoute sur la bande HF. Ce système a été développé et produit par Thales (Thomson-CSF à l'époque du programme) dans les années 1990. Photo Auteur

Un drone tactique SDTI Sperwer du 61ème Régiment d'Artillerie. En Afghanistan, les Sperwer ont effectué 2 500 missions sous les couleurs du Canada, des Pays Bas et de la France. Photo Sirpa Terre

Matériel organique de nouvelle génération du 54ème RT, les véhicules SAEC - Station d'Appui Electronique de Contact de Thales – opèrent sur les bandes radio et radar. Le véhicule est en présentation dynamique à Haguenau. Photo Auteur

Un hussard d'une patrouille de recherche doté de la nouvelle jumelle infrarouge multifonction JIM LR. Opérant en réseau, elle est dotée de fonctions de localisation de cibles. Photo Auteur

La Convention 2013 de l'AOC à Washington DC

Du 27 au 30 octobre dernier s'est tenue à Washington DC (USA) la convention annuelle des « Old crows » dont Guerrelec est le chapitre français. Ce fut une occasion de retrouver pendant quelques jours toute la communauté internationale de la Guerre Electronique autour de réunions d'échange, de conférences techniques et d'un vaste hall d'exposition.

Cette 50ème édition réunissait de nombreux participants de nations différentes. Après les allocutions des personnalités de la défense américaine, les journées de travail se structuraient autour de conférences thématiques dont celle de notre administrateur, Philippe Guillaume, sélectionné pour sa « mise en relation des mini-UAS et de la GE ». Des temps réservés, ainsi que des pauses, durant ces journées offraient des moments privilégiés pour visiter les nombreux stands installés dans le hall d'exposition.

Essentiellement industriels, les exposants présentaient une multitude de nouveautés et d'innovations dans le domaine de la RF et de la HF, des radios et des détecteurs radar, des équipements et autres systèmes, des antennes ou du cyber, etc… Enfin quelques événements conviviaux permettaient aux organisateurs de remettre des « Awards » et récompenses aux membres, aux invités ou aux Chapitres les plus dynamiques ou les plus méritants dans le domaine de la Guerre Electronique.

Le panneau Guerrelec à l'AOC

Philippe Guillaume lors de sa conférence

En résumé, l'AOC fut une convention annuelle aux multiples possibilités pour que ses participants (re)nouent les liens d'une communauté forte de 13 000 membres en 2013.

Pierre-Alain **ANTOINE**

(d'après un compte rendu oral d'Olivier Terrien et publié avec son autorisation)

MILIPOL 2013

La 18ème édition du Salon MILIPOL vient de se tenir au Parc des Expositions de Villepinte, du 19 au 22 novembre 2013. Les 915 exposants, dont 64% d'internationaux, venus de 49 pays ont présenté leurs innovations aux 25 834 visiteurs professionnels venus de 150 pays, 161 délégations officielles (+46% de plus qu'en 2011) de 97 pays.

Ce succès est le signe que le marché des industries de sécurité reste très porteur, nonobstant la baisse des budgets étatiques. Les états cherchent en fait à avoir une politique sécuritaire et des forces de l'ordre les plus efficaces et les plus réactives possibles, dans un processus qui dans le monde industriel serait décrit comme une augmentation de productivité, en particulier grâce à l'investissement technologique.

Ce phénomène est amplifié par l'émergence de nouvelles menaces et formes de criminalité, en particulier celles faisant appel aux nouveaux moyens de communication, réseaux sociaux et outils de paiement. La lutte contre cette cybercriminalité fait naturellement appel à de nouvelles spécialités, mais également à des moyens dédiés, largement représentés dans les allées du Salon. Cette situation a été particulièrement mise en exergue cette année par le couplage physique entre les Salons CARTES et MILIPOL, montrant, s'il est nécessaire la sensibilité du phénomène d'usurpation d'identité sous toutes ses formes.

Les hasards de l'actualité ont fait que l'inauguration du Salon par le ministre de l'intérieur, le 19 novembre, a eu lieu en pleine recherche de l'individu qui s'est attaqué aux rédactions de *Libération* et *BFM TV*. Ceci l'a conduit à souligner l'importance de garder un temps d'avance technologique pour mieux lutter contre toute forme de criminalité : « Nous devons donc toujours être à la pointe des technologies, voire posséder une technologie d'avance pour toujours agir et lutter efficacement contre ces dévoiements de la technologie » juge-t-il. Manuel Valls a ainsi mis en avant l'usage accru des nouvelles technologies par ses équipes : la biométrie, l'informatisation des fichiers d'empreintes digitales et génétiques, la vidéo-protection, la lecture automatique des plaques d'immatriculation... Pour continuer cet effort, il vient de lancer le projet de « Police 3.0 », afin d'avoir une police et une gendarmerie au fait des dernières technologies agissant dans une monde en réseau.

