GAZETTE CASSIC

Collectif des **A**nciens des **S**ystèmes de **S**urveillance, d'**I**nformation et de **C**ommunications

Porte-parole du CASSIC et rédacteur de la Gazette CASSIC :
Jean BIBAUD – jean.bibaud@wanadoo.fr – 06.62.80.46.09

Édition n° 2 – décembre 2021

Bienvenue à bord de cette nouvelle année 2022 !

Votre "*compagnie Air CASSIC*" vous remercie de votre confiance et vous souhaite beaucoup de joie, de sérénité et d'apaisement... et bon vol qui va durer 365 jours.
C'est parti pour le décollage !
Le plan de vol déposé pour ce voyage mémorable est composé de bonheur, de réussite, de santé et d'amour à savourer sans modération ! Bon vol à toutes et tous !

Éditorial

Cher(e)s ami(e)s,

Cette seconde édition de la Gazette du CASSIC (***C**ollectif des **A**nciens des **S**ystèmes de **S**urveillance, d'**I**nformation et de **C**ommunications*) **tient compte des remarques et suggestions de la toute première de septembre 2021.**

Elle est une fois encore relativement chargée. Et pour cause… Ce monde des SSIC qui nous concerne en premier chef (*c'est notre culture de SSIC'Men*) est un vaste domaine en perpétuel évolution technologique, structurelle et organisationnelle. C'est la raison pour laquelle il prend une telle place dans cette seconde édition, accent qui sera mis en avant à l'avenir qu'à l'occasion d'évènements intéressants seulement. L'objectif est de rester le plus possible dans le "coups" vis-à-vis de nos camarades qui œuvrent dans ce milieu de plus en plus complexe : certains le qualifient de "guerre des étoiles". Essayons donc d'acquérir le minimum d'informations indispensables au dialogue que nous pourrions avoir avec les plus jeunes et surtout avec nos relations extérieures de toutes natures.

À votre demande, deux nouvelles rubriques apparaissent dans cette édition, "Quid des Membres du CASSIC" (*memoriam, heureux évènements, messages personnels*…), et "Un peu d'humour". À vous toutes et tous d'apporter de l'eau au moulin pour faire vivre non seulement ces deux rubriques, mais aussi toutes les autres. Cette gazette est le lien essentiel qui nous unit. Nous devons donc le nourrir.

Enfin, un de nos camarades juge que le logo du CASSIC couché sur la première édition de la Gazette (*et réitérer sur celle-ci*) lui paraît "trop chargé". Je vous propose donc de bien vouloir prendre position (*définitivement*) sur l'une des propositions faites en annexe n° 1 ci-jointe. Vous pouvez également faire d'autres propositions. Merci d'avance.

Le prochain rassemblement du CASSIC, évènementiel contrarié jusqu'alors par la pandémie de la COVID 19, permettra d'évaluer la viabilité de notre collectif et surtout des moyens nécessaires au

maintien, voire à l'amélioration de nos relations amicales (*la Gazette, nos échanges et nos rencontres, nos actions, la mémoire, l'avenir…*). En accord avec l'ACMA, il est fixé le jeudi 12 mai 2021 à la Chapelle Mémorial de l'Aviation, à Lescar. La rubrique suivante "Infos Générales CASSIC" vous livre l'essentiel de ce rassemblement et vous invite à vous manifester si vous souhaitez y participer.

Bonnes fêtes de fin d'année, et Meilleurs vœux 2022 à vous et vos familles.
Bonne lecture.
Bien amicalement.

Votre rédacteur et porte-parole Jean BIBAUD :

- Courriel : jean.bibaud@wanadoo.fr (*contact à privilégier*)
- Téléphone : 06.62.80.46.09

Infos CASSIC

La gazette CASSIC

Le retour d'expérience de la première édition a été marqué par huit remarques :

- Simplification du logo CASSIC apparaissant encore sur la première page de cette édition n° 2, logo jugé trop chargé. Il vous est donc demandé de bien vouloir prendre position (*définitivement*) sur l'une des propositions faites en **annexe 1 ci-jointe**.
- Recours le plus largement possible au renvoi en annexes des textes importants afin que l'essentiel des informations soit seulement couché dans le corps de la gazette. Il sera également fait appel à des renvois vers des informations complémentaires vers d'autres sources grâce à des QR Code et des adresses Web (*par simple clic*).
- Approbation (*aucune remarque en retour de l'édition N° 1 de la Gazette*) de la Charte du CASSIC. Elle est donc "virtuellement" validée.
- Diffusion d'un annuaire numérique des membres du CASSIC très controversée. Il est question de sécurité et de protection des informations vis-à-vis d'Internet et de véracité quant au suivi dans le temps de cet annuaire (*mises à jour difficiles sans suivi de cotisations, sans groupes régionaux*...). Une solution pourrait satisfaire la grande majorité, à savoir que le porte-parole du CASSIC qui tient à jour pour l'instant cet annuaire ("*dans son jus*"), puisse renseigner ponctuellement un membre du CASSIC (*à sa demande*) sur tel ou tel autre membre, ou groupe de membres. À vous toutes et tous de faire remonter les infos vers le rédacteur de la gazette. Ce point reste à discuter lors de notre prochain rassemblement.
- Privilège donné aux articles et reportages des membres du CASSIC, ce qui est prioritairement pris en compte à condition qu'ils soient adressés (*et exploitables*) au rédacteur de la gazette : un seul article reçu pour cette édition n° 2.
- Intégration d'une rubrique humoristique, ce qui est réalisé dans cette édition n° 2. Là encore, à vos "plumes" !
- Intégration d'une rubrique pour les évènements heureux et malheureux, ce qui est réalisé dans cette édition n° 2. À vous toutes et tous de faire remonter les infos vers le rédacteur de la gazette.
- L'organisation du prochain rassemblement du CASSIC se déroulera en mai 2022. Le jeudi 12 mai 2022 convient le mieux que le 19 également proposé. En accord avec l'ACMA, cette date est confirmée : reste plus qu'à l'organiser (*ordre du jour à peaufiner, prestations à définir dans le détail*…).

N'oublions pas les principaux objectifs de cette gazette CASSIC : fédérer, fidéliser, donner un sens aux échanges, valoriser la culture collective, partager des informations, préparer et organiser un rassemblement ou un évènement…

Effectif / Memoriam

Memoriam

Chers amis,

Nous avons été touchés en apprenant la disparition de Daniel, Jeanine, Françoise, Émilie, Michel… Toutes nos pensées et nos souvenirs vont vers eux, et leur gentillesse va nous manquer à tous. Nous partageons le chagrin d'Odile, Roger, Émile, Chantal, Laure… et les assurons de notre soutien.

Daniel FAURE est décédé le 18 septembre 2021. Daniel est né le 7 avril 1946 à Ruffec (*16700*). Major et réserviste, exploitant des transmissions, il était membre de l'ANATC / Gr 003 FNAM depuis 2012. Durant sa brillante carrière militaire dans l'armée de l'air et de l'espace, il fut muté hors métropole, entre autres affectations dans l'hexagone, à : Djibouti de 1965 à 1967 et de 1972 à 1974, au Maroc de 1989 à 1992, et dans le Golfe en 1995. Il était Titulaire de la Reconnaissance de la Nation depuis 1997, et décoré de la Médaille Militaire. Nos très sincères condoléances vont à son épouse, Odile, et à toute sa famille.

Jeanine GOUBERN est décédée en octobre 2021 : épouse de Roger GOUBERN (*93 ans en janvier 2022 – Adhérent ANATC / Gr 003 FNAM depuis*

1986). Nous avons eu le grand plaisir de côtoyer Jeanine lors de nos réunions et nos rassemblements de l'ANATC, toujours souriante et de bonne humeur. Nos sincères condoléances vont à Roger, son époux, et à toute sa famille.

Françoise LE CORRE est décédée le 30 juin 2021 : épouse d'Émile (*dit Mimile*) LE CORRE (*77 ans en novembre 2021 – Adhérent ANATC depuis 2001*). Nous avons eu le grand plaisir de côtoyer Françoise lors des rassemblements du Groupe régional Centre Ouest au sein duquel elle participait très activement à leur organisation (*et de l'administration de ce Gr CO-ANATC*) au côté de Mimile, toujours souriante et très engagée dans l'action. Nos sincères condoléance vont à Émile, son époux, et à toute sa famille.

Mme Émilie GROLIER est décédée le 29 octobre 2021 à l'âge de 96 ans, à son domicile de Sarcelles (*Val-d'Oise*). Depuis le décès de son époux en 1978, André GROLIER, elle avait maintenu le lien en s'étant portée adhérente de l'ANATC. Nos sincères condoléances vont à Mme Chantal GROLIER, sa fille, et à toute sa famille.

Michel MENAND (*M4E – né le 29/11/1944 à Rochefort-sur-Mer*) est décédé le 24 novembre 2021. Lieutenant-colonel et réserviste, technicien des transmissions formé à Rochefort-sur-Mer, il était membre de l'ANATC depuis le 14/12/1992. Les dernières affectations de sa brillante carrière militaire dans l'armée de l'air et de l'espace, furent Commandant de l'ET 00.804 (*Aix en Provence*) – Saint-Denis de La Réunion - Chef de la STB 82.103 de Cambrai - Commandant en second du GT 10.803 de Cenon. Il était Titulaire de la Reconnaissance de la Nation, et décoré Chevalier de l'ONM et Chevalier de la LH. Nos très sincères condoléances vont à sa fille, Laure, et à toute sa famille.

Prochain rassemblement du CASSIC.

En accord avec l'ACMA, **le rassemblement du CASSIC, réservé à ses membres et ceux de l'ACMA,** conjoint(e)s compris(e)s, **se déroulera à la Chapelle Mémorial de l'Aviation et du Camp Guynemer** (*route de l'Aviation – RD 289 – 64230 Lescar*)**, le 12 mai 2022, de 10h00 à 17h00**.

Le programme retenu à ce jour est le suivant :

- 10h00 – Accueil et visite de la Chapelle Mémorial
- 10h30 – Discussions (*Organisation du CASSIC – Gazette CASSIC - Archives ANATC – Drapeau ANATC / Gr 003 FNAM – Relations CASSIC / ACMA - Adhésions à l'ACMA…*)
- 11h30 – Dépôt de gerbe au pied de la stèle ANATC / GR 003 FNAM suivi de la remise du drapeau ANATC / GR 003 FNAM à la Chapelle Mémorial de l'Aviation
- 12h15 – Déjeuner dans un restaurant (*25 € / personne*), à moins de 4 km de la Chapelle
- 15h00 à 17h00 – Visite ou activité (*en cours de définition, au plus près du restaurant*)

L'hébergement des participants sera libre et à leur charge tout entière.
Deux dîners en commun seront proposés, la veille (*11 mai 2022*) et en fin d'après-midi du rassemblement (*12 mai 2022 à partir de 19h00*) dans un restaurant dont les coordonnées seront précisées plus tard (*participation actuellement envisagée entre 20 et 25 € / personne et par dîner*).

Le paiement de la participation et de ce(s) dîner(s) s'effectuera à l'arrivée des participants à la Chapelle de l'Aviation, le 12 mai 2022 (*par chèque à l'ordre de Jean BIBAUD*).

Les personnes désirant participer à ce rassemblement avec ou sans leur conjoint(e) sont invitées à se manifester auprès de Jean BIBAUD d'ici fin janvier 2022. Un bulletin d'inscription sera ensuite adressé à toutes et tous, bulletin qui détaillera l'ordre du jour du rassemblement et qui devra être adressé en retour (*dûment rempli*) au porte-parole du CASSIC, Jean BIBAUD, avant 31 mars 2022.

Vous y êtes attendus nombreux.

Reportage(s)

Cette rubrique consacrée aux reportages des activités des membres du CASSIC (*en groupe ou pas, avec photos si possible*), s'agissant de sorties, de manifestations, de visites, de retrouvailles, d'expériences personnelles ou collectives peu ordinaires, de découvertes…doit absolument se développer. Elle est essentielle par le fait qu'elle caractérise incontestablement notre dynamisme collectif. Alors, qu'attendez-vous ?

Armée de l'air et de l'espace

Prise de commandement du CEMAAE

La cérémonie de la prise de commandement du GAA Stéphane MILLE (*ayant pour surnom : Milou*), nouveau chef

Sa prise de fonction en vidéo

d'état-major de l'armée de l'air et de l'espace a eu lieu le 10 septembre 2021 sur la base aérienne de Villacoublay. La vidéo de cette cérémonie est accessible via le QR Code ci-avant.

Le GAA Stéphane MILLE a pour devise "Tant qu'on n'a pas tout donné, on n'a rien donné" (*de Georges GUYNEMER*).

Organigramme de l'Armée de l'Air et de l'Espace

L'organigramme de l'armée de l'air et de l'espace (*AAE*) est accessible soit via le QR Code ci-contre, soit en cliquant sur le lien Internet également ci-après : www.air.defense.gouv.fr/armee-de-lair-et-de-lespace/fiche/organisation

Les officiers généraux hors structure commandement AAE sont :

- Le GAA Philippe LAVIGNE – OTAN (*Organisation du Traité de l'Atlantique Nord*) - Commandant suprême allié Transformation à Norfolk
- Le GAA Éric AUTELLET– EMA (*État-Major des Armées*) - Major général des armées
- Le GCA Fabien MANDON – MINARM (*ministère des Armées*) - Chef du cabinet militaire
- Le GCA Luc RANCOURT – MINARM - Directeur général adjoint des relations internationales et de la stratégie
- Le GCA Pascal DELERCE – OTAN – Commandant adjoint du commandement Air de l'OTAN à Ramstein
- Le GCA Vincent COUSIN – PM (*Premier Ministre*) – Secrétaire général adjoint de la défense et de la sécurité nationale
- Le GDA Laurent MARBOEUF – EMA – Officier général des relations internationales militaires EMA
- Le GDA Xavier BUISSON – EMA – Commandant supérieur des forces armées en Guyane et commandant de la Base de Défense Guyane
- Le GDA Éric CHARPENTIER – EMA – Adjoint directeur de projet
- Le GDA Stéphane DUPONT – EMA – Commandant des forces françaises stationnées à Djibouti
- Le GDA Étienne PATY – EMA – Directeur du centre interarmées de concepts, de doctrine et d'expérimentation
- Le GDA Didier TISSEYRE – EMA – Officier général commandant de la cyberdéfense EMA
- Le GDA Jean-Marc VIGILANT – EMA – Directeur de l'École de guerre
- La GDA Véronique BATUT – MINARM – Secrétaire générale de la garde nationale et du Conseil supérieur de la réserve militaire
- Le GBA Franck MOLLARD – MINARM – Directeur du bureau enquête accidents pour la sécurité aéronautique d'Etat
- Le GBA Stéphane VIREM – MINARM – Directeur de la sécurité aéronautique d'Etat

Pour plus d'informations concernant l'armée de l'air et de l'espace (*présentation, missions, moyens, défis, traditions, presse, ambassadeurs, dossiers, à la une…*), cliquez sur le lien ci-après : https://www.defense.gouv.fr/air

À l'ère des opérations multi-milieux et multi-champs (*M2MC*)

Les opérations multi-milieux et multi-champs, également nommées opérations multi-domaines, sont une vision conceptuelle de la guerre de demain et des défis auxquels les armées devront faire face. Depuis quelques années, l'armée de l'Air et de l'Espace (*AAE*) a initié une réflexion sur le sujet. C'est l'un des concepts phares d'aujourd'hui : "Réfléchir encore et encore à la guerre dite de haute intensité".

Cet article fait l'objet de l'**annexe n° 2 ci-jointe**

SYRACUSE 4

L'objectif du programme Syracuse 4 est de permettre le maintien de la permanence des communications en tout temps (*paix, crise ou catastrophe majeure*), grâce à une nouvelle génération de satellites militaires français de télécommunication en orbite géostationnaire.

Cet article fait l'objet de l'**annexe n° 3 ci-jointe**.

Les armées

Sous-marin Barracuda, blindés, avions, frégates… ce que nos armées doivent recevoir en 2022

La défense tricolore doit une fois de plus s'étoffer, en 2022. Le budget du ministère des Armées va bondir de plus de 4%, à 40,9 milliards d'euros, conformément à la loi de programmation militaire 2019-2025, selon le projet de loi de finances publié par le gouvernement. Pour la quatrième année de

suite, l'enveloppe consacrée à la défense augmente de 1,7 milliard d'euros, comme l'avait déjà annoncé mi-septembre 2021 la ministre des Armées Florence Parly. Hors de ce périmètre, les crédits de la mission "Anciens combattants" continuent de s'éroder *(-3%, à 2,02 milliards d'euros*), conséquence de l'avancée en âge de cette population.

D'une enveloppe globale de 295 milliards d'euros sur sept ans, la LPM 2019-2025 prévoit une nette hausse du budget défense après des années de baisse. Mais les augmentations les plus importantes (*+3 milliards par an*) sont prévues à partir de 2023, soit après la prochaine élection présidentielle. En 2022, les grands programmes d'armement devraient voir leur budget augmenter de 6,5% à 8,1 milliards, dont 100 millions d'euros pour le plan de soutien à la filière aéronautique. Côté livraisons, les armées recevront notamment en 2022 245 blindés de nouvelle génération (*Griffon, Jaguar, Serval*), 8 hélicoptères NH90 pour l'armée de Terre, une frégate de défense aérienne, un deuxième sous-marin Barracuda, un bâtiment ravitailleur, 6 avions de transport et de ravitaillement et 5 satellites, dont le premier satellite de communications militaires Syracuse 4.

Les dépenses d'entretien des matériels augmenteront de 8,3% pour atteindre 5,1 milliards d'euros. Celles consacrées à la dissuasion nucléaire connaîtront une hausse de 6,6% sur un an. Un milliard d'euros sera dédié à l'innovation de défense.

Côté ressources humaines, 26.200 personnes seront recrutées en 2022, et quelque 450 emplois supplémentaires seront créés, essentiellement pour le renseignement et la cyberdéfense. Le ministère poursuivra par ailleurs la simplification de la rémunération des militaires, qui comptait auparavant quelque 170 primes et indemnités différentes.

Le montant des provisions destinées à financer les opérations extérieures françaises (*Sahel, Levant*...) est de nouveau fixé à 1,1 milliard d'euros, ainsi qu'à 100 millions pour les opérations intérieures (*Sentinelle, Résilience*).

SSIC d'aujourd'hui

La DA d'aujourd'hui (*juin 2021*)

La Défense Aérienne française est née dans les années 1950.
Ses outils essentiels étaient les Stations Maître Radar (*SMR*) de l'époque dont on ne savait exploiter la détection que localement ; les performances du radar étant, en outre, modestes, le dispositif comportait une quinzaine de stations pour couvrir le territoire national. Enfin, la situation aérienne (*menace*...) était présentée à l'échelon de décision avec un retard de plusieurs minutes, car il fallait la "raconter" verbalement après plusieurs relais téléphoniques.
En l'espace de 50 ou 60 ans, on a découvert le langage binaire, inventé les ordinateurs et les moyens de communication ont fait un bond fantastique ; de son côté, l'Armée de l'Air et de l'Espace a maintenu en service et modernisé presque tous ses grands radars d'infrastructure et les radars moins puissants de ses terrains tandis que la Défense Aérienne a largement utilisé les améliorations techniques de leur exploitation (*ordinateurs et transmissions*) afin d'accomplir son plan d'équipement.

Cet article fait l'objet de l'**annexe n° 4 ci-jointe**

Les Contrôleurs et contrôleuses aériens

En juin 2020, le trafic aérien en France a chuté de 84,51 % par rapport à 2019, selon les données officielles. Au mois d'avril de la même année, la baisse était même de 93,28 %. Cela a touché de plein fouet les compagnies aériennes du monde entier, et du même coup l'ensemble de l'industrie aéronautique et la sous-traitance. Cette période de "vaches maigres" 2020 et 2021 n'a cependant pratiquement pas touché le monde des contrôleurs/contrôleuses aériens en France. Faisons donc connaissance avec ce "monde de l'ombre", qu'il soit civil ou militaire.
Le contrôleur aérien ou la contrôleuse aérienne (*également appelé aiguilleur/aiguilleuse du ciel*) guide les avions, contrôle et assure la sécurité et la fluidité de l'espace aérien. Ingénieur de contrôle de la navigation aérienne (*ICNA*) dans le civil, il peut également exercer au sein de l'armée de l'air et de l'espace (*AAE*), de la marine ou de l'armée de terre (*ALAT*).

Cet article fait l'objet de l'**annexe n° 5 ci-jointe**.

Contrôle aérien des drones

Le contrôle du trafic aérien des drones sera automatisé.
La mise en place d'un trafic aérien organisé et contrôlé s'impose désormais comme un préalable indispensable pour assurer le décollage commercial des drones.

Dans une étude, PWC (*Price Waterhouse Coopeers*) a évalué en 2020, à 127 milliards de dollars, le marché des activités liées aux drones mais cite en bonne place, parmi les conditions sine qua non à remplir, l'organisation sécurisée du trafic

des drones dans l'espace aérien. La réglementation, en effet, ne peut suffire à faire évoluer sans risque des drones au-dessus de nos têtes : il faut que chaque appareil puisse se faire reconnaître des autres aéronefs et s'inscrire dans le grand-huit d'une régulation du trafic qui ne pourra être qu'automatisée.

Cet article fait l'objet de l'**annexe n° 6 ci-jointe**

Guerre électronique / informatique, une guerre plus que jamais présente…

Depuis un peu plus d'un siècle, ce nouveau mode de guerre "technologique" s'amplifie et n'épargne pratiquement plus personne. On parle de guerre électronique, de cyber-attaque et de cyberdéfense, de cyber-guerre et de harcèlement électromagnétique, de renseignement d'origine électromagnétique… bref, une nouvelle "guerre mondiale", sournoise, est bel et bien là n'épargnant personne.

Cet article fait l'objet de l'**annexe n° 7 ci-jointe**.

Faisceau hertzien (*FH*) : comment ça marche ? points positifs et négatifs.

L'ADSL et la fibre sont les moyens de connexions les plus connus. Parfois coûteux, inaccessibles en zone rurale ou montagneuse, non fiables ou au débit ralenti, il peut être intéressant de porter sa réflexion vers une autre technologie. **La technologie du Faisceau Hertzien (*FH*) est une bonne solution lorsque les besoins du professionnel en matière de connectivité doivent être plus puissants, en zones géographiques à risques ou "blanches".** On détaille à l'**annexe n° 8 ci-jointe**, son mode de fonctionnement, les facteurs perturbateurs, ses avantages et ses inconvénients, son utilité pour les professionnels ou encore son histoire. Le faisceau hertzien (*FH*) est proposé par des fournisseurs au sein de leurs offres et services.

Système de transmission par le sol

Un **système de transmission par le sol**, ou **TPS** en abrégé (***T**ransmission **P**ar **S**ol*) et parfois appelé "tellurophone" (*de tellurique*), est un système de communication en milieu souterrain utilisant des ondes électromagnétiques transmises par le sol continu.

Le TPS, le système Nicola, le système FAUCHEZ… sont tous des systèmes de radiocommunication utilisés notamment :

- en spéléologie, en particulier pour les opérations de secours ;
- pour des applications militaires ;
- pour des applications radio-amateurs ;
- pour des mines souterraines.

L'**annexe n° 9 ci-jointe** détaille ce type de transmission

Nouvelles technologies

Qu'est-ce que le "MÉTAVERS" ?

"Métavers" est le successeur de l'internet mobile présenté par Mark Zuckerberg (*cofondateur du site et du réseau social Facebook*) en juillet 2021. Peu après, le 18 octobre 2021, Facebook a annoncé le recrutement de quelque 10.000 personnes en Europe sur les cinq prochaines années pour développer ce nouvel univers virtuel.

Le terme "métavers" est une simple contraction des mots "méta" (*qui fait référence à une vision d'ensemble*) et "univers". Il est issu de romans de science-fiction du début des années 90, décrivant des mondes virtuels dans lesquels les individus peuvent interagir, souvent à l'aide d'accessoires comme des casques de réalité virtuelle. Ainsi, tout monde virtuel dans lequel un individu est invité à se créer un double numérique peut être considéré comme un "métavers".

L'**annexe n° 10 ci-jointe** détaille ce nouvel univers.

Mémoire - Souvenir

Antoine de Saint-Exupéry

Saint-Exupéry est un personnage connu de tous, et avec lui c'est tout l'imaginaire nostalgique des premiers temps de l'Aéropostale qui ressurgit, et reprend vie.

Saint-Exupéry, ou mieux, "Saint-Ex", a été présenté comme un "paladin", un "chevalier errant" comparable aux héros de la guerre, car il faisait partie d'une nouvelle génération d'aviateurs attelée à une besogne immense, la création de l'Aéropostale. Il est également qualifié de "camarade le plus exquis" et de "pilote le plus casse-cou de la ligne", c'est à la fois un "enfant" et un "héros" dont l'aspect le plus pur serait encore le "côté insouciant". Son surnom de "Pique la lune" lui est resté, non seulement en

raison de son nez en trompette mais aussi d'une tendance certaine à se replier dans son monde intérieur.

Voir la suite dans l'**annexe n° 11 ci-jointe**

1912, il y aura bientôt 110 ans.

Roland GARROS va obtenir son premier très grand succès à Angers, en juin 1912. Le Grand Prix de l'Aéroclub de France couronnait le vainqueur du circuit d'Anjou. Il s'agissait d'accomplir sept fois et en deux jours, le dimanche 16 et le lundi 17 juin 1912, le triangle Angers-Cholet-Saumur, soit un peu plus de 1.100 kilomètres. Roland GARROS, qui se présente avec son Blériot personnel (*il a depuis longtemps mis un point d'honneur à ne voler que sur ses propres machines*), est opposé aux trente-trois meilleurs pilotes du monde, soutenus par tous les moyens possibles des firmes industrielles les plus puissantes du monde. Si quelques courageux ont pris leur envol malgré le vent et la tempête, GARROS resta bientôt le seul en l'air avec le jeune BRINDEJONC-DES-MOULINAIS qui, malheureusement pour lui, a franchi la ligne d'arrivée en dehors du temps réglementaire. Roland GARROS est donc le seul à terminer les épreuves du premier et du deuxième jour. Les journalistes ne l'appellent plus désormais que "le champion des champions".

L'**annexe n° 12 ci-jointe** vous dévoile les valeurs exceptionnelles de cet homme

Info(s) de la FNAM

Mise en vente du Domaine de la Grande-Garenne

En application de ses statuts, l'assemblée générale de la Fédération Nationale André Maginot a été appelée à se prononcer le 8 septembre 2021 à Nancy sur la résolution suivante (*communiqué du 13 septembre 2021 du général RIDEAU, Président de la FNAM*) :

« *À la suite du vote en assemblée générale le 12 septembre 2017 à Dijon, il a été réalisé, par les Domaines, une évaluation de la propriété de la Grande-Garenne. Les Domaines ont évalué cette propriété d'environ 98 ha (sans y inclure l'EHPAD) à 2.800.000 € avec une marge de plus ou moins 10%.*
La Grande-Garenne est quasiment fermée depuis mars 2020 par suite des confinements successifs.
Au vu des circonstances et de la faible visibilité économique et sociale du devenir de ce domaine, le conseil d'administration réuni le mai 2021 vous propose d'accepter la vente du domaine de la Grande-Garenne, hors EHPAD, sur la base de l'évaluation des Domaines de 2.800.000 €.
A cet effet, l'assemblée générale donne au Président de la FNAM, les pouvoirs :

- *pour arrêter l'activité du domaine à toute date antérieure au 1er janvier 2023 ;*
- *pour vendre le domaine au prix actuel de 2.800.000 €, avec marges de plus ou moins 10% ;*
- *aux effets ci-dessus, d'accomplir toutes démarches administratives ou autres, négocier et signer tous mandats, et, avec tous pouvoirs de délégation, faire tout ce qu'il jugera utile et nécessaire.* »

Cette résolution a été adoptée à la majorité, l'EHPAD Résidence André Maginot n'est d'aucune manière concernée par les dispositions adoptées. Précisons que la diminution du nombre d'anciens combattants et le lourd déficit de l'établissement dû à une trop faible fréquentation en sont les deux principales causes.

Voilà une nouvelle page de notre histoire (*celle de l'ANATC / Gr 003 FNAM*) qui se ferme. Cette vente du domaine de la Grande-Garenne a fait l'objet d'un article dans le journal local "LE BERRY Républicain" du 05 octobre 2021.

Info(s) de l'ACMA

Vœux 2022 de Noël POTIER, président de l'ACMA en **annexe n° 13 ci-jointe**

En bref

En **annexe n° 14 de cette gazette**, l'ACMA rend hommage à Louis BLERIOT en participant activement à la mise en place d'une stèle près de l'aéroport de Pau, et au colonel Jean ADIAS, qui fut un pilote hors norme de l'armée de l'air.

Où en est l'agrandissement de la chapelle mémorial de l'aviation à Lescar ? Après accord par le service de l'urbanisme le dossier est entre les mains du Syndicat du Haut Ossau qui en est le propriétaire. Il devrait apporter son aide en fournissant les matériaux pour la construction.

La remise du drapeau de l'ANATC à l'ACMA est prévue le 12 mai 2022

L'Amicale de la Chapelle Mémorial de l'aviation possède des récits sur la carrière du colonel Jean ADIAS (*mémoire*), soit un total de plus de 280 pages réparties en 7 fascicules. Ces fascicules sont en vente sur commande exclusivement à la chapelle. Les bénéfices en sont reversés aux missionnaires de Betharran pour le Vietnam (*vœux du colonel ADIAS*)

Le livre Pau aérodrome est toujours en vente à la chapelle au prix de 14 € plus frais de port.

Publication(s)

Magazine Air Actualités

Profitez des actualités de l'armée de l'air et de l'espace. Le CASSIC vous invite à souscrire un abonnement à ce magazine mensuel très bien illustré.

Ce type de coupon d'abonnement est à retourner à : **ECPAD – Service abonnements – 2/8 rue du Fort d'Ivry – 94205 Ivry-sur-Seine Cedex**.
Vente possible au numéro : contacter l'**ECPAD** ou **01.49.60.52.44** ou à :
routage-abonnement@ecpad.fr.

Tarif spécial réservé aux personnels et organismes de la défense, anciens militaires et moins de 25 ans. Il est conditionné à l'envoi d'un justificatif par le bénéficiaire.

Chèque à l'ordre de l'**agent comptable de l'ECPAD.**

Coupon d'abonnement

Nom :
Prénom :
Adresse :
Code postal :
Ville :
Téléphone :
E-mail :
Signature :

TARIFS (frais de port inclus)		
France		
6 mois (5 n°)	☐	20 €
	☐	16,75 € (tarif spécial)*
1 an (10 n°)	☐	34 €
	☐	30,40 € (tarif spécial)*
2 ans (20 n°)	☐	61 €
	☐	51,40 € (tarif spécial)*
DROM-COM**		
6 mois (5 n°)	☐	31,87 €
	☐	27,25 € (tarif spécial)*
1 an (10 n°)	☐	55,60 €
	☐	51,40 € (tarif spécial)*
2 ans (20 n°)	☐	103,90 €
	☐	93 € (tarif spécial)*
Étranger (hors-taxes)**		
6 mois (5 n°)	☐	36,70 €
1 an (10 n°)	☐	64 €
2 ans (20 n°)	☐	114,40 €

Un peu d'humour

A la demande de certains d'entre-nous, cette nouvelle rubrique "Un peu d'humour" est ouverte à toutes et tous : partageons nos histoires humoristiques !

Quoi de mieux que la campagne, la nature, rencontrer ceux qui la façonne… se détendre... En attendant notre très prochaine balade champêtre, voici quelques "blagounettes du cru" à l'**annexe n° 15 ci-jointe**

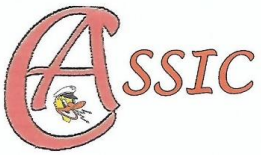
ANNEXE 1

Propositions pour du logo définitif de CASSIC logo

SVP, adressez le n° du logo que vous préférez au porte-parole du CASSIC d'ici fin janvier 2022. Vous avez également la possibilité de faire d'autres propositions le plus tôt possible (avant fin janvier 2022). In fine, le logo qui obtiendra le plus de voix sera définitivement retenu.

LOGO n° 1

LOGO n° 2



LOGO n° 3

LOGO n° 4

LOGO n° 5

LOGO n° 6

ANNEXE 2

À L'ÈRE DES OPÉRATIONS MULTI-MILIEUX ET MULTI-CHAMPS (*M2MC*)

LES OPÉRATIONS MULTIMILIEUX ET MULTICHAMPS, également nommées opérations multi-domaines, sont une vision conceptuelle de la guerre de demain et des défis auxquels les armées devront faire face. Depuis quelques années, l'armée de l'Air et de l'Espace (*AAE*) a initié une réflexion sur le sujet. C'est l'un des concepts phares d'aujourd'hui : "Réfléchir encore et encore à la guerre dite de haute intensité".

L'armée de l'Air et de l'Espace travaille sur le sujet depuis 6 ans avec l'US Air Force et la Royal Air Force. C'est-à-dire dès le moment où le général David L. Golfein, alors chef d'état-major de l'US Air Force, a annoncé que le C2 multi-domaines était l'un de ses objectifs pour son temps de commandement. C'est alors que le bureau Plans de l'état-major de l'armée de l'Air et de l'Espace a constitué une équipe de quatre personnes dirigées par le colonel Montaigne de Poncins qui s'appelle le Trilateral Strategic Steering Group (*TSSG*). Il est animé avec un colonel américain et un Wing Commander britannique. Deux aviateurs français sont détachés respectivement dans des structures équivalentes à Washington et à Londres. Ce TSSG a trois objectifs : développer la confiance entre les trois armées, l'interopérabilité technique, humaine et doctrinale. Il s'agit aussi de travailler ensemble sur l'Air Advocacy, c'est-à-dire la promotion de la puissance aérienne militaire.

Sur le plan purement AAE, trois groupes de travail ont été constitués sur demande de l'EMAAE en juillet 2020. Le contrat était de définir la vision Air et Espace du concept multi-milieux et multi-champs afin de la partager en interarmées. Le premier groupe de travail (*GT*), dirigé par le Commandement de la défense aérienne et des opérations aériennes (*CDAOA*), est axé sur le C2 (*Command and Control – commandement et conduite*). Il a pour objectif de définir comment planifier, commander et conduire les opérations multi-domaines. Le deuxième GT répond à la problématique de l'appui spatial et de l'intégration de l'espace aux opérations M2MC. Il est mené par le Commandement de l'espace (*CDE*). Le troisième GT est sous la responsabilité du Centre d'expertise aérienne militaire (*CEAM*). Il s'agit de répondre à la question : « *Quelles opérations allons-nous mener demain ?* ». La conclusion des réflexions menées par ces trois GT a permis de publier un document appelé "Concept exploratoire multi-domaines Air".

Basé sur la base aérienne 942 de Lyon-Mont Verdun, le nouveau Centre air de planification et de conduite des opérations (*CAPCO*), doté des plus récentes innovations technologiques, est opérationnel. C'est le fleuron de l'AAE en matière de C2 (*Command and Control*). En juin 2021, il a permis de conduire l'opération de projection de puissance "Heifara" en Polynésie française. À l'horizon 2040, le C2 Air devra être au rendez-vous du Système de combat aérien futur (*SCAF*).

Le volet spatial est un enjeu majeur dans tout le spectre des missions et contribue à toutes les opérations d'aujourd'hui et de demain. Drones à longue endurance, missiles de croisière, bombes guidées, communications longue distance, prévisions météorologiques précises, navigation, "Blue force traking" (*"Suivi de force bleu" = terme militaire désignant une capacité compatible GPS qui fournit aux commandants et aux forces militaires des informations de localisation sur les forces militaires amies et hostiles*), etc. Autant d'éléments qui seraient inopérants sans moyens satellitaires. L'espace est décisif pour assurer une supériorité en matière de renseignement mais aussi pour la conduite d'opérations complexes à distance, quand elles impliquent, par exemple, l'usage de drone ou de munitions guidées avec précision. En septembre 2019, le Commandement de l'espace (*CDE*) a été créé comme organisme à vocation interarmées relevant de l'AAE. Aujourd'hui, l'intégration du milieu extra-atmosphérique dans les opérations se fait à partir du Centre de commandement et de conduite des opérations spatiales (*C3OS*) du CDE, situé à Paris. Il agrège les données des unités tactiques spatiales que sont le Centre militaire d'observation par satellite (*CMOS*) et le Centre opérationnel de surveillance militaires des objets spatiaux (*COSMOS*). Le CDE collecte également des données en provenance de partenaires civils, des alliés et des services de renseignement. Le CMOS assure le recueil des besoins et l'ensemble des opérations de traitement des images hormis leur exploitation. Le COSMOS a en charge la surveillance permanente de l'espace extra-atmosphérique. Les aviateurs du COSMOS étudient les trajectoires des milliers de satellites en orbite au-dessus de nos têtes et des débris spatiaux.

En pleine montée en puissance, le CDE travaille avec la Direction de l'armement (DGA) sur le développement du système d'information spatiale SisNext, premier incrément du C4 (*Computerized Command, Control, Communications*) en mesure d'exploiter et de traiter les masses colossales de données spatiales. SisNext est un outil fondamental pour permettre une intégration au C2 pour faire du multi-domaine.

L’interarmées tel que pratiqué actuellement, c’est de l’ordre de la coordination et de la mise en cohérence. Si on opte pour le M2MC, il faudra passer au niveau supérieur : l’intégration. Ce concept novateur modifierait notre vision actuelle des armées aussi bien sur le plan organisationnel que sur le plan culturel.

Par ailleurs, les perspectives offertes par les technologies émergentes, notamment en matière de maîtrise de la circulation de l’information, d’aide à l’analyse des données et à la décision, grâce à l’intelligence artificielle, permettent d’ores et déjà d’envisager une réelle connectivité et une parfaite synergie de tous les acteurs.

Forte de son expérience, l’AAE a pris de l’avance en matière de réflexion stratégique sur les opérations multi-milieux et multi-champs mais avance prudemment et méthodiquement pour passer de la théorie à la pratique.

Concevoir la guerre de demain dans un environnement multi-domaine et préparer l’arrivée du SCAF (Système de Combat Aérien du Futur) sont au centre des préoccupations du Centre d’expertise aérienne militaire (CEAM). La préparation aux opérations multi-domaines et aux conflits de demain est dans le cahier des charges de l’Air Warfare Center, autre appellation du CEAM. Ainsi, les réflexions sur les opérations M2MC ont vocation à alimenter les études capacitaires mais aussi les exercices majeurs. En collaboration avec le CFA (*Commandement des forces aériennes de l’AAE*) et le CDAOA, la réflexion passe par des scénarios d’entraînement intégrant l’approche M2MC lors de la prochaine édition de l’exercice "Volfa" (***Exercice annuel national majeur et de haute intensité de l’armée de l’Air et de l’Espace incontournable pour la préparation au combat des forces aériennes, avec participation d’unités étrangères*****), et de la prochaine édition 2023 de l’exercice interarmées d’ampleur "Orion" orienté vers la haute intensité.**

ANNEXE 3

SYRACUSE 4

L'objectif du programme Syracuse 4 est de permettre le maintien de la permanence des communications en tout temps (*paix, crise ou catastrophe majeure*), grâce à une nouvelle génération de satellites militaires français de télécommunication en orbite géostationnaire.

SYRACUSE 4 (*SYstème de RAdioCommunication Utilisant un SatellitE, anciennement connue sous le nom de COMSAT-NG*) est un programme de télécommunications militaires par satellites géostationnaires destiné à remplacer les satellites Syracuse 3A et Syracuse 3B actuellement en orbite. Le projet Syracuse 4 est de développer, pérenniser, construire et placer en orbite opérationnelle 2 satellites géostationnaires.

La Direction générale de l'armement (*DGA*) a confié le développement de ces deux types de satellites au groupement Airbus Defence and Space (*plateforme Eurostar 3000*) et Thales Alenia Space (*plateforme SpaceBus Neo 100*), les deux maîtres d'œuvre de Syracuse 4.

Syracuse 4 développe des innovations pour améliorer les performances des communications des forces armées, parmi lesquelles de nouvelles antennes principales et de nouveaux centres de contrôle au sol, ainsi que des bandes de fréquences plus importantes (*Bande X : 8 -12,5 GHz, et Bande Ka : 26,5 - 40 GHz*) et un système antibrouillage, offrant des performances accrues en matière de capacités de communication, de flexibilité et de résistance au brouillage. La charge utile est identique pour les deux satellites. Le premier des deux beaux bébés (*Syracuse 4A et plus tard Syracuse 4B*) de 3 852 kilogrammes s'est envolé le 23 octobre 2021. Placé en orbite, Syracuse 4A a décollé de Kourou, en Guyane, à bord de la fusée Ariane 5 ECA.

Les deux satellites de télécoms doivent répondre d'une part à l'augmentation des débits liée à la numérisation croissante du champ de bataille et apporter la capacité SATCOM à de nouveaux utilisateurs, notamment les drones, les stations terrestres en mouvement et les porteurs aéronautiques. Leur durée de vie est évaluée à 15 ans.

Syracuse 4A, ou satellite 4A pour le diminutif, permettra aux armées françaises déployées partout dans le monde de communiquer en toute sécurité depuis des relais au sol, aériens, marins et sous-marins. Jusqu'à présent cette communication était assurée par les satellites de la génération précédente, Syracuse 3A et Syracuse 3B. Les deux compères étaient en service depuis 2007, il était temps pour eux de prendre leur retraite.

Le nouveau satellite 4A devrait permettre de multiplier par trois le débit de ses prédécesseurs. *« Il y a une loi presque mathématique d'augmentation régulière des volumes de data »*, souligne le colonel Stéphane Spet, porte-parole de l'armée de l'air et de l'espace, citant les besoins générés par les systèmes de commandement, la représentation des situations tactiques du terrain, la vidéo (*venant par exemple des drones Reaper déployés au Sahel*). Ou encore le traitement en temps réel des données venues de plusieurs endroits de la planète.

A terme, la France disposera de 400 stations capables de communiquer avec S4 depuis le sol, un aéronef, un navire ou un sous-marin, selon la Direction générale de l'armement (*DGA*). Le déploiement de ce satellite, bien que prévu de longue date, tombe à point nommé alors que Paris pousse son projet de souveraineté européenne en matière de défense. La France, qui dispose d'espaces maritimes souverains sur toutes les mers du globe, ne peut se passer d'une assise technologique puissante.

Outre son débit impressionnant, Syracuse 4A devrait également être capable de se protéger face à des attaques. Syracuse 4A est conçu pour résister aux agressions militaires depuis le sol et dans l'espace ainsi qu'au brouillage. En outre, il est équipé de moyens de surveillance de ses abords proches et est capable de se déplacer afin d'esquiver une agression.

La chose fait très science-fiction mais les risques sont bien réels. En juillet 2020, le commandement spatial américain avait accusé Moscou d'avoir conduit un test non-destructeur d'une arme antisatellite depuis l'espace. Et en 2017, le satellite espion russe Louch-Olympe avait déjà tenté de s'approcher du satellite militaire franco-italien Athena-Fidus. Une vraie guerre des étoiles.

Et, ultime détail sensationnel : S4 peut se protéger contre des impulsions électromagnétiques qui résulteraient d'une explosion nucléaire. Un détail qui n'en est pas un pour l'armée française, puisque la dissuasion nucléaire du pays repose en grande partie sur ses sous-marins. Si un adversaire est capable de modifier, pirater, endommager les communications avec les sous-marins, c'est la fin de la dissuasion.
L'expert en prolifération des armes Marc Finaud évoque au passage le risque potentiel venant de la « nébuleuse *de hackers, pirates, acteurs criminels ou terroristes qui pourraient se lancer dans une sorte de guerre des étoiles plus artisanale* ». Quant à la géopolitique spatiale, elle se tend un peu plus chaque année. On parle de guerre spatiale et ce risque-là est admis par tout le monde.

En plus d'améliorer les communications militaires, S4 va permettre à l'Hexagone de redorer son blason. Quelques semaines après l'humiliation reçue par l'Australie, qui a renoncé à un immense contrat de sous-marins français au profit de submersibles américains, fragilisant d'autant la puissance française en Indopacifique, le satellite S4 redonne une fierté à la bête blessée. *« Politiquement, c'est la mise en évidence que la France reste une puissance peut être moyenne, mais dont l'étendue d'action reste internationale »,* insiste le directeur de la Fondation pour la recherche stratégique (*FRS*) et spécialiste des questions spatiales Xavier Pasco. *« Elle a besoin de ce segment-là pour montrer qu'elle a les moyens de ses ambitions »,* ajoute Xavier Pasco. Cela crédibilise l'ensemble de son outil militaire, de même que sa capacité industrielle.

L'investissement, lui aussi, est astronomique. La Direction générale de l'armement (*DGA*) s'est engagée avec Thalès à hauteur de 354 millions d'euros pour le segment sol du système sécurisé de Syracuse 4. Un autre accord, conclu avec Airbus, s'élève à 117 millions d'euros. Il contribuera, pour sa part, à développer un nouveau portail de gestion centrale des différents systèmes de communications par satellites utilisés par les armées françaises. Dans son ensemble, le programme Syracuse représente un investissement total d'environ 4 milliards d'euros.
Avec ses 2 milliards d'euros d'investissements annuels dans le spatial militaire et civil, l'Hexagone reste loin du trio de tête : 50 milliards pour les Etats-Unis, 10 pour la Chine et 4 pour la Russie, selon des chiffres de 2020 du gouvernement français. Mais S4 permet à la France de rester dans le peloton de tête et confirme que Paris participe bien à la course aux armements.

ANNEXE 4

La DA d'aujourd'hui (*juin 2021*)

La Défense Aérienne française est née dans les années 1950.
Ses outils essentiels étaient les Stations Maître Radar (*SMR*) de l'époque dont on ne savait exploiter la détection que localement ; les performances du radar étant, en outre, modestes, le dispositif comportait une quinzaine de stations pour couvrir le territoire national. Enfin, la situation aérienne (*menace*...) était présentée à l'échelon de décision avec un retard de plusieurs minutes, car il fallait la "raconter" verbalement après plusieurs relais téléphoniques.
En l'espace de 50 ou 60 ans, on a découvert le langage binaire, inventé les ordinateurs et les moyens de communication ont fait un bond fantastique ; de son côté, l'Armée de l'Air a maintenu en service et modernisé presque tous ses grands radars d'infrastructure et les radars moins puissants de ses terrains tandis que la Défense Aérienne a largement utilisé les améliorations techniques de leur exploitation (*ordinateurs et transmissions*) afin d'accomplir son plan d'équipement.

Actuellement, tous les radars terrestres, de grande ou de courte portée, civils et militaires, sont connectés aux ordinateurs ; ceux-ci analysent la redondance des informations radar reçues et en élaborent une image panoramique présentant les vols sous la forme de symboles qui se déplacent sur des écrans plats ; on les appelle toujours des pistes. Les opérateurs peuvent interroger ces pistes avec leur souris pour obtenir instantanément des informations (*identité, altitude …*) afin s'exécuter leur mission de surveillance ou de contrôle. On n'exploite donc plus directement les échos analogiques recueillis par les radars, on "visualise" une situation aérienne synthétique, qu'on dénomme la "Visu", laquelle a évolué, elle aussi, puisque nous en sommes à la "Visu 5".
Précisons que si un avion de surveillance radar est en vol sur la zone, les autres avions et hélicoptères ne peuvent plus passer inaperçus en cheminant au ras du sol ou au creux des vallées ; autrefois on ne les décelait que très fugacement ou pas du tout.

Avec la "Visu 5" (*poste VISU 5 ci-contre*) :

- les consoles encombrantes des opérateurs sont remplacées par des "interfaces homme-machine" ergonomiques,
- les écrans monochromes des tubes cathodiques ont cédé la place aux écrans LCD sur lesquels les pistes apparaissent en couleur,
- un calculateur particulièrement puissant équipé d'un nouveau logiciel permet au CDC (*Centre de Détection et de Contrôle*) de se connecter à un maximum de 50 radars,
- la capacité de détection des CDC peut encore être complétée par les radars d'un CDC mobile déployé à l'endroit imposé par les opérations, ainsi que par les avions de surveillance radar, et par les radars du porte-avions et des frégates pour les espaces océaniques,
- les transmissions sol-air étant adaptées, un CDC peut contrôler n'importe quelle partie de l'espace aérien national et de ses approches.

Le résultat est le suivant :
- l'espace aérien national et ses approches maritimes sont parfaitement couverts,
- le dispositif fixe repose sur le Centre National des Opérations Aériennes (*CNOA*) de Lyon-Mont-Verdun, directeur tactique, et seulement sur trois CDC : Cinq-Mars la Pile, Lyon-Mont-Verdun et Mont-de-

Marsan (*VISU 5 Sud-Ouest ci-contre*) ; ils assument l'ensemble des missions de défense aérienne et contrôlent les mouvements aériens militaires,

- la situation aérienne établie par la DA selon les critères nationaux (*Ami, Menaçant, En détresse, Prioritaire*...) est transmise en temps réel, non seulement au CNOA, mais aussi au PC gouvernemental, et aux PC opérationnels Terre et Marine, jusqu'aux batteries de missiles sol/air et aux chars d'assaut modernes.

Ces nouvelles capacités techniques ont permis d'élargir la mission de défense aérienne aux espaces non conquis par les avions. Le CNOA assure en effet la surveillance des satellites au moyen du radar GRAVES.

Le Grand Réseau Adapté à la Veille Spatiale (*GRAVES – antennes GRAVES ci-contre*) est opérationnel depuis 2005. Il s'agit d'un radar français de conception nouvelle qui est associé à un système de traitement automatisé ; ce système entretient de façon autonome un catalogue des satellites et des débris en orbite basse (*moins de 1000 km d'altitude*) de la classe des Hélios, Spot et Ikonos survolant la métropole. L'antenne d'émission est située à 400 kilomètres de l'antenne de réception.

La couverture du ciel est donc parfaitement assurée, qu'il s'agisse de l'espace national, de ses approches ou d'un théâtre d'opérations. Et dans le cadre de l'interopérabilité, les moyens du commandement tactique ont aussi été améliorés et durcis.

Afin de s'élargir au système OTAN en Europe, la réalisation des centres ACCS de Lyon-Mont-Verdun, de Cinq-Mars la Pile et de Mont-de-Marsan sont en cours.

Pour conclure, on peut dire que si, en un siècle, les avions de combat ont évolué d'une façon prodigieuse, dans la moitié de ce temps, la Défense Aérienne est née et a atteint son plein épanouissement :

- détection de la menace ;
- transmission de celle-ci en temps réel ;
- extension du domaine d'intervention ;
- mobilité des moyens ;
- fiabilité des matériels.

Cependant des insuffisances très pénalisantes demeurent :

- disponibilité des matériels réduite par les restrictions du budget de la Défense et du fait que la Loi des Programmes Militaires (*LPM*) est rarement exécutée dans ses prévisions ;
- quelques-uns de nos grands radars d'infrastructure ont plus de 20 ans de service ;
- le réseau des transmissions sol /air est âgé lui aussi ;
- sept escadrons de chasse seulement subsistent ; la maintenance et le renouvellement de ces vecteurs très sollicités par les opérations extérieures, tardent ;
- plus que jamais indispensables à l'Armée de l'Air et de l'Espace et à la Marine, les ravitailleurs en vol C135F servent depuis 50 ans et ne sont que trop lentement relevés par les MRTT Phénix.

Jean Hauviller (octobre 2021)

ANNEXE 5

Les Contrôleurs et contrôleuses aériens

En juin 2020, le trafic aérien en France a chuté de 84,51 % par rapport à 2019, selon les données officielles. Au mois d'avril de la même année, la baisse était même de 93,28 %. Cela a touché de plein fouet les compagnies aériennes du monde entier, et du même coup l'ensemble de l'industrie aéronautique et la sous-traitance. Cette période de "vaches maigres" 2020 et 2021 n'a cependant pratiquement pas touché le monde des contrôleurs/contrôleuses aériens en France. Faisons donc connaissance avec ce "monde de l'ombre", qu'il soit civil ou militaire.

Le contrôleur aérien ou la contrôleuse aérienne (*également appelé aiguilleur/aiguilleuses se du ciel*) **guide les avions, contrôle et assure la sécurité et la fluidité de l'espace aérien. Ingénieur de contrôle de la navigation aérienne** (*ICNA*) **dans le civil, il peut également exercer au sein de l'armée de l'air et de l'espace** (*AAE*)**, de la marine ou de l'armée de terre** (*ALAT*)**.**

D'une manière générale, le contrôleur aérien est la cheville ouvrière de la sécurité de la circulation aérienne.

Dans le civil comme dans l'armée, depuis la tour de contrôle, le contrôleur aérien ou aiguilleur du ciel gère et surveille les décollages et les atterrissages des avions, les survols de l'aéroport et des espaces limitrophes. Il donne des instructions très précises à chaque pilote pour rouler, décoller, voler, atterrir, se parquer. C'est lui qui indique l'altitude à prendre et contrôle les avions pendant toutes les phases de mouvement au sol et en vol. Il fournit aux pilotes toutes les indications nécessaires.
Répartis généralement en équipe de deux, sur une position de contrôle, les contrôleurs suivent chaque appareil sur leur écran et communiquent par radio avec les pilotes.
Importance du trafic, conditions météo, plans de vol et trajectoires des avions, l'aiguilleur du ciel gère de nombreuses informations simultanément. Il analyse et anticipe les situations. Il doit toujours être en mesure de réagir et de prendre des décisions avec une extrême rapidité.
Lorsque des avions quittent son espace aérien, le contrôleur aérien de l'aéroport procède au transfert de contrôle des avions vers les contrôleurs des "centres en route". Ces derniers assurent le relais et donnent des instructions et des autorisations aux pilotes pendant la phase "en route" du vol : trajectoire (*cap*), altitude, vitesse.

Le champ d'action des contrôleurs aériens recouvre l'ensemble de l'espace aérien national, en liaison avec les contrôleurs des pays voisins.

Le métier est éprouvant et lourd de responsabilités. Comme le pilote, le contrôleur aérien tient la vie des occupants d'un avion entre ses mains. Il doit être en parfaite condition physique et nerveuse.
Il communique en anglais avec les pilotes dans la plupart des cas. Il travaille en horaires décalés. Le service fonctionne sept jours sur sept et, dans certains cas, 24 heures sur 24.

En France, dans le civil, les aiguilleurs du ciel ont la particularité d'être tous fonctionnaires. Ils travaillent soit dans un aéroport ou dans l'un des 5 centres de contrôle régionaux (*Aix-en-Provence, Athis-Mons, Bordeaux, Brest et Reims*).

L'Armée de l'air et la Marine nationale emploient également des contrôleurs aériens**.** Ils ont le rang d'officiers et de sous-officiers, et sont employés au sein d'une tour de contrôle sur base aérienne ou au sein d'un centre de détection de contrôle.
Tout comme son homologue dans le civil, le contrôleur aérien de statut militaire assure la régulation des aéronefs sur les aérodromes militaires et leurs zones d'approche (*dialogue avec les équipages, guidage radar...*). Il assure également une mission de surveillance de l'espace aérien national. Il alerte et assiste tous les avions civils ou militaires en difficulté ou en détresse dans l'espace aérien français (*problèmes de trajectoire, pannes de transpondeur...*). Il envoie et guide, lors de la détection d'un avion non identifié, la "police du ciel " et si nécessaire les avions d'interception lors du déclenchement des missions d'alerte.
Le contrôleur aérien militaire est également partie prenante lors des opérations aériennes. Il guide les avions en mission (*interception, combat...*) en France ou sur des théâtres d'opérations extérieures.
L'officier contrôleur encadre et dirige une équipe de spécialistes du contrôle des avions militaires (*décollages, atterrissages, phases d'approche, missions en zones réservées*) et quelquefois civils (*décollages, atterrissages, transits*). Il est titulaire de la licence européenne de contrôle. Il assure la surveillance de l'espace aérien national dans un volume bien déterminé depuis la salle d'opérations de son centre de contrôle. Il peut être amené à exercer ces fonctions en dehors du territoire national dans le cadre d'opérations diligentées par l'ONU ou l'UE

et généralement dirigées par l'OTAN. Acteur incontournable des opérations aériennes et de la sécurité des vols, il est en contact permanent avec le personnel navigant. Il participe également très activement à la mission de recherche et sauvetage des personnes lors d'un crash aérien. Ses champs d'intervention couvrent les différents domaines d'activité de la circulation aérienne tels que la surveillance, le contrôle et l'alerte (*dialogue et rencontres avec les équipages, militaires et civils, guidage radar lors de mauvaises conditions météorologiques...*). Il peut être affecté un escadron des services de la circulation aérienne (*ESCA*), dans un centre militaire de contrôle (*CMC*), dans un centre militaire de coordination et de contrôle (*CMCC*), voire embarqué sur AWACS au sein du 36ème escadron de détection et de contrôle aéroporté (*EDCA*), au sein d'un état-major, au sein d'un organisme interarmées ou interalliés. Son statut d'Officier de carrière lui confère pour principale mission, celle d'encadrer son équipe pour assurer le contrôle des appareils en circulation aérienne militaire et générale (*civile*) en espace aérien inférieur.

Dans le cadre du ciel unique européen, la coopération entre civils et militaires se renforce au-delà d'une simple co-implantation. L'enjeu est d'optimiser la gestion du trafic civil et militaire et d'améliorer la sécurité des vols. Pour répondre à ces attentes, l'armée de l'air a fait évoluer les DMC en CMCC : en ajoutant à la coordination la capacité de contrôle "en route" des aéronefs militaires jusqu'alors dévolue aux centres de détection et de contrôle (*CDC*). L'arrivée d'officiers de coordination contrôle défense permet de simplifier les relations et la gestion de l'espace entre civils et militaires.

La complexité de ce métier est au reflet du document ministériel de 237 pages précisant (*en son temps*) le règlement de la circulation aérienne militaire (*Procédures*), contenu au vu duquel on mesure l'ampleur de cette complexité : document consultable via internet (*Google*) :

https://www.dircam.dsae.defense.gouv.fr/images/Stories/Doc_DSAE/PCAM.pdf

Études / Formation pour devenir Contrôleur aérien / Contrôleuse aérienne

Dans le civil

La formation professionnelle pour exercer ce métier est dispensée à l'ENAC. Elle est gratuite et rémunérée.
Pour candidater, il faut être âgé de moins de 26 ans, être passé par une classe prépa ou être titulaire d'un bac + 2 : accès au concours d'admission via la banque d'épreuve CCINP (*http://www.concours-commun-inp.fr/fr/index.html*).
Le concours est très sélectif (*environ une cinquantaine de places par an*). Il ne peut être tenté que trois fois.
La formation des ingénieurs du contrôle de la navigation aérienne (*ICNA*) dure trois ans. L'enseignement est théorique et pratique pendant ces 3 ans. Les stages s'étendent sur 18 mois et comprennent une formation au brevet de pilote privé, un séjour de 8 semaines dans un pays anglophone et un stage dans une compagnie aérienne. En cours de formation, le futur ingénieur choisit son affectation en fonction de son classement : les centres régionaux ou les aéroports.
Les élèves sont rémunérés dès leur entrée en formation :

- 1ère année : environ 1 500 €
- 2ème année : environ 1 800 €
- 3ème année : environ 2 200 €

La formation confère le grade de master en management et contrôle du trafic aérien (*MCTA*).
Après sa formation, l'ICNA intègre la DGAC (*Direction générale de l'aviation civile*) et doit 7 ans à l'administration.

Dans l'armée de l'air et de l'espace

Les conditions d'accès sont :

- avoir la nationalité française
- être âgé de moins de 30 ans lors de la signature du contrat
- être titulaire d'un bac
- réussir les tests de sélection dont les tests médicaux.

En cas de réussite à tous ces tests et ayant reçu l'aval de la commission d'intégration, le candidat intègre l'armée de l'air et signe son contrat (*6 ans sauf cas particuliers*).
Formation rémunérée de 48 à 59 semaines comprenant une formation militaire (*16 semaines*), une formation de contrôleur (*6 semaines*) et un stage de qualification.

Salaires

Civil

La rémunération brute mensuelle des contrôleurs aériens en début de carrière est de l'ordre de 4800 à 5000 € brut (*solde d'un colonel échelon exceptionnel*).

Armée de l'air
Solde pour un célibataire :

- Dès l'entrée en école : 1 450 € net (*grade sergent*), 1 700 € (*10 ans de service*)
- Une prime d'engagement initial à partir d'environ 1 600 € brut est versée le 13ème mois suivant l'engagement.
- Des indemnités peuvent s'ajouter à cette solde de base en fonction de la situation familiale et de l'affectation géographique.

Si le contrôle aérien civil n'éprouve aucun mal à recruter, l'armée de l'air et de l'espace (*AAE*) a quant à elle d'énormes difficultés depuis une quinzaine d'années à recruter ses propres contrôleurs/contrôleuses aériens… Quelques rumeurs circulent à ce propos dans les rangs, à savoir :

- Une rémunération nettement inférieure à celle de leurs homologues civils. Une prime (*intégrée en totalité ou partiellement au calcul de la pension final*) à la hauteur de leurs responsabilités de contrôleurs/contrôleuses aériens semblerait les satisfaire, ou même titre que la solde à l'air des pilotes par exemple.
- Une formation à développer en phase avec celle de l'ENAC, et la possibilité d'obtenir des "diplômes" ou des qualifications reconnus dans le monde du contrôle civil (*DGAC*…).
- …

Evolutions de carrière

- **Dans le civil**, par voie de concours internes, le contrôleur aérien peut évoluer (*suivant son ancienneté*) vers des fonctions d'études, d'encadrement ou de management dans les services de l'aviation civile.
- **Dans l'armée de l'air et de l'espace**, de grade d'aviateur jusqu'au grade de caporal-chef après 4 mois de service, puis grade de sergent à compter du 13ème mois de service avec possibilité d'évolution par la suite vers le statut de sous-officier de carrière, voire d'officier.

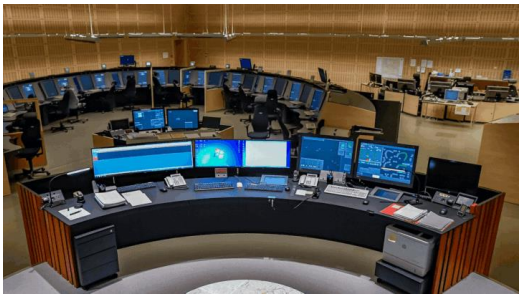
« *Vive les Chouettes !* »

Voici maintenant cinq choses que vous ne saviez probablement pas encore sur le contrôle aérien chez nos voisins belges (*23/02/2021*)

1. La Belgique est complexe
C'est vrai à bien des égards, mais certainement en ce qui concerne l'espace aérien belge… C'est un espace aérien limité, mais très densément fréquenté par divers usagers. Ainsi, il y a naturellement l'aviation commerciale et militaire, le trafic privé et récréatif, mais aussi, et de plus en plus, le trafic aérien sans équipage (*les drones*). Et la proximité de grands aéroports dans les pays voisins a pour conséquence que leur trafic aérien passe également dans l'espace aérien inférieur belge en phases de décollage ou d'atterrissage.

Il existe deux critères pour définir la complexité d'un espace aérien : les volumes de trafic et la structure de l'espace aérien. L'espace aérien belge est surtout complexe sur le plan structurel, car il n'y a pas moins de 6 aéroports pour l'aviation civile dans un espace plutôt restreint, et une multitude de zones d'entraînement militaire qui occupent environ 50% de l'espace aérien total. Vous avez dit complexe ? Exactement !

2. L'espace aérien exige un travail d'équipe (inter)national



Skeyes **(***issu de la Régie des voies aériennes en 1998 et dénommé Belgo-control jusqu'en 2018, est l'entreprise publique autonome belge chargée du contrôle du trafic aérien, de la formation des contrôleurs aériens et personnel technique, et de l'installation et de l'entretien de l'infrastructure de navigation aérienne dans la zone dont la Belgique est responsable*) gère le trafic aérien belge jusqu'à une altitude d'environ 7500 m (*FL245*). Au-dessus de cette altitude, le *Maastricht Upper Area Control Centre* (*MUAC*) d'Eurocontrol prend le relais. Cela vaut en premier lieu pour toute l'aviation civile. Mais naturellement, il existe aussi un pendant pour l'aviation militaire. Depuis décembre 2019, le site de skeyes à Steenokkerzeel est devenu le centre névralgique de ces deux aviations : les contrôleurs aériens de l'aviation civile et les contrôleurs aériens de la Force aérienne belge partagent la même salle opérationnelle pour le trafic aérien en approche et en survol. De cette manière, chacun peut exploiter l'espace aérien belge encore plus efficacement et avec davantage de flexibilité. Le ministère de la Défense et skeyes ont d'ailleurs l'ambition commune d'intégrer complètement leurs services de navigation aérienne et de les "prester" (*terme belge signifiant fournir ensemble – accomplir un travail*) ensemble d'ici 2030.

3. Cela ne se résume pas à la tour de contrôle

Les contrôleurs aériens n'ont pas tous les mêmes tâches. Nous passerons brièvement ici en revue leurs 3 rôles différents. Dans la tour de contrôle, les contrôleurs aériens vérifient tous les mouvements au sol *et* donnent le feu vert pour les décollages. Ils guident ensuite les avions jusqu'à ce qu'ils quittent l'espace aérien de l'aéroport. Dès cet instant, le contrôleur aérien d'approche (*APP*) prend le relais et guide l'avion vers le bon couloir aérien. Ce collègue ne se trouve pas dans la tour de contrôle, mais au centre de contrôle aérien CANAC 2. Dès que l'avion met le cap sur sa destination, un collègue contrôleur aérien de l'ACC l'intègre à son tour dans le flux du trafic. Tous les contrôleurs aériens veillent en permanence à ce que soient respectées les distances de sécurité correctes entre les avions : dans une tour cette séparation est visuelle, dans un environnement radar nous désignons ces distances en *miles* (*1609 m - horizontalement/latéralement*) et en pieds (*30,48 cm - verticalement*).

4. Une course éliminatoire pour les candidats

Au total, cela prend quasiment trois ans avant de pouvoir se dire officiellement "*air traffic controller"* (*ATCO*). Le processus de sélection initial dure six mois. Finalement, seul(e)s les candidat(e)s ayant les qualités requises pour devenir contrôleur aérien sont retenu(e)s. Au cours de la formation qui s'ensuit - organisée à Steenokkerzeel - des évaluations sont effectuées à différents moments. Au fait, saviez-vous que toute la formation est dispensée en anglais et que toutes les évaluations (*aussi bien écrites qu'orales*) se déroulent aussi dans la langue par excellence de l'aviation ? Lorsque vous avez terminé votre formation, vous êtes prêt(e) pour commencer votre stage.

5. Skeyes est active partout en Belgique

Les contrôleurs aériens guident chaque avion du tarmac jusque dans les airs (*et inversement*) à Brussels Airport et dans les aéroports régionaux d'Anvers, de Charleroi, de Liège, de Courtrai et d'Ostende. La majorité du personnel travaille à Steenokkerzeel, juste à côté de l'aéroport, et il y a également des stations radar à Bertem et à Saint-Hubert. Enfin, skeyes ambitionne également d'ériger des tours digitales pour les besoins des six aéroports belges. Elles remplaceront progressivement les tours de contrôle classiques.

ANNEXE 6

Contrôle aérien des drones

Le contrôle du trafic aérien des drones sera automatisé.
La mise en place d'un trafic aérien organisé et contrôlé s'impose désormais comme un préalable indispensable pour assurer le décollage commercial des drones.

Dans une étude, PwC (*PriceWaterhouseCoopeers*) a évalué en 2020, à 127 milliards de dollars, le marché des activités liées aux drones mais cite en bonne place, parmi les conditions *sine qua non* à remplir, l'organisation sécurisée du trafic des drones dans l'espace aérien. La réglementation, en effet, ne peut suffire à faire évoluer sans risque des drones au-dessus de nos têtes : il faut que chaque appareil puisse se faire reconnaître des autres aéronefs et s'inscrire dans le grand-huit d'une régulation du trafic qui ne pourra être qu'automatisée.
La multiplication des signalements de drones évoluant dans des zones où ils n'ont rien à faire mais aussi et surtout la pression exercée par les initiateurs de grands projets (*livraisons par voie aérienne, activités de surveillance ou d'inspection des infrastructures, entre-autre*) incitent les différents acteurs à se concerter. Un premier pas a été réalisé à Genève. Les représentants d'une soixantaine d'administrations de l'aviation civile (*dont la DGAC française et ses homologues britannique, allemande, suisse, italienne ou belge…*), de fabricants de drones (*Parrot, DJI, DelairTech…*), de sociétés de services (*Airmap, Matternet, PrecisionHawk, Nokia*…) ainsi que plusieurs laboratoires universitaires chinois se sont accordés pour constituer *"un groupe de standardisation du trafic des drones civils"*. Organisée sous l'égide de DroneApps, structure proche de l'Ecole Polytechnique de Lausanne, cette initiative vise à créer une interface au sein de laquelle les différents acteurs pourront confronter leurs contraintes et déterminer la meilleure façon d'organiser le trafic. Les groupes de travail formés à Genève se penchent notamment sur le type de transpondeur qui permettra d'identifier un drone ou encore sur le partage d'informations météo. *« Il existe une forte demande en faveur d'une organisation globale de l'espace aérien en dessous de 150 mètres. Les autorités de régulation ont besoin de savoir ce qu'il est possible de réaliser techniquement et les entreprises ont besoin de connaitre les standards qu'elles devront appliquer »* estime Benoit Curdy, l'un des animateurs de DroneApps. *« Autant éviter les affres de l'affrontement des normes que l'on a connu dans la vidéo ou la téléphonie mobile »* insiste-t-il.

S'agissant de la mise en place d'un mode automatisé de régulation du trafic, le leader technologique incontesté est la Nasa.
L'agence spatiale américaine semble avoir pris une nette avance dans la conception d'un système dit *"sense and avoid"* (*"repérer et éviter")* permettant aux engins sans pilote de modifier automatiquement leur trajectoire afin d'éviter un obstacle, fixe ou mobile. La Nasa est parvenue à faire voler simultanément 22 drones dans le cadre d'un contrôle automatisé, en liaison avec la FAA (*Federal Aviation Administration*). En revanche, la Nasa ne peut se poser comme creuset d'une concertation mondiale associant des interlocuteurs américains mais aussi européens et chinois. Ce qui laisse un espace aux initiatives comme celle de DroneApps. Cependant, ces contraintes n'empêchent pas les autorités américaines de pousser les feux sur l'organisation de l'espace aérien. La FFA vient tout juste de nommer le directeur général d'Intel, Brian Krzanich, à la tête d'un comité consultatif chargée de *"proposer des stratégies d'intégration"* afin d'insérer les engins volants sans pilote dans l'espace aérien.

Voici la liste des documents à présenter en cas de contrôle dedrone en France
(*Mise à jour effectuée le 7 juillet 2021 avec la relecture de Laurent Raynaud du centre de formation Flying Manta*).
Imaginez que vous êtes en train de faire voler votre drone dans le cadre d'une mission professionnelle avec toutes les précautions d'usage alors qu'au loin, le véhicule "SUV bleu bariolé jaune et rouge" des gendarmes s'arrête. Pas de panique, voici la liste de tout ce que les télépilotes professionnels doivent présenter en cas de contrôle de drone par les autorités **(***Bonne nouvelle : Vous pouvez présenter vos documents justificatifs au format papier ou électronique*).
Pour justifier votre activité de télépilote de drone professionnel, si vous êtes contrôlé en cours de mission, vous devez montrer :

- **Le CATT** ou Certificat d'Aptitude Théorique de Télépilote de drone, obligatoire pour être référencé auprès de la DGAC et exercer à titre professionnel en toute légalité.
- **L'attestation de suivi de formation** à l'usage des drones de loisirs (transmise par votre organisme de formation)

- **L'attestation d'aptitude aux fonctions de télépilotes** pour ceux qui ont passé leur certificat théorique avant le 1et juillet 2018 et qui n'ont pas passé le CATT.
- **Le MANEX** – manuel d'exploitation, anciennement MAP (manuel d'activités particulières)
- Et on n'oublie pas qu'il vaut mieux avoir sa **RC Pro** -Assurance Responsabilité Civile Professionnelle, sur soi ainsi qu'une attestation à **l'assurance R.C. Risques Aériens**, qui bien qu'elle ne soit pas obligatoire, est fortement recommandée.

A noter :

- **Le livret de progression** pour suivre et attester l'acquisition des compétences pratiques, n'a pas à être montré sur le terrain.

Les documents du contrôle de drone pour le drone

Côté drone, il existe également des documents à présenter aux autorités pour attester de la conformité de votre drone :

- **L'étiquette d'enregistrement drone,** lisible à 30 cm**,** que **v**ous pouvez recevoir gratuitement et qui contient les informations suivantes : votre n° d'exploitant européen (*de la forme UAS-FR-XXXXX*), votre nom, votre adresse et votre n° de téléphone, et enfin le n° d'enregistrement du drone si sa masse est supérieure à 800g ou si le drone émet un signalement électronique.
- **Les éléments fournis par le constructeur du drone** : l'attestation de conformité drone (*si votre appareil le nécessite …. S3 à + de 2 kg ou S2 par ex*.), l'attestation de conception drone, le manuel d'entretien et le manuel d'utilisation ne sont pas obligatoirement à présenter sur le terrain mais doivent être à disposition des autorités au minimum dans votre exploitation.

Les documents du contrôle de drone pour la mission

Avant votre mission vous avez la responsabilité d'avoir en votre possession toutes les autorisations, accords, protocoles, déclarations, notifications que votre mission pourrait nécessiter (*par ex : vol en agglomération, vol S2, vol en zone D, P, R, etc. …*) pour assurer votre vol en toute sécurité et en toute légalité.

- Si vous volez en scénario S1 (*ou catégorie spécifique STS-01*) : aucune autorisation n'est nécessaire
- Si vous volez en scénario S2 (*ou catégorie spécifique STS-02*) ou S3 : vous devez avoir fait votre demande sur Alpha Tango.

Il est à noter qu'il n'y a aucune autorisation à attendre pour un vol en S2 (*régime déclaratif*), en S3 (*possibilité de la Préfecture de vous limiter ou interdire mais pas d'autorisation*), dans certaines SETBA et VOLTAC.

Attention : quel que soit le scénario de vol, il faut également tenir compte des restrictions éventuelles pour lesquelles il faudra obtenir différentes autorisations.

Par exemple : obtenir un protocole avec les aéroports, obtenir l'autorisation du CDAOA de l'armée de l'air et de l'espace pour les zones interdites, etc.

Et d'autre part, vous devez également être en possession d'autorisations selon les types de prises de vues :

- Pour la prise de vue en spectre visible (*c'est à dire visible par l'œil humain*) : aucune autorisation n'est à obtenir, c'est un régime purement déclaratif. Vous devez adresser le formulaire de déclaration à la DSAC qui vous délivrera un accusé de réception.
- Pour la prise de vue en spectre invisible (*via caméra infrarouge, radar…*) : vous devez faire une demande d'autorisation à la préfecture qui est donnée après une courte enquête (*quelques semaines*) et qui est valable 3 ans, à renouveler. Si vous avez l'autorisation de prise de vue en spectre invisible, vous devrez présenter votre attestation en cours de validité.

Préparation des fiches missions pour les vols de drones dans les zones sous contrôle de l'espace aérien

La préparation des fiches missions est une étape indispensable mais fastidieuse. Pour chaque vol de drone, vous établissez une fiche correspondante destinée au contrôle aérien ?

Plus de vingt aéroports utilisent les solutions de Clearance pour gérer les vols de drones dans leurs espaces aériens. Le système génère automatiquement les fiches missions. Vous pouvez les imprimer, les transmettre au format PDF, ou laisser les personnes autorisées les consulter en ligne.

Le demandeur saisi lui-même les paramètres de son vol

Le télépilote saisi lui-même les informations relatives à son vol, sur une interface en ligne. Le télépilote n'entre que les informations nécessaires. En revanche le système n'autorisera pas la transmission d'une demande incomplète. La plateforme vérifie la cohérence des informations, afin d'éviter oublis et erreurs.

N'hésitez pas à découvrir par vous-même l'interface dédiée aux exploitants de drones.

La plateforme déduit automatiquement certaines informations, comme l'adresse ou l'altitude du sol par exemple. Vous recevez donc toutes les informations nécessaires, et la saisie reste simple et rapide pour le télépilote.

Analyse et contrôle de la demande
Vous pouvez analyser les demandes directement en ligne. En fonction de vos besoins, nous paramétrons la carte et les analyses automatiques. Vous rendez votre avis d'un simple clic, autorisant ou refusant les demandes, ou en y apportant des restrictions ou des commentaires.

Édition automatique des fiches missions
Pour chaque mission, la plateforme édite une fiche récapitulative. Elle reprend toutes les principales informations liées à la mission, comme la date, la hauteur et les coordonnées du télépilote. Bien entendu, vos consignes y figurent également. Nous distinguons à ce sujet deux types de consignes :

- les consignes générales
- les consignes particulières

Pour chaque mission, les consignes générales sont ajoutées. Il peut s'agir par exemple de la conduite à tenir en cas d'incident, ou d'un rappel réglementaire. Les consignes particulières sont optionnelles, et peuvent être personnalisées pour chaque mission. Vous pouvez également définir une liste préétablie de consignes particulières pour celles que vous utilisez le plus souvent.
Enfin, la zone de la mission est représentée sous forme cartographique, par exemple :

CLEARANCE

Mission Drone : D-BO19-058

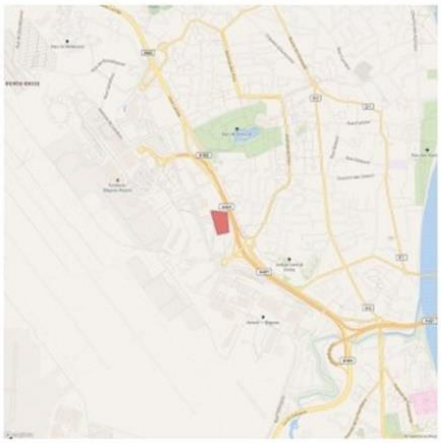
Date de génération du document : 20/08/2019 06h57Z
Date du vol : 20/08/2019 - 30/08/2019
Durée du vol : 0h15 (dans la période 06:30 - 14:30 UTC soit 08:30 - 16:30 locales)
Hauteur sol : 150 m - 492 ft(soit 981 ft AMSL)
RDL 124° / 0.8 NM
Zone : CTR Toulouse Blagnac
Adresse / Commune : a 621, 31700 Blagnac, France
Coordonnées géographiques : 43.62813N 1.3825E
Nom de l'entreprise : Clearance Demo
Nom du télépilote : [redacted]
Numéro de téléphone : 0612345678

Statut : La mission a été acceptée.

Consignes générales

Le pilote doit être joignable au numéro de téléphone indiqué pendant toute la mission.

- Transmettre ce document à la BGTA dès réponse du SNA/Sud : [redacted] blagnac@gendarmerie.interieur.gouv.fr et coordonner la mission auprès de la BGTA avec un préavis de 2h au [redacted]
- Si la mission se déroule dans la LF-R23 Francazal, demander l'accord à l'organisme gestionnaire : [redacted]
- Si la mission se déroule dans la LF-R112 Fonsorbes, demander l'accord à l'organisme gestionnaire (DGA) : [redacted]
- Tout incident ou évènement de sécurité observé et impliquant au moins un aéronef extérieur à la société devra être notifié dans les 48h par mail à la subdivision Qualité de Service Sécurité du SNA / Sud : sna-s-[redacted]



Les fiches missions sont transmises par courriel, et/ou au télépilote.

ANNEXE 7

Guerre électronique / informatique, une guerre plus que jamais présente…

Depuis un peu plus d'un siècle, ce nouveau mode de guerre "technologique" s'amplifie et n'épargne pratiquement plus personne. On parle de guerre électronique, de cyber-attaque et de cyberdéfense, de cyber-guerre et de harcèlement électromagnétique, de renseignement d'origine électromagnétique… bref, une nouvelle "guerre mondiale", sournoise, est bel et bien là n'épargnant personne.

La **GUERRE ÉLECTRONIQUE** consiste en l'exploitation des émissions radioélectriques d'un adversaire et, inversement consiste à l'empêcher d'en faire autant. Il s'agit donc de toutes les opérations visant à acquérir la maîtrise du spectre électromagnétique, pour intercepter et/ou brouiller les ordres ou informations circulant dans les systèmes de communication de l'adversaire.

Dans la pratique, nous pouvons considérer que la guerre électronique est née le 19 octobre 1917.
A cette époque, pendant la Grande Guerre, la flotte de *Zeppelin* allemands, qui se déplace sur de longues distances pour mener des bombardements de jour comme de nuit, est une menace importante pour la France. Le colonel Gustave Ferrié, pionnier dans le domaine de la radiodiffusion, ayant les pleins pouvoirs pour développer la Télégraphie sans fil (TSF) au sein de l'armée, met en place un réseau de radiogoniométrie reliant la station centrale de la tour Eiffel, plus haute station radiophonique au monde, et les stations de province, afin de localiser et de suivre les *Zeppelin*. Des stations terrestres mobiles sont installées pour localiser les lieux d'émission. Mise en œuvre parallèlement au front, l'installation permet de déterminer avec précision la position des dirigeables ainsi que les stations ennemies. À l'époque, les risques de raid sur Paris sont importants. Il est décidé qu'en cas d'attaque, les communications seraient brouillées entre les ballons et les postes d'émission allemands, qui transmettent les informations à l'arrière.
Le 19 octobre 1917 au soir, une escadre d'une dizaine de *Zeppelin* tente un raid sur la France. Ils sont repérés par l'installation du colonel Ferrié avant même de passer la frontière française et sont suivis sur une carte alors qu'ils traversent le Nord du Luxembourg, la Belgique puis le Pas-de-Calais. Le colonel Gustave Ferrié donne alors l'ordre à certaines stations du front de brouiller les communications des *Zeppelin* en accordant les émetteurs sur la longueur d'onde des dirigeables. Mais le colonel Ferrié veut aller plus loin et maquille les postes français en émetteurs allemands. Les rectifications de route qui sont communiquées aux Allemands les conduisent au-dessus des camps d'aviation et des batteries. Les dirigeables ennemis sont alors abattus ou contraints d'atterrir dans les lignes françaises, excepté un appareil, qui, désorienté, descend la vallée du Rhône pour disparaître aux abords de la Corse. C'est le premier exemple de mise en œuvre d'une contre-mesure active grâce aux émissions d'onde, qui donnera naissance à la guerre électronique. Cet événement marque une défaite pour l'aviation allemande ainsi que la fin de l'épopée des *Zeppelin*, qui n'effectueront plus aucune grande sortie jusqu'à la fin de la guerre. Ces mesures de renseignement électronique et d'intrusion (*leurrage*) sont encore aujourd'hui les composantes majeures de la guerre électronique, qui consiste à maîtriser le spectre électromagnétique et qui englobe toutes les dimensions de la guerre. Elle a donné naissance aux mesures de protection électronique.

Cette pratique très largement utilisée durant la Seconde Guerre Mondiale s'est depuis rapidement développée touchant aujourd'hui notre propre quotidien.
L'utilisation de la radiocommunication durant la Première Guerre mondiale par les belligérants a conduit aux premiers systèmes d'écoutes et de tentatives de brouillage radio. L'utilisation du radar durant la Seconde Guerre mondiale a institué les règles de brouillage radar.

Cet Handley Page Halifax-B Mark III du 462 Squadron de la Royal Australian Air Force en 1945 a appartenu au Groupe 100 RAF spécialisé dans la protection des raids de bombardements stratégique Alliés en Europe. Sous son fuselage se trouve du matériel de brouillage radar et de contre-mesures.

La guerre électronique se divise en 3 domaines, l'attaque électronique, le soutien électronique et la protection électronique.

L'**attaque électronique** consiste à attaquer l'adversaire à l'aide d'armes électroniques. Afin de tuer ou de neutraliser l'adversaire aux moyens d'armes électroniques, ou de détruire ses équipements, l'attaquant cherchera également à neutraliser ou détruire les ressources électroniques de l'ennemi. Il s'agit donc pour l'essentiel de mesures de brouillage de ses émissions électromagnétiques et de mesures de "leurrage" ou d'intrusion de ses systèmes électromagnétiques humains mais également non-humains. Le brouillage rend inexploitable les émissions de l'adversaire ; le leurrage et l'intrusion lui donnent de fausses indications ou de fausses pistes.

L'ensemble de ces moyens était autrefois appelé "contre-mesures électroniques" (*CME*), en anglais ECM pour *Electronic Counter Measures*. L'attaque électronique inclut également l'emploi d'armes à énergie dirigée, destinées à détruire les systèmes électroniques adverses. Elle implique l'utilisation de "moyens actifs", donc indiscrets.

Le **soutien électronique** ou "renseignement électronique" rassemble tous les "moyens passifs" de la guerre électronique, son objectif est le *"contrôle du spectre radioélectrique"*. Les militaires employaient autrefois l'expression "mesures de soutien électronique" ou ESM (*pour l'équivalent anglophone : Electronic Support Measures*). Il s'agit d'utiliser les émissions électroniques de l'adversaire pour détecter sa présence, le localiser par goniométrie, et si possible identifier ses unités, obtenir des informations sur les systèmes qu'il utilise et écouter ses communications.
Le renseignement d'origine électromagnétique (*ROEM*), aussi appelé SIGINT en anglais pour *Signals Intelligence*, comprend :

- le COMINT (*pour Communication Intelligence*), le renseignement issu de l'écoute de communications (*démodulation, décodage, décryptage, traduction...*) ;
- l'ELINT (*pour Electronic Intelligence*), le renseignement technique et de localisation obtenu par l'analyse d'émissions autres que communications, par exemple l'interception des signaux radar et la localisation d'antennes émettrices.

La **protection électronique** inclut tous les dispositifs et toutes les procédures permettant de contrer les attaques électroniques et les moyens de renseignement électronique de l'adversaire. On parlait autrefois de mesures de protection électronique et de contre contre-mesures électroniques (*en anglais ECCM pour Electronic Counter Measures*).
Il sagit soit :

- de concevoir des bâtiments ou des aéronefs de combat furtifs, c'est-à-dire avec une "signature" radar réduite en utilisant des formes dispersant les ondes et des revêtements absorbants ;
- d'appliquer des plans d'utilisation de fréquences et des procédures de silence radio et radar ;
- d'utiliser des systèmes d'identification électronique ;
- d'utiliser des systèmes électroniques à évasion ou à saut de fréquence, ou encore, pour les communications, des systèmes à émissions brèves ;
- d'utiliser, pour les communications, des codes et du chiffrement ;
- d'utiliser un système de filtrage des interférences ou d'annulation des interférences (*suppression de l'activité du brouilleur en lui superposant une propriété inverse, ce qui reste difficile en raison du besoin de compenser le déphasage*).

D’autres modes "guerriers" liés à l’usage de l’informatique ont vu le jour. Il est notamment question de cyberattaque, de cyberdéfense, de cyberguerre, de Harcèlement électromagnétique…

Une **CYBER-ATTAQUE** est un acte malveillant envers un dispositif informatique via un réseau cybernétique. Une cyberattaque peut émaner de personnes isolées, Kevin Mitnick étant une des plus célèbres, d'un groupe de pirates ou plus récemment de vastes organisations ayant des objectifs géopolitiques.
Pour A. Coustillère, vice-amiral alors chargé de la cyberdéfense française, la cyberattaque se définit comme "une action volontaire, offensive ou malveillante, menée au travers du cyberespace et destinée à provoquer un dommage aux informations et aux systèmes qui les traitent, pouvant ainsi nuire aux activités dont ils sont le support". L’ANSSI (*Agence Nationale de la Sécurité des Systèmes d'Information*), l’assimile à une "tentative d’atteinte à des systèmes d’information réalisée dans un but malveillant. Elle peut avoir pour objectif de voler des données (*secrets militaires, diplomatiques ou industriels, données personnelles bancaires, etc*.), de détruire, endommager ou altérer le fonctionnement normal de systèmes d’information (*dont les systèmes industriels*)". En raison de la létalité réduite de certaines cyberattaques, on privilégie plutôt le terme de "vandalisme cybernétique" ou "vandalisme virtuel". Intentionnelle et planifiée, la cyberattaque résulte "de l’emploi de capacités cyber dans le but premier d’atteindre des objectifs dans ou par le cyberespace, utiliser des ordinateurs en réseau dans le but de perturber, interdire, dégrader, manipuler ou détruire des informations dans le système d’information cible". Plus simplement, elle est l’une des méthodes pour affaiblir, paralyser, corrompre ou détruire une cible dépendante totalement ou en partie de la cyber-sphère.
Selon certains, le terme de cyberattaque prête à confusion. En Effet, l'attaque en ligne, en elle-même, réduit donc le champ de la réflexion. La cybernétique est un mot valise intégrant le cyber (*gouvernance ou pilotage selon la racine grecque*), le cyber (*crypté en anglais*), l'électronique et l'automatisme. C'est pourquoi le terme de cyber-agression, ou d'agression cybernétique comprend en effet davantage les crimes et les délits dans le cyber-univers.

Selon ces derniers, les agressions dans la cyber-sphère se répartissent en 12 grandes familles : les ADS (*Attaque par Déni de Services pour neutraliser un système informatique et le rendre inopérant*) :

- le cyber-espionnage
- le cyberharcèlement
- la cyberfraude (*triche aux examens, lors de vote, falsification de documents officiels, etc*.)
- le cyber-whistleblowing (*considéré comme un délit voire un crime dans les dictatures notamment*)
- la cyber--contrefaçon (*musique, livre, jeux-vidéo, logiciels) et le cybermarché noir (achat en ligne de marchandises illégales*)
- la cyber-finance criminelle
- la cyberpropagande
- la cyber-usurpation d'identité
- le cybercambriolage (*vol de données*)
- le défaçage (*modifier l'apparence d'un site, d'un blog, etc*.)

Les objectifs et les moyens des cybercriminels sont très variés. Une liste non-exhaustive des objectifs avec des profils associés peut cependant être établie :

Tableau des différents objectifs des cybercriminels

Objectif	Profils	Moyens	Dangerosité
Lucratif	Mercenaires, escrocs, etc.	Élevés	Haute
Géopolitique	Unités spécialisées, états, etc.	Élevés	Haute
Ludique	Adolescents désœuvrés, scripts kiddies, etc.	Bas	Basse
Technique	Experts chevronnés, etc.	Bas	Basse
Pathologique	Vengeurs, employés mécontents, etc.	Bas	Moyenne
Idéologique	Hacktivistes, terroristes, patriotes, etc.	Moyen	Moyenne

Chronologie de quelques cyber-attaques

En 1982, les services secrets américains auraient introduit volontairement un bug dans le logiciel canadien de gestion du gazoduc transsibérien, provoquant une importante explosion dans une zone inhabitée.

Le début de l'année 1990 est concomitant à l'émergence d'une sous-culture criminelle cybernétique. La première intervention de taille nationale sera l'Operation Sundevil en 1990. L'émergence du cyberespace accélère également la démocratisation du *cracking*, du *phreaking* et des techniques d'hacking.

En 2007, la première cyberattaque recensée visant une structure étatique durant plusieurs semaines, avec des moyens suffisants pour saturer durablement les sites visés et causer un déni de service prolongé, a émané de sites russes contre des sites de l'administration estonienne, ainsi que ceux de banques et de journaux de ce pays. La majorité des institutions estoniennes ayant adopté une bureaucratie sans papier, entièrement informatique et reliées entre elles par internet, ce pays se trouve très vulnérable à ce type d'attaques.

Il s'agit d'une attaque simple mais efficace, qui consiste à connecter un maximum d'appareils à un même réseau et ainsi déclencher une saturation de celui-ci. Cette méthode est souvent utilisée pour sa discrétion (*niveau traçabilité*) car elle est dirigée par une seule personne contrôlant plusieurs ordinateurs infectés par celle-ci. Comme il y a un afflux d'appareils, l'option du traçage IP est à rejeter (*par l'abondance de celles-ci*). C'est la méthode dite du botnet.

L'attaque survient à la suite du conflit diplomatique généré autour du projet de déplacement du Soldat de bronze planifié par le gouvernement estonien en avril 2007 mais ayant abouti à des nuits d'émeutes, émanant d'une minorité de nationalistes russophones implantée dans le pays.

Bien que la jurisprudence de l'OTAN ne prenne alors pas encore en compte ce genre d'attaques, certains responsables estoniens considéraient la cyberattaque, par son organisation et sa durée, comme un acte de guerre à part entière, car les structures visées se sont retrouvées entièrement inopérantes, de la même manière que si elles avaient été frappées par des missiles. Le porte-parole du département de la défense estonien, Madis Mikko a déclaré « *Si un aéroport ou une banque sont attaqués au missile, c'est la guerre. Mais si on fait la même chose avec des ordinateurs… comment appelle-t-on cela ?* ». Le président de l'Estonie, Thomas Hendrik Ilves, a considéré ces actes de déstabilisation comme une nouvelle forme de terrorisme. Mais de telles attaques posent un problème de "traçabilité", à savoir la possibilité de remonter jusqu'à leur auteur et surtout de le prouver.

Selon le magazine américain "60 minutes", les grandes pannes du réseau électrique brésilien de janvier 2005 (*Rio de Janeiro*) et de septembre 2007 (*Espírito Santo*) seraient la conséquence de cyberattaques, dont la source n'est pas identifiée. Cette hypothèse a également été évoquée pour la coupure géante d'électricité du 10 novembre 2009, au Brésil, mais n'est avérée dans aucun de ces cas.

La Corée du Sud, **en juillet 2009** a subi des cyberattaques à grande échelle. 25 sites dont les sites Internet de la présidence sud-coréenne, du ministère de la Défense, du ministère des Affaires étrangères, de la Shinhan Bank et Korea Exchange Bank ont été touchés, sur fond de tensions avec la Corée du Nord. Selon la presse sud-coréenne, le National Intelligence Service aurait sous-entendu la responsabilité de Pyongyang, sans fournir de preuves.

Dans les années 2009-2010, le monde occidental s'inquiète de la prolifération de centrales nucléaires en Iran, officiellement civiles. Tous les médias s'interrogent régulièrement sur la probabilité d'un raid israélien qui permettrait d'en détruire au moins une pour envoyer un signal fort, mais soulignent que cela serait techniquement extrêmement risqué, impliquerait le survol de plusieurs pays qui s'y opposeraient et pourrait résulter en une réplique démesurée de l'Iran, comme l'envoi de missiles à longue portée sur les principales villes d'Israël.
La cyberattaque qui va paralyser la centrale nucléaire de Bouchehr permet d'atteindre l'objectif visé (*mettre la centrale iranienne hors d'état*) sans prendre le moindre risque ni humain, ni politique, ni militaire. Elle va consister à paralyser les ordinateurs de la centrale avec un virus d'un niveau de sophistication extrême dont Israël et les États-Unis sont hautement soupçonnés.
Le virus impliqué s'appelle Stuxnet. Il est authentifié par Windows comme étant sans danger, ce qui implique qu'il utilise des clés numériques de sécurité volées dans des entreprises de logiciels de Taïwan. Il a transité jusqu'à la centrale par des clés USB donc avec des complices humains, le réseau informatique de la centrale n'étant pas connecté au monde extérieur. Il a déréglé le contrôle des automatismes, des robots, de la distribution d'électricité, tout un système de pilotage complexe de type SCADA fabriqué par l'Allemand Siemens. Le malware est passé inaperçu pendant des mois, causant progressivement de nombreux dégâts dont le dérèglement de centrifugeuses conduisant à leur destruction physique. Le développement d'un tel virus a nécessité probablement un investissement de plusieurs millions de dollars.
En 2011, c'est un second virus encore plus élaboré qui apparait, dénommé Flame, et qui semble avoir un lien de parenté avec Stuxnet.

En mai 2011, c'est au tour de Lockheed Martin, entreprise majeure du secteur de l'armement aux États-Unis qui fabrique notamment les avions de combat F-16, de subir de plein fouet une cyberattaque massive dont l'origine n'est toujours pas officiellement connue. Tous ses systèmes informatiques ont été paralysés pendant plusieurs heures et tous ses codes de sécurité ont été dérobés.

En juin 2011, on apprend le piratage de plusieurs centaines de comptes Gmail appartenant à des hauts fonctionnaires américains, des dissidents chinois, des responsables de plusieurs pays asiatiques, des militaires et des journalistes. Selon Google, l'origine de cette cyberattaque se situe à Jinan, où se trouve un commandement militaire chinois, et surtout une école formée avec le soutien de l'armée, qui avait déjà été accusée d'avoir pénétré les serveurs de Google. La Chine a démenti.

En septembre 2011, une vague d'attaques informatiques est orchestrée au Japon, tout particulièrement contre des sites Internet du gouvernement.

En juin 2012, jusqu'à 80 millions de dollars sont détournés dans une vague de cyberattaque visant des banques américaines, européennes et latino-américaines.

En février 2014, les établissements américains du groupe de loisirs Las Vegas Sands sont victimes d'une cyberattaque majeure incluant le piratage du réseau informatique, un vol massif de données confidentielles puis la mise hors service d'une partie importante du système d'information et de télécommunications. Le piratage serait attribué à un groupe de hackers iraniens et ferait suite à la suggestion publique en octobre 2013 du milliardaire Sheldon Adelson, actionnaire majoritaire de Las Vegas Sands, de "raser" Téhéran sous le feu nucléaire.

En novembre et décembre 2014, Sony Pictures Entertainment est victime d'une très importante fuite de l'ensemble de ses données, qui sont révélées par à-coup et revendiqué par le groupe Guardian of Peace".

Les 8 et 9 avril 2015, TV5 Monde est victime d'une cyberattaque entraînant l'arrêt de la diffusion de ses programmes.

En février 2016, la Banque du Bangladesh est victime d'un piratage informatique se faisant dérober 81 millions de dollars.
Une autre banque, équatorienne cette fois, la Banco del Austro, fut également victime d'une cyberattaque, en janvier 2015. Cette attaque ne fut confirmée que le dimanche 22 mai 2016. Le préjudice est estimé à 10,7 millions d'euros.

Les 12 et 13 mai 2017, une cyberattaque de grande ampleur paralyse les ordinateurs de multinationales et de services publics d'une centaine de pays. Des hôpitaux britanniques, les multinationales Renault et FedEx, le ministère russe de l'Intérieur, l'opérateur de télécoms espagnol Telefónica, la compagnie ferroviaire allemande Deutsche Bahn font partie des victimes.
Cette cyberattaque se répand grâce à des courriels comportant un lien internet qui, une fois cliqué, permet au virus d'être téléchargé dans l'ordinateur sans que l'utilisateur ait donné son accord. Il se répand aussi grâce au protocole SMB, puis exploite le système obsolète Windows XP, et toutes les versions antérieures à Windows 10 n'ayant pas effectué les mises à jour, pour libérer une charge utile, constituée de malwares, qui chiffrent les données contenues dans l'ordinateur avant de réclamer une rançon à l'utilisateur en échange de clés de décodage. Les ordinateurs contaminés par le virus sont estimés à plus de 230 000, dans 150 pays.
Parallèlement, une autre cyberattaque (*nommée Adylkuzz et plus silencieuse que WannaCry*), fait des centaines de milliers de victimes. Elle repose sur les ressources des ordinateurs infectés pour faire du cryptomining, c'est-à-dire créer et miner une monnaie virtuelle concurrente du Bitcoin, le Monero.

Le 27 juin 2017, une nouvelle vague massive de cyberattaques "rappelant le mode d'action du virus WannaCry en mai" a touché simultanément des entreprises majeures en Ukraine, affectant le fonctionnant des banques et aéroports, en Russie, le géant pétrolier Rosneft a été visé ainsi que des grosses banques ukrainiennes, Mars, Nivea, Auchan et des structures gouvernementales ukrainiennes, « *Le site du gouvernement a cessé de fonctionner* », a déclaré à l'AFP une porte-parole ministériel. Des informations émanant de plusieurs entreprises font état "d'un virus faisant apparaître une demande de rançon de 300 dollars sur l'écran de leurs ordinateurs". Sur sa page Facebook, le métro de Kiev indiquait "ne pas pouvoir accepter de paiements en carte bancaire à ses guichets à cause d'une cyberattaque". À l'aéroport Borispol de Kiev en raison de dysfonctionnements des panneaux d'affichage, des vols pouvaient être retardés. Dans les heures qui suivent les attaques s'amplifient et elles sont qualifiées de "cyberattaque mondiale" qui touchent plusieurs multinationales dont le français Saint-Gobain. Le parquet de Paris ouvre une enquête en flagrance pour "accès et maintien frauduleux dans des systèmes de traitement automatisé de données, entrave au fonctionnement de ces systèmes, extorsions et tentatives d'extorsions".

En avril 2018, des pirates informatiques ciblent l'infrastructure informatique en Russie et en Iran, avec des répercussions sur les fournisseurs de services Internet et les centres de données. Aucun vol de données n'est signalé, l'objectif aurait été d'"envoyer un message".

En août 2018, une étude menée par la société McAfee annonce une croissance importante des cyberattaques "sans fichier" extrêmement difficile à détecter.

Le 2 novembre 2018 la banque HSBC révèle un incident de sécurité touchant un nombre non précisé de clients "HSBC a appris que des utilisateurs non autorisés avaient eu accès à des comptes en ligne entre le 4 et le 14 octobre 2018".

Le 13 décembre 2018, le ministère des Affaires étrangères informe d'un piratage de sa messagerie courriel. Les noms, courriels et numéros de téléphone de "personnes à prévenir" inscrits sur une liste du ministère ont pu être dérobés.

Le 4 janvier 2019, la révélation d'une importante cyberattaque en Allemagne provoque une vive émotion. Des milliers de documents confidentiels, appartenant à des responsables politiques sont publiés en ligne. Un étudiant de 20 ans avoue avoir effectué le piratage. Aucun lien n'a été découvert avec un service de renseignement d'un pays étranger.

Fin janvier 2019, Airbus annonce avoir été victime d'une intrusion dans le système d'information de sa branche des avions commerciaux. Paradoxalement, avec sa filiale Airbus Cyber Security, l'avionneur est aussi un expert en sécurité informatique.

En mars 2019, des chercheurs de Kaspersky signalent que des centaines de milliers d'ordinateurs Asus ont été victimes d'un logiciel malveillant.

En juin 2019, les États-Unis lancent des cyberattaques contre l'Iran. Le même mois, le *New York Times* rapporte que le gouvernement américain a intensifié ses cyberattaques contre le réseau électrique russe.

Selon l'hebdomadaire : « *l'administration Trump, dans le cadre élargi d'une guerre froide numérique entre Washington et Moscou, utilise de nouveaux pouvoirs pour déployer des outils informatiques de manière plus agressive* ».

En 2020, avec la généralisation du télétravail, les cyberattaques se sont intensifiées. Neuf organisations françaises sur dix ont été ciblées cette année-là.

Le 6 avril 2021, le retour de la classe à la maison, une forte attaque informatique venue de l'étranger touchait le Centre national d'enseignement à distance (*CNED*).

Le 7 mai 2021, le Colonial Pipeline aux États-Unis cesse ses activités pendant près d'une semaine suite à une attaque ransomware.

Le cabinet d'étude PWC estime à 177.300 le nombre de cyberattaques quotidiennes à travers le monde.
En 2014, le nombre d'incidents a augmenté de 48 %. Depuis 2009, les incidents détectés ont augmenté de 66 % par an (*en moyenne*).
Par ailleurs, le coût annuel moyen attribué aux cyberattaques atteint les 2,7 millions de dollars en 2014, soit une augmentation de 34 %.
Selon la société américaine Akamai Technologies, au 2e trimestre 2014, les 10 principaux pays d'origine des cyberattaques sont :

Rang	Pays	% des Attaques
1	Chine	43
2	Indonésie	15
3	États-Unis	13
4	Taïwan	3,7
5	Inde	2,1
6	Russie	2,0
7	Brésil	1,7
8	Corée du Sud	1,4
9	Turquie	1,2
10	Roumanie	1,2
-	Autres	16

La **CYBER-DÉFENSE** regroupe l'ensemble des moyens physiques et virtuels mis en place par un pays dans le cadre de la guerre informatique menée dans le cyberespace. Selon le ministère français des armées, elle est "l'ensemble des mesures techniques et non techniques permettant à un Etat de défendre dans le cyberespace les systèmes d'informations jugés essentiels" et comme "l'ensemble des activités qu'il conduit afin d'intervenir militairement ou non dans le cyberespace pour garantir l'efficacité de l'action des forces armées, la réalisation des missions confiées et le bon fonctionnement du ministère".
La cyberdéfense rassemble, la cyber sûreté, la cybersécurité, la cyber résilience (*lutte informatique défensive*), et la cyber agression (*lutte informatique offensive*). Les approches proactives et réactives sont comprises dans certaines de leurs composantes.
En France, l'Agence nationale de la sécurité des systèmes d'information (*ANSSI*) définit la cyberdéfense comme "l'ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels".
La cyberdéfense est à différencier de la cybercriminalité qui correspond à l'ensemble des crimes et délits traditionnels ou nouveaux réalisés, via les réseaux numériques.
La cyberdéfense représente un enjeu considérable. À l'échelle planétaire, selon le magazine *Forbes* en 2015, elle portait sur un marché évalué à 75 milliards de dollars, culminant à 170 milliards de dollars en 2020.
Le cadre de la cyberdéfense dépasse la simple sécurité informatique dans la mesure où elle entraîne des conséquences directes sur la sécurité nationale et vient donc intéresser les différents organismes de Défense d'un pays. Avec la lutte informatique défensive (*LID*) et la lutte informatique offensive (*LIO*), la cyberdéfense permet de défendre et d'attaquer des ensembles de réseaux et d'ordinateurs qui contrôlent un pays.
Avec des degrés d'importances plus ou moins grands, ces réseaux et leurs systèmes de contrôle baptisés SCADAs peuvent permettre de contrôler les systèmes suivants :

- surveillance de processus industriels ;
- transport de produits chimiques ;
- systèmes municipaux d'approvisionnement en eau ;
- commande de la production d'énergie électrique ;
- distribution électrique ;
- canalisations de gaz et de pétrole ;
- recherche et études scientifiques et industrielles.

Reconnaissant le caractère critique de la cyberdéfense, la plupart des États s'emparent aujourd'hui du sujet pour le placer au cœur de leurs doctrines militaires.
En France, la cyberdéfense est essentiellement prise en charge par l'ANSSI, agence qui répond directement au premier ministre ainsi que par le centre d'expertise technique DGA MI basée à Bruz près de Rennes (*rattachée au ministère des Armées*). Elle est désormais enseignée aux élèves officiers de l'École de l'air, des écoles de Saint-Cyr-Coëtquidan (*la leçon inaugurale de la chaire de cyberdéfense et cybersécurité Saint-Cyr Sogeti Thales a été prononcée le 13 novembre 2012*) mais aussi par le centre de formation de l'École des transmissions (*ETRS*) de Cesson-Sévigné (*campus de Rennes - Beaulieu*).
Le Livre blanc sur la Défense et la Sécurité nationale de 2008 a marqué un véritable tournant, en définissant clairement la protection des systèmes d'information comme une composante à part entière de la politique française de défense et de sécurité, en préconisant la mise en place d'une stratégie de défense active en profondeur et en évoquant pour la première fois le besoin de développer des "capacités offensives".
L'Agence nationale de la sécurité des systèmes d'information (*ANSSI*) a été créée le 7 juillet 2009, par un décret du Premier ministre, en remplacement de la direction centrale de la sécurité des systèmes d'information (*DCSSI*) du secrétariat général de la défense et nationale, tout en renforçant ses attributions, ses effectifs et ses moyens.
Depuis le 1er janvier 2017, le **Commandement de la cyberdéfense** (*COMCYBER*) rassemble l'ensemble des forces de cyberdéfense des armées françaises sous une même autorité opérationnelle, permanente et interarmées. Placé sous l'autorité du Chef d'État-Major des armées, le COMCYBER est responsable de la protection des systèmes d'information placés sous sa responsabilité, de la conduite de la défense des systèmes d'information du ministère (*à l'exclusion de ceux de la DGSE et DRSD*) et de la conception, de la planification et de la conduite des opérations militaires de cyberdéfense, sous l'autorité du sous-chef d'état-major "opérations". Il est également responsable de la préparation de l'avenir et de la politique du domaine cyber.
Le COMCYBER assiste et conseille le ministre des Armées dans son domaine de compétence. Il dispose d'un état-major (*EM-CYBER, à Paris*) avec un centre des opérations CYBER (*CO-CYBER*).
Le COMCYBER a près de 3400 cyber-combattants sous sa responsabilité. La Loi de Programmation Militaire 2019 – 2025 prévoit le recrutement de plus de 1000 nouveaux cyber-combattants.
Les entreprises liées à la cyberdéfense sont de plus en plus nombreuses. Parmi celles-ci, on trouve en France Airbus CyberSecurity (*filiale de Airbus Defence and Space*), Thales, CS, DCNS, ou encore le Groupe Orange, qui a développé depuis 2016 sa filiale Orange Cyberdéfense.

La **CYBER-GUERRE**, **guerre cybernétique** (*en anglais : cyberwarfare*) ou **guerre de la toile** consiste en l'utilisation d'ordinateurs et d'Internet pour mener une guerre dans le cyberespace.
Depuis le début du XXIe siècle, le réseau global est devenu un lieu de confrontation militaire majeur. L'utilisation d'Internet permet de s'infiltrer rapidement dans tous les réseaux les plus sensibles du monde. De nouveaux champs de bataille se sont organisés avec comme cibles les sites et organisations gouvernementales, les institutions, les grandes et moyennes entreprises, les organisations privées et les particuliers. Les acteurs de ces attaques sont les groupements de pirates informatiques, les organisations terroristes, les escrocs de tous genres mais aussi les armées et les organisations gouvernementales.
Rencontré dans certains romans de science-fiction, le blocage informatique des moyens informatiques et donc des centres de commandements ou de transmission d'information est une pratique redoutée par les personnes préoccupées par la sécurité informatique. Les virus informatiques, les vers informatiques et les dénis de services sont les premières armes de ce type d'attaque.
L'attaque informatique nécessite peu de moyens et peu d'hommes. Une centaine d'ingénieurs informatiques et de hackers suffisent pour infiltrer ou bloquer une partie du réseau mondial, bien qu'une attaque de type Stuxnet, Flame ou mini-Flame demande beaucoup plus de capacité informatique et l'intervention de services secrets. Les pays les plus développés et les plus dématérialisés sont aussi les plus vulnérables d'autant plus que certains d'entre eux présentent d'importantes lacunes dans leur sécurité informatique.
Il existe plusieurs méthodes d'attaques, cette liste les recense de la plus anodine à la plus grave :

- le vandalisme : attaques visant à modifier ou défigurer des pages web, ou les attaques de déni de service. Ce type est simple à combattre et cause généralement peu de dommages ;

- la propagande et la désinformation : des messages politiques (*ou autres*) peuvent "bombarder" tout utilisateur de l'Internet ;
- l'espionnage politique/industriel ou la collecte de données (*à l'aide de chevaux de Troie et de spywares*) : des informations confidentielles qui ne sont pas correctement sécurisées peuvent être interceptées et modifiées, rendant possible l'espionnage d'un bout à l'autre du monde ;
- l'arrêt ou le sabotage d'équipements : les activités militaires qui mettent en œuvre des ordinateurs et des satellites permettant de coordonner des moyens de défense sont particulièrement visés par ce type d'attaques. Les ordres et les communications peuvent être interceptés ou modifiés, mettant ainsi les troupes en danger ;
- attaques d'infrastructures sensibles : centrales électriques, distribution d'eau, oléoducs et pétroliers, communications et moyens de transports sont vulnérables à ce genre d'attaques.

En 1999, les colonels chinois Qiao Liang et Wang Xiangsui imaginaient dans *La Guerre hors limites* