N° 56
Décembre
2019

Lettre d'information de
# Guerrelec
Si vis pacem para bellum... electronicum

## Le mot du Président

*Chers amis, chers adhérents*

***La GE se réveille… comme je vous l'écrivais dans la dernière Lettre d'Information Guerrelec.***

*Premier signe tangible : la signature le 18 novembre par la ministre des armées du lancement de la phase de réalisation du programme ARCHANGE (avion de recueil SIGINT). Deuxième signe, la signature d'une convention CYBER le 14 novembre entre huit grands groupes industriels de l'armement et le MINARM. En effet, plusieurs de ces grands groupes ont été victimes de cyber attaquants. L'enjeu de cette convention CYBER est la sécurité de toute l'industrie de la défense, depuis les plus petits sous-traitants jusqu'aux plus grands maîtres d'œuvre. On ne peut plus tergiverser, le MINARM a pris le taureau par les cornes et souhaite investir plus de 1,5 Md € pendant la LPM et embaucher des centaines d'ingénieurs supplémentaires sur le pôle CYBER à DGAIMI pour maîtriser cette problématique. C'est pourquoi nous avons souhaité mettre en exergue, dans votre lettre préférée, une place importante à la Cybersécurité.*

*En cette fin d'année, je rappelle à tous qu'adhérer à une association signifie approuver et défendre une cause qui réunit tous les membres de cette association. Une association ne peut vivre que si ses membres s'investissent pour son rayonnement et son expansion. Nous avons besoin de vos idées, de vos propositions d'amélioration et de vos souhaits pour animer Guerrelec. Je compte sur votre implication pour dynamiser notre action l'année prochaine.*

*En attendant, je vous souhaite un joyeux Noël et vous présente mes meilleurs vœux pour l'année 2020. Je vous dis « A l'année prochaine ».*

*Bonne lecture et bonnes vacances à tous.*

Pierre **Grandclément**
*Président de Guerrelec*

## Florence Parly, ministre des Armées, lance la réalisation du programme ARCHANGE

Résultat de dix années d'études sur des technologies de pointe, l'ensemble des capteurs constituant la charge utile d'ARCHANGE[1] sera développé par Thales. Cette charge utile, basée sur des technologies innovantes (antennes multi-polarisation, intelligence artificielle pour améliorer les traitements automatiques), permettra de détecter et d'analyser les signaux radar et de communication grâce à des capteurs intégrés sur un avion d'affaires *Falcon 8X* construit par Dassault Aviation.

Ces *Falcon 8X* modifiés avec leur système de mission bord et sol porteront le nom d'ARCHANGE. Conformément à la loi de programmation militaire 2019-2025, trois systèmes remplaceront les deux *Transall C-160 « Gabriel»*. Une plateforme d'entraînement au sol dont le déploiement est prévu sur la base aérienne d'Evreux complètera le dispositif.

Les systèmes ARCHANGE accroîtront significativement les capacités de renseignement électromagnétique aéroporté français et contribueront à l'effort particulier sur la fonction stratégique « connaissance et anticipation », gage de l'autonomie de décision de la France et de sa supériorité en opération. Le programme ARCHANGE contribue ainsi à la remontée en puissance des armées voulue par le Président de la République.

**Communiqué de Presse du Ministère des Armées**

[1] **ARCHANGE**: **A**vions de **R**enseignement à **CHA**rge utile de **N**ouvelle **GE**nération

# Milipol 2019 : sûreté et sécurité intérieure


La dernière édition de Milipol s'est tenue du 19 au 22 novembre 2019 à Paris Nord Villepinte avec plus de mille exposants de 53 pays, couvrant des domaines allant de l'équipement individuel du policier (et de son chien) à la surveillance du cyberespace. MILIPOL se présente comme l'événement mondial de la sûreté et de la sécurité intérieure des états. La protection des grands événements constituait naturellement, avec l'approche des JO 2024, le fil conducteur des présentations sur de nombreux stands.

Dans le spectre d'intérêt de Guerrelec, on notera :

- Les outils de supervision de plus en plus puissants centrés sur une collecte massive de données hétérogènes et potentiellement incohérentes,
- Une offre toujours plus complète de Cybersécurité, couvrant tout le cycle de vie des solutions et permettant aux opérateurs de s'entraîner comme on le ferait sur un champ de tir, la zone grise du domaine cyber-physique étant toutefois peu couverte,
- Un regain d'intérêt pour la protection contre les drones, de la détection électronique ou optique, à leur neutralisation, qui reste… un point dur.

Affaire à suivre…

Jean-François **Sulzer**

# DSEI fête ses 20 ans

Après la fusion de deux salons indépendants, l'un de la British Army (armée de terre), l'autre de la marine (Royal Navy), DSEI regroupant les deux domaines est repris en 1999. Aujourd'hui, ce salon de la défense et de la sécurité (DSEI) qui n'a cessé de grandir est organisé tous les deux ans par Clarion Events à qui il appartient depuis 2008. Il recoupe les 5 domaines-clés : Air, Marine, Terre, Sécurité et Interarmes.

Les priorités ont bien changé depuis le 11 septembre 2001 et l'industrie a considérablement évolué. La menace du champ de bataille électronique, l'expansion du savoir-faire technologique combinés avec les coupes budgétaires dans le domaine de la défense ont transformé la façon dont les industriels se comportent sur le marché. Cette année DSEI s'est concentrée sur les technologies émergentes : l'Intelligence Artificielle, les Systèmes Autonomes, la Robotique, le Big Data, etc. En dépit des polémiques de politiciens dont ce salon a fait l'objet, en particulier, à cause de la nature des pays invités, DSEI est le lieu de rencontre d'industriels de la défense et de la sécurité avec la participation de 1 600 exposants de 69 pays et l'organisation d'un vaste programme de conférences devant 34 000 visiteurs.

L'édition 2019 s'est tenue du 10 au 13 septembre à Londres, avec 35 000 visiteurs, 1 700 exposants, plus de 300 conférenciers, de 69 pays et plus de 44 pavillons internationaux dont pour la première fois cette année la Lettonie et la Lituanie.

Pierre-Alain **Antoine**

# Thales et la Cybersécurité

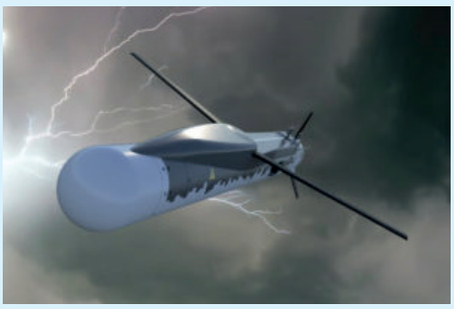
Thales était présent à DSEI, Londres, en septembre avec la démonstration de son savoir-faire et la maîtrise de la chaîne de décision critique dans les composantes : air, terre, marine, sécurité et espace. La compagnie a investi dans les quatre domaines de la connectivité/ IoT (Internet of Things), le Big Data, l'intelligence artificielle et la Cybersécurité.

Thales a démontré son leadership dans la maitrise de la chaîne critique de décision dans les cinq domaines air, terre, mer, espace et sécurité. Ce salon a par ailleurs fait l'objet d'une conférence le 11 septembre avec le titre « Electronic Warfare Transformation », c'est-à-dire l'exploration de la transition de la GE traditionnelle à une GE combinée à la Cybersécurité qui est un enjeu majeur. La conférence a couvert une gamme de sujets variés allant de la gestion des données à l'intelligence artificielle, en passant par la gestion des menaces et la visualisation de la GE dans le futur.

Dans ce même domaine de la Cybersécurité, Thales vient par ailleurs d'obtenir pour sa sonde de détection de cyberattaques, *Cybels Sensor*, le Visa de sécurité ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) pour sa qualification élémentaire. Ce visa permettra aux Opérateurs d'Importance Vitale (OIV) de se mettre en conformité avec la loi de programmation militaire 2014-2019 pour la détection de cybermenaces, face à l'augmentation de menaces informatiques. Cette sonde de détection bénéficie de l'expertise historique de plus de 40 ans de Thales dans les domaines de la détection de cyberattaques et du développement sécurisé de systèmes d'information critiques. En analysant en temps réel de grands volumes de données dans lesquels elle détecte les menaces potentielles, la sonde permet d'alerter au plus tôt les équipes en charge de la supervision de sécurité pour maximaliser la protection des réseaux surveillés. Elle permet aux OIV et aux entreprises de détecter les cyberattaques en supervisant leurs réseaux en toute confiance. La sonde de détection bénéficie de l'expertise historique de plus de 40 ans de Thales dans les domaines de la détection de cyberattaques et du développement sécurisé de systèmes d'information critiques.

Pierre-Alain **Antoine**

# Le Royaume-Uni à l'offensive avec le SPEAR de MBDA



*Le missile SPEAR emportera une charge de GE (Photo MBDA)*

Dans le cadre de l'équipement du *Tempest*, le nouveau chasseur britannique de 6ème génération qui entrera en service en 2035 pour remplacer l'*Eurofighter Typhoon,* la Royal Air Force s'est intéressée au développement d'une nouvelle version du missile air-sol SPEAR de MBDA dotée d'une charge de guerre électronique pour brouiller les moyens de détection ennemis.

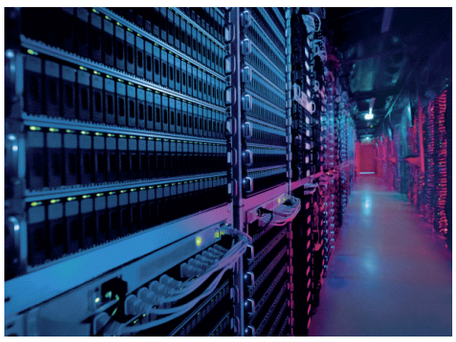
MBDA vient de se voir octroyer par le MoD britannique un contrat pour ce démonstrateur d'une nouvelle version GE de la famille du système d'armes SPEAR, en partenariat avec l'Italien Leonardo (groupe aéronautique et de défense) pour compléter la panoplie étendue de missions SEAD. SPEAR intégrera la charge utile miniaturisée de pointe conçue par Leonardo qui agira comme un brouilleur stand-in pour accroitre la survivabilité d'un appareil de la RAF et qui détruira les défenses ennemies en agissant comme un démultiplicateur de forces. « *Ces nouveaux brouilleurs électroniques leurreront nos adversaires et garderont nos pilotes en sécurité dans l'espace aérien* », a précisé le ministre britannique Anne-Marie Trevelyan, en charge des acquisitions.

L'idée est de remplacer les charges militaires par des charges utiles miniaturisées fabriquées par Leonardo, qui peuvent brouiller les défenses ennemies, selon une déclaration de MBDA au salon DSEI à Londres en septembre. Le système SPEAR vient de terminer chez BAE Systems une série de tests au sol et des essais de fonctionnement d'un lanceur sur l'*Eurofighter Typhoon*. Notons que MBDA est le fabricant désigné pour le programme *Tempest*.

Pierre-Alain **Antoine**

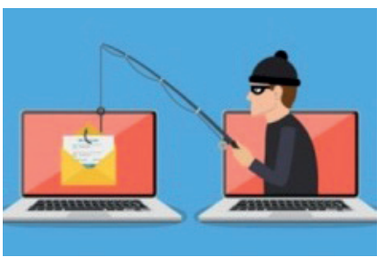
# Cyber-sécurité : une victoire de la Gendarmerie

Les hackers et les pirates informatiques ont souvent une longueur d'avance sur la cybersécurité. Pourtant l'alliance de la cyber-gendarmerie et du groupe tchèque Avast vient de prouver le contraire en démantelant un réseau de pirates informatiques qui, grâce à un malware informatique, a discrètement infecté les ordinateurs.



La gendarmerie française a annoncé au début de l'automne être parvenue à neutraliser un réseau d'ordinateurs piratés agissant sur plusieurs centaines de milliers de machines, après avoir reçu des informations de l'éditeur d'anti-virus Avast. Le réseau d'ordinateurs était commandé par un serveur hébergé en Ile-de-France. Toutes les machines, localisées notamment en Amérique centrale et en Amérique du sud, avaient été infectées par le virus *Retadup* qui permettait aux pirates d'en prendre le contrôle à distance, à l'insu de leur propriétaire.

Afin de mettre fin au développement du réseau de robots générés par *Redatup*, le Centre de lutte contre les Criminalités numériques (C3N) dirigé par la Gendarmerie Nationale a cherché à comprendre comment fonctionnait ce botnet et a ensuite analysé la façon dont il se propageait en s'associant au groupe tchèque Avast connu pour le développement de son antivirus pour réussir à démanteler *Redatup*, ainsi qu'aux services du FBI. Alertée par Avast de l'existence de *Retadup* et de la présence du serveur de contrôle en France, la gendarmerie a d'abord réalisé au printemps 2019 une « copie discrète » du serveur en cause, chez son hébergeur en Ile-de-France, sans que les pirates ne s'en rendent compte. L'analyse du serveur a montré l'existence d'une faille dans le logiciel utilisé par les pirates, selon le récit de la gendarmerie. Les cyber-limiers du centre de lutte contre les criminalités numériques (C3N) de la gendarmerie ont ensuite pu utiliser cette faille pour désinfecter à distance tous les ordinateurs touchés, avec l'aide notamment du FBI, la police fédérale américaine. Pour ce faire, ils ont en juillet substitué au serveur des pirates une machine qu'ils contrôlaient eux-mêmes et qui a pu envoyer les instructions nécessaires aux machines touchées.



Cette première mondiale aboutit à désinfecter à l'heure actuelle 800 000 machines, selon la gendarmerie. « *Les investigations se poursuivent pour identifier le groupe criminel à l'origine des faits* », a-t-elle précisé. Le réseau d'ordinateurs infectés permettait notamment aux pirates de générer de la cryptomonnaie Monero.

L'opération a été menée sous le contrôle de la section F1 du Parquet de Paris, spécialisée dans la cybercriminalité. Cette technique de piratage est connue sous le nom de « phishing ». *Redatup* incite les internautes à cliquer sur n'importe quoi en faisant parvenir un e-mail piégé à des destinataires et leur propose de cliquer sur un lien. C'est ainsi qu'ils autorisent un fichier malveillant à s'installer dans de leur ordinateur... C'est ainsi qu'après plus d'un mois et demi de recherches, les trois entités ont réussi à mettre fin à la propagation du programme informatique malveillant et à désinfecter les machines à distance. Pour le plus grand bien des utilisateurs !

Pierre-Alain **Antoine**
Sujet proposé par Jean-François Sulzer
(Source AFP et Les partenaires de Science et Avenir)

# Guerre Cyber : les USA durcissent le ton en Iran

**L'US Air Force se sert de la guerre cyber pour supprimer les défenses aériennes ennemies et mettre en lumière son potentiel afin de soutenir les opérations air à venir. Ces défenses ont été prises pour cible par une riposte cyber américaine immédiatement après l'attaque.**

Le 20 juin dernier, la mission OCA (Offensive Counter Air) a pris un tournant tout en nuances mais néanmoins important. Après la destruction d'un drone HALE « Global Hawk » RQ-4A de Northrop Grumman appartenant à l'US Navy par un SAM iranien Sayyad-2C/3, longue portée, haute altitude, le Cyber Command américain (USCYBERCOM) a prononcé une attaque cyber contre le système de défense aérienne intégré iranien IADS (Iranian


*En juin 2019 les systèmes de défense aérienne sol de l'Iran ont illustré leur puissance en abattant un Global Hawk RQ-4B de la marine américaine.*
*(Photo Iranian Air Defences Wikimedia)*

Integrated Air Defence System). La presse rapporte que l'attaque était portée contre des calculateurs contrôlant les batteries SAM. Le champ exact de l'attaque n'a pas été révélé, cependant il aurait pu rendre inutilisables temporairement les systèmes de commande et de contrôle des systèmes Sol-Air ou priver l'IADS de sa capacité à partager cible et données de suivi entre les installations. Il semble que l'attaque était la première action de cette sorte entreprise par USCYBERCOM depuis qu'il est devenu un commandement opérationnel à part entière en mai 2018. Cela est le premier emploi de la nouvelle plateforme unifiée (offensive et défensive) de combat cyber de Northrop-Grumman bien que ceci n'ait pas été confirmé par le Ministère de la Défense américain.

Alors que les actions de USCYBERCOM représentent un important progrès dans le développement de la guerre cyber pour soutenir les opérations aériennes, elles ont été le point culminant de plusieurs années de développement dans l'usage des armes cyber pour soutenir les missions OCA et SEAD. L'arme cyber OCA/SEAD la plus connue est probablement le projet Suter de BAE Systems. Suter a été commandé par le 645th Aeronautical Systems Group de l'US Air Force, plus connu sous le nom de *Big Safari* qui a pour mission de développer ce qui est par euphémisme appelé les « armes spéciales » pour la force aérienne. Suter permet initialement de localiser et identifier les radars hostiles qu'il faudrait attaquer.

Cela pourrait être fait en utilisant les avions de collecte de renseignement électronique stratégique comme le Boeing RC-135U « Combat Sent » de l'US Air Force. Suter est alors utilisé pour générer des formes d'onde de fréquence radio transmises dans les radars offensifs. Cela peut faire appel à la technologie DRFM (Digital Radio Frequency Memory) qui échantillonnera un signal de radar hostile, changera sa modulation et d'autres paramètres pour les transmettre au radar. Cela peut avoir pour effet de brouiller discrètement le radar en question en lui faisant afficher de fausses informations en ce qui concerne la vitesse de la cible, la position ou l'altitude, bien que les systèmes DRFM puissent habituellement effectuer une myriade d'autres profils d'attaque électronique. C'est à ce stage que le programme Suter peut peut-être infecter un IADS hostile en injectant un virus dans le signal de brouillage transmis afin de neutraliser la Cybersécurité utilisée par le radar ou l'IADS. Lorsque la transmission RF du Suter est reçue par le radar, elle est numérisée. On peut alors raisonnablement partir

de l'idée que, pour que le but du Suter réussisse lorsqu'il attaque un IADS hostile, l'ouverture du radar à travers ce qu'il pénètre doit être mise en réseau dans l'architecture IADS plus large, soit par fibre optique, soit par faisceau hertzien. Une fois que l'IADS est pénétré, il est possible de continuer à le nourrir avec de fausses informations et/ou contrôler les senseurs IADS. Par exemple, cela pourrait être piloté à distance en ciblant un morceau de ciel où les opérations aériennes sont en cours.

Des informations accessibles au public font remarquer que le programme comprend plusieurs segments. Suter Block-1 permet à l'utilisateur de voir l'image radar tirée d'un radar hostile, de générer un ordre de bataille électronique pour son adversaire et d'évaluer les paramètres des radars en question. Suter Block-2 permet à l'utilisateur de prendre contrôle de ce radar tandis que Suter Block-3 est conçu pour pénétrer les réseaux de calculateurs contrôlant des cibles sensibles au temps telles que des lanceurs de missiles balistiques mobiles. Des versions diverses non dévoilées du programme ont été utilisées durant les opérations aériennes en Afghanistan et en Irak, conjointement avec le EC-130H « Compass-Call » de Lockheed-Martin, le RC-135V/W « Rivet Joint», avion de collecte de renseignement et de signaux et le F-16CJ « Viper Weasel » SEAD de General Dynamics/Lockheed Martin Il est possible que le RC-135U soit équipé du logiciel du Suter Block-1 comme partie de ses capacités de collecte ELINT. Le programme Suter Block-2 peut être installé à bord de la plateforme électronique EC-130H, ce qui aurait du sens vu sa mission.

Est-ce que Suter a été utilisé pour attaquer des parties ou le tout de l'IADS iranien en juin ? L'aspect déconcertant de l'incident est qu'il n'y avait pas d'autres avions impliqués dans cette attaque ou ses répercussions sauf le RQ-4A et un Boeing P-8A « Poseidon », avion de patrouille maritime de la marine américaine. Aucun des avions censés être capables de déployer le programme Suter ne semble avoir été au voisinage de l'Iran lorsque les Américains ont réalisé leur attaque cyber. Comme expliqué précédemment, il se peut qu'une plateforme aéroportée soit une condition *sine qua non* pour utiliser Suter. Cela n'est pas surprenant car cela aurait du sens que l'avion transportant le programme soit en vue d'un radar, très probablement ses lobes secondaires, afin d'éviter la détection ou bien une antenne de communication connectée à l'IADS pour injecter le programme Suter. On a spéculé sur le fait que Suter ait pu


*L'avion de collecte de renseignement ELINT stratégique RC-135U « Combat Sent » de l'US Air Force a les moyens d'employer des parties du programme Suter contre les systèmes hostile de défense aérienne au sol (photo USAF)*

être intégré à bord de drones secrets pilotés par l'US Air Force, bien qu'on ne sache pas si ces plateformes incluent le RQ-4A. Cela pose la question de savoir si les Américains ont à la place réalisé la cyberattaque directement depuis les USA ou depuis des installations américaines au Moyen-Orient… Si oui, une telle attaque pourrait avoir été effectuée avec la plateforme unifiée et réalisée par la 24th Air Force de l'USAF, elle-même partie prenante du CYBERCOM. Le 11 octobre, la 24th Air Force et la 25th Air Force, l'unité de collecte de renseignement principale de l'US Air Force, ont fusionné pour former la 16th Air Force. C'est cette unité qui doit réaliser des cyberopérations en soutien à des opérations aériennes combinées dans l'avenir….

Il est possible que nous connaissions jamais le système cyber exact utilisé pour attaquer les défenses iraniennes le 20 juin, mais nous savons que la guerre cyber comme complément aux missions OCA et SEAD est maintenant une réalité. Il semble que cela doive jouer un rôle croissant dans le soutien des futures opérations aériennes américaines.

Dr. Thomas **Withington**

***Thomas Withington*** *est depuis 20 ans journaliste et analyste en Guerre Electronique. Son expérience couvre la GE, les communications militaires et les radars militaires. Il a largement travaillé sur les aspects contemporains et historiques de ces domaines durant sa carrière et est l'éditeur de la Newsletter Armada International traitant de la Guerre Electronique. Il est aussi un commentateur expérimenté sur des questions de défense pour les organes de presse du monde entier.*

# L'effigie d'un casseur de code sur le futur billet de £50 au Royaume-Uni

*Alan Turing*

Alan Turing est l'un des plus grands mathématiciens que la Grande-Bretagne ait jamais eus à Bletchley Park, haut lieu des services secrets de Churchill durant la Seconde Guerre mondiale pour le cassage de codes d'*Enigma*, c'est-à-dire le Chiffre utilisé par les Nazis pour cacher les heures et les lieux d'attaques de sous-marins. Le gouvernement britannique s'était tourné vers lui pour casser *Enigma* qui amenait des pertes considérables au royaume.

Après avoir été discriminé pour son orientation sexuelle qui l'amena à se suicider, le gouvernement vient de le réhabiliter en proposant d'imprimer son visage sur le nouveau billet de £50 livres qui sera lancé en 2021.

A la fin de la guerre, Turing devenu très vulnérable fut poursuivi en 1952 pour « indécence de comportement ». Plutôt que d'aller en prison, il choisit la castration chimique, ce qui affecta son talent intellectuel. Puis il ingéra du cyanure, dit-on, en mordant une pomme en 1954, ce qui fut révélé deux ans plus tard. Le gouvernement britannique se lança alors dans des excuses posthumes. Peut-être la marque à la pomme Apple s'en est-elle inspirée pour dessiner son logo…

La contribution de Turing à l'effort de guerre contre l'Allemagne nazie durant ses années à Bletchley Park est incalculable. Cette connaissance permit à la British Navy de se préparer à contre-attaquer avec succès. Alors commencèrent à poindre une série d'excuses publiques envers Turing. Puis ce fut le pardon royal, presque 60 ans après sa disparition. Le gouverneur de la Bank of England a récemment déclaré que Alan Turing était un mathématicien extraordinaire dont le travail a eu un effet énorme sur nos vies d'aujourd'hui. Il est le père de l'ordinateur et de l'intelligence artificielle.

La banque a lancé un concours pour recueillir des suggestions sur celui qui pourrait enrichir le nouveau billet qui sortira en 2021. Près de 230 000 noms furent proposés, mais seulement 1 000 d'entre eux ont satisfaits aux critères requis.


*Alan Turing © Bank of England*

Geneviève **Moulard**

# Les nouvelles armes de Poutine

A l'heure où la France va évoluer vers la création d'un commandement de l'espace, on peut s'attarder sur les intentions russes de se doter d'une panoplie de missiles de nouvelle génération.

Alors que des dizaines de programmes ont été développés dans les années 80, le président russe a dévoilé en 2018 de nouveaux systèmes de missiles. Il a souligné leur capacité à contourner la défense anti missile adverse. Parmi les six armes stratégiques présentées se trouve la torpille ***Poséidon*** filant sous la mer à 200 km/h grâce à une unité de propulsion nucléaire miniaturisée et emportant une charge atomique susceptible de déclencher un tsunami radioactif pour détruire installations portuaires et bases navales. Puis, vient le planeur hypersonique ***Avangard*** muni de charges conventionnelles et nucléaires qui pourrait être déployé cette année avec un objectif de dix à douze unités en 2027 et lancé à terme par un missile balistique. Ensuite, devraient être testés en vol cette année le missile ***Sarmat***, le ***Peresvet***, arme laser susceptible d'éblouir les systèmes électroniques les plus performants, ou encore le ***Kinzhal***, missile hypersonique de haute précision pouvant évoluer à Mach 10 et lancé depuis un avion MiG-31K.

*Le missile Bourevestnik*
*(photo Reuters, article Michel Moutot, AFP)*

Le plus remarqué est le ***Bourevestnik***, ***SSC-8 pour l'OTAN***, missile subsonique, à propulsion nucléaire et volant entre 50 et 100 mètres du sol, capable d'esquiver les défenses anti missiles dont la portée serait quasiment illimitée. Il aurait déjà été expérimenté. « *C'est une arme invincible* » a souligné Vladimir Poutine.

Course aux armements, concurrence entre des technologies militaires ? La course n'a jamais existé, précise un officiel russe, mais la qualité a remplacé la qualité.

Pierre-Alain **Antoine**
Sujet fourni par Roland Campo
Et d'après Alain Barluet, correspondant à Moscou,
« Faut-il craindre les supermissiles de Poutine »,
*Le Figaro* du 16 septembre 2019.

# Conférences / Evènements Guerrelec du 2ème semestre 2019

## Lundi 23 Septembre

**2019-2025 : la rupture en matière d'espace de bataille numérisé aéroterrestre** par le général de division Charles Beaudouin, Sous-chef d'Etat-Major "Plans et Programmes" / Etat Major de l'armée de terre.

*Le général Beaudouin*

*Pierre Grandclément avec le général Beaudouin*

## Lundi 14 Octobre

Conférence basée sur l'ouvrage « ***Les Espions de l'Elysée, le Président & les Services de Renseignement*** » (auteurs : Alexandre Papaemmanuel et Florian Vadillo).
Par Alexandre Papaemmanuel, enseignant à Sciences Po, directeur Défense Renseignement et Sécurité au sein d'une entreprise innovante du numérique.


*Le conférencier Alexandre Papaemmanuel*

*La conférence Guerrelec au féminin*

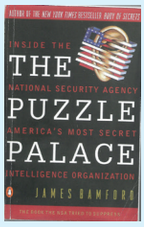
## Lundi 25 novembre

**RETEX sur ses années OTAN, les innovations et la Guerre Electronique** par le général Denis Mercier, ancien chef d'état major de l'Armée de l'air.

*Le général Denis Mercier durant la conférence*

*Photo « Armée de l'air » avec le colonel Fabrice Cinquetti, le commandant David Favrie et le général Denis Mercier*

## The Puzzle Palace (Inside the NSA)




**Auteur :** James Bamford
**Editeur :** Penguin books
**Pages :** 655
**Prix :** $ 20
**ISBN :** 978-0-14-006748-4

Ce livre en langue anglaise mais écrit avec un vocabulaire simple nous apprend beaucoup de choses sur l'Histoire des écoutes américaines depuis la 1ère Guerre Mondiale. Son sous-titre est *Inside the National Security Agency America's most secret intelligence organisation*, mais la traduction de la dernière ligne de la 1ère de couverture est : « Le livre que la NSA a essayé de faire interdire… ». Ce qui en dit long sur les pratiques de Fort Meade et de ses 100 00 agents de par le monde. Vous découvrirez également que l'accord UKUSA signé en 1947 – mais jamais rendu public – entre les Etats-Unis, le Royaume-Uni, impliquant le Canada, l'Australie et la Nouvelle-Zélande, régit toujours les écoutes en tous temps par les Etats-Unis, et ce, par des méthodes que la morale pourrait être appelée à réprouver… Gros pavé à ingurgiter en anglais, mais tellement révélateur…

### par Geneviève Moulard

## 41 Histoires extraordinaires de la guerre invisible


**Auteur :** Pierre-Alain Antoine
**Editeur :** Gérard Louis
**Taille :** 24 x17 cm, 254 pages
**Prix :** 20 €
**ISBN :** 978-2-35763-141-0

Les chroniqueurs et les livres d'histoire relatent les événements de guerre qui se voient mais plus rarement les manoeuvres secrètes qui souvent font changer l'issue d'un conflit. Cet art du secret et la désinformation que certaines puissances manient avec habileté pour tromper leurs opposants est la doctrine de la guerre invisible. Au début du XXIe siècle, en pleine mondialisation économique dans un contexte d'insécurité grandissant, le recours au renseignement et à l'espionnage est vital pour les Etats soucieux de préserver leur intégrité et la Liberté de leurs citoyens.

Dans cet ouvrage, l'auteur s'appuie sur *L'Art de la guerre*, oeuvre du général chinois Sun Tzu écrite autour du 5ème siècle avant J.-C. et prônant le culte du secret garant de la victoire pour expliquer la finalité des stratagèmes et des jeux de dupes utilisés par les protagonistes au cours des siècles.

Avec ses 41 histoires (presque) méconnues de la guerre invisible, parfois de la Guerre Electronique, l'auteur révèle certains éléments gardés secrets pendant plus de soixante ans, tels le Radiogramme de la Victoire du 3 juin 1918 ou le décodage des machines allemandes *Enigma* et *Lorenz* de 1938 à 1945. La recherche discrète des intentions de l'ennemi durant la Guerre froide n'a pas été laissée de côté, pas plus que les manoeuvres occultes et les plans stratégiques d'intoxication découverts à la réunification des deux Allemagne.

Un livre qui étonnera peut-être….

## Les missions spéciales pendant la Première Guerre mondiale


**Auteur :** Olivier Lahaie
**Editeur :** Histoires & Collections
**Pages :** 24 x 15,2 cm, 223 pages
**Prix :** 17 €
**ISBN :** 978-2-35250-504-4

Lors de la Première Guerre, des agents secrets étaient déposés par avion derrière les lignes allemandes. Il s'agissait d'acquérir du renseignement sur l'adversaire (et parfois de saboter ses voies ferrées). Leur particularité résidait dans le fait que les agents étaient mis en place derrière les lignes ennemies par voie aérienne de nuit … Une innovation certes, mais qui était surtout un véritable défi technique et humain, en ces temps où l'aviation militaire en était encore à ses balbutiements. Ces missions furent organisées dans le plus grand secret. Les agents étaient souvent des douaniers et des soldats anonymes mis en place par des pilotes casse-cou (tels les fameux Védrines, Guynemer ou Navarre et bien d'autres As français encore).

Cent ans après les faits, une étude précise de ces missions spéciales restait à mener. L'auteur de ce livre, a décidé de combler ce vide historiographique. Docteur en histoire moderne, le lieutenant-colonel Olivier Lahaie a été longtemps attaché au Service Historique de la Défense à Vincennes ainsi qu'à Saint-Cyr-Coëtquidan comme chef du département Histoire et Géographie et chercheur au centre de recherches

## La guerre des scientifiques


**Auteur :** Jean-Charles Foucrier
**Editeur :** Perrin
**Pages :** 24 x15,2 cm, 440 pages
**Prix :** 24 €
**ISBN :** 978-2-262-06793-9

Dans l'enfer de la Seconde Guerre mondiale, alors que le monde est martyrisé par les combats, les maladies, le rationnement et l'angoisse, des hommes et des femmes se battent pour trouver des solutions. Ils n'utilisent pas d'armes et portent rarement l'uniforme. Leurs recherches se mènent loin des champs de bataille, dans le secret des laboratoires ou des bureaux militaires. Ce sont des scientifiques, qui le plus souvent ont décidé volontairement d'apporter leur aide à l'effort de guerre. Certains anoblissent l'intelligence humaine, en soulageant les souffrances avec de nouveaux vaccins et remèdes. D'autres la pervertissent en infligeant le mal sur les champs de bataille ou dans les camps de la mort en conduisant des expérimentations pseudo-scientifiques. La plupart se contentent de résoudre avec satisfaction des problèmes complexes. De la recherche médicale aux prémices de la bombe atomique, du décryptage d'*Enigma* à la bataille des ondes, *La Guerre des scientifiques* est le fruit de nombreuses années de recherches et de l'exploitation de sources inédites qui dresse avec justesse le portrait des soldats de cette armée des ombres méconnue.

Jean-Charles Foucrier est docteur en histoire contemporaine de l'université de Paris-Sorbonne. Son livre devra se trouver dans toutes les bibliothèques des membres de Guerrelec. A lire absolument.

www.guerrelec.fr

## Les sociétés membres de Guerrelec

**• ATOS • Rafaut • Airbus Défense • Arinc SA • Arpège SAS • Bertin • DCI • Docaret • Ineo Défense • Lacroix Défense et Securité • MBDA Systems • Thales DMS • Thales Sixt**

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

**Réalisation et impression : Scan Emotion**

**Ont collaboré à cette édition : Pierre-Alain Antoine, Pierre Grandclément, Geneviève Moulard, Jean-François Sulzer, Thomas Withington.**