Dans la foulée, il a annoncé la désignation prochaine d'un délégué ministériel aux industries de la sécurité pour être l'interlocuteur de la filière, dont la formalisation vient d'être officialisée par le Premier Ministre.

Autre exposant institutionnel majeur de cette édition, la Commission Européenne (Direction Générale Entreprises et Industrie) s'est déclarée très satisfaite d'avoir pu rencontrer les bénéficiaires potentiels du programme de recherche « Horizon 2020 : relever le défi pour une société plus sûre » sur le point d'être lancé avec des thèmes aussi variés que les menaces cyber sur les réseaux de transport d'électricité que peuvent faire peser les compteurs intelligents, une meilleure préparation aux catastrophes naturelles découlant des dérèglements climatiques ou les investigations policières après une attaque NRBC, le tout doté de plusieurs centaines de millions d'euros.

Cette diversité se retrouvait le long des allées ou au cœur des pavillons nationaux, avec les matériels duaux classiques (véhicules, radiocommunications, armes, équipements de protection individuels pour humains et… pour chiens), des drones adaptés aux applications civiles, tous les moyens d'écoute, les différents capteurs et protections NRBC, les moyens de se préparer et de réagir aux attaques cyber, l'exploitation massive de la vidéo-protection, etc.

Exposant leurs domaines d'excellence sur ces thèmes, les grands intégrateurs que sont Cassidian, Morpho et Thales étaient naturellement présents ; signe de la mise en place de la filière des industries françaises de confiance et de sécurité ou bien effet des circonstances, c'est plus leur complémentarité qu'une confrontation frontale qui était offerte aux visiteurs.

La composante cybercriminalité du Pôle Judiciaire de la Gendarmerie Nationale (Photo Auteur)

Le Ministre de l'Intérieur reçu par Jean-Bernard Lévy et Marc Darmon sur le stand de Thales, lors de l'inauguration (Photo Auteur)

Equipement de protection individuelle pour chiens (Photo Auteur)

En avant-première de notre conférence du 16 décembre, Michel Cailliau, ancien Trésorier, membre Guerrelec, se fait présenter par Elodie Roché (Thales) les nouveaux outils vidéo adaptés à la sécurité dans les transports (Photo Photo Auteur)

par Pierre-Alain Antoine

LES CASSEURS DE CODES DE LA SECONDE GUERRE MONDIALE

Auteur : Sinclair McKay
Editeur : Ixelles éditions
ISBN : 978-2-87515-178-0
Pages : 400
Prix : 23,90 Euros

Des jeunes gens arrivent de nuit à la gare de Bletchley Park, 80 kilomètres au nord de Londres. Ils sont conduits jusqu'à une vaste demeure sombre et lugubre. Ils ne savent pas encore pour quelle mission ils ont été recrutés. Ainsi commence l'incroyable aventure de ces civils qui, enrôlés auprès des plus brillants cerveaux britanniques, ont changé le cours de l'Histoire.

De la Bataille d'Angleterre au Japon, en passant par le Blitz, El Alamein ou encore le jour J, le travail de Bletchley Park est demeuré complètement invisible. Pourtant il a joué un rôle crucial dans le conflit. Loin des champs de bataille, les casseurs de codes vous font partager leur vie insolite et passionnante au cœur du renseignement et de la cryptanalyse.

Un des premiers livres traduits en français de cette fabuleuse histoire.

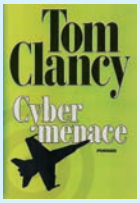
Doit avoir une place de choix dans la bibliothèque d'un membre de Guerrelec

ELECTRONIC WARFARE FROM THE BATTLE OF TSUSHIMA

Auteur : Marco de Archangelis
Editeur : Blanford Press, Poole, Dorset
ISBN : 0-7137-1501-4
Pages : 320
Prix : £ 13,97

En un seul ouvrage en langue anglaise, l'auteur nous brosse un siècle de Guerre Electronique. Tous les événements marquants y sont traités en détails. Ponctués de cartes et de photos peu connues, ce livre peut rester dans la poche d'un membre de Guerrelec car il lui permettra de répondre à toutes les « colles » en la matière…

CYBERMENACE



Auteurs : Tom Clancy
Editeur : Albin Michel
ISBN : 978-2-226-25202-9
Pages : 715
Prix : 25 Euros

Les ambitions territoriales de la Chine ne cessent de croître. En ligne de mire : Taïwan et le sud de la mer de Chine où patrouille la flotte de l'US Navy. De retour à la Maison Blanche, Jack Ryan Sr. est confronté à une crise internationale majeure. A l'heure où les deux superpuissances sont au bord de l'affrontement, le Président sait qu'il peut compter sur l'organisation antiterroriste clandestine qu'il a initiée.

Mais la taupe menace l'existence du campus, en proie à des attaques ciblées. Jack Jr. et ses hommes pourront-ils prévenir à temps une cyberguerre mondiale aux conséquences terrifiantes ?

Ce livre est en plein dans les nouvelles orientations de notre Association Guerrelec. Thomas Leo Clancy Jr, est né à Baltimore dans le Maryland, le 12 avril 1947, il est mort le 1er octobre 2013 dans cette même ville. Les romans d'espionnage du genre techno-thriller de ce romancier sont techniquement très documentés et tournent autour du milieu du renseignement américain et, plus précisément, de la CIA sur fond de guerre froide ou de terrorisme.

Cybermenace est son avant-dernier livre, son dernier roman *Command Authority* sortira en décembre 2013 à titre posthume…

ELECTRONIC WARFARE – AIR FORCE DOCTRINE DOCUMENT 3-12-1 (AFDD)

Auteur : **USAF**
Editeur : Amazon.co.uk, Ltd
ISBN : 978-1-4802-7183-8
Pages : 50
Prix : 5,50 Euros

Ce document, édité par Amazon, n'est autre que la doctrine de l'USAF en matière de Guerre Électronique en date du 5 novembre 2002, amendé du « Change 1 » du 28 juillet 2011.

En six chapitres, tout est écrit. Ce sont :

- Chap 1 : Background
- Chap 2 : EW Operational Concepts
- Chap 3 : Electronic Warfare Organisation
- Chap 4 : Planning and Employment
- Chap 5 : Equip and Sustain
- Chap 6 : Education and Training
- Glossary

GUERRE FROIDE, ESPIONNAGE NAVAL

Auteur : Peter A. Huchthausen, Alexandre Sheldon-Duplaix
Editeur : Nouveau monde
ISBN : 978-2-7089-9239-9
Pages : 687
Prix : 24,50 Euros

Ignoré par les ouvrages traitant de la guerre froide, l'espionnage naval permit aux deux blocs d'utiliser les océans et les ports pour surveiller et pénétrer le camp adverse. Nourri par des entretiens avec des protagonistes soviétiques et occidentaux et par l'exploitation des archives américaine et britannique et de publications russes, ce récit fourmille d'anecdotes inédites, parfois terrifiantes. On y apprend qu'un cuirassé soviétique, ex-italien, explosa mystérieusement à Sébastopol en 1955, laissant croire à un sabotage par un prince fasciste, qu'un marin soviétique aurait obtenu d'un général français les plans de frappe de l'OTAN qui décidèrent Khrouchtchev à déployer des missiles à Cuba et qu'une erreur de traduction dans un message intercepté poussa Johnson à engager les Etats-Unis au Vietnam. Et plein d'autres chose encore…

L'amiral Pierre Lacoste, ancien directeur de la DGSE (1982-1985), dit de cet ouvrage : « Un livre riche en informations inédites, révélations sensationnelles et nouveaux jugements qui passionnera à la fois les spécialistes de combat naval et le grand public curieux d'Histoire ».

LES JETS ALLEMANDS DE LA SECONDE GUERRE MONDIALE

Auteur : Dominique Breffort, dessins d'André Jouineau
Editeur : Histoires et collections (avions et pilotes n° 17)
ISBN : 978-2-35250-223-4
Pages : 90
Prix : 18 Euros

L'Allemagne est non seulement la première nation à avoir fait voler un appareil à réaction (le Heinkel He 178, en août 1939), mais aussi le seul pays engagé dans le second conflit mondial à avoir produit en grande série et surtout à avoir engagé au combat plusieurs types d'appareils utilisant ce mode de propulsion, ouvrant ainsi la voie à la guerre aérienne telle que nous la connaissons aujourd'hui.

Pratiquement tous les pays alliés se sont inspirés, après la guerre, des options prises par le Reich en matière d'aviation à réaction. Ce ne sont pas les Français qui me démentiront car les réacteurs ATAR de la SNECMA, ont été dessinés et mis au point par l'équipe d'Hermann Östrich, ancien chef du bureau d'étude de BMW.

Une bonne base de travail.

www.guerrelec.fr

Les sociétés membres de Guerrelec

AMESYS • ARINC • DCI AIRCO • DIGINEXT • EADS ASTRIUM• INEO DEFENSE • LACROIX DÉFENSE & SÉCURITÉ • MBDA • RUBISOFT • SAFRAN • THALES Communications • THALES DAE • THALES UNIVERSITE • VECSYS

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, Charles d'Aumale, Pierre Grandclément, Charles-Philippe Récamier, Jean-François Sulzer, Jean Tournier et Philippe Wodka-Gallien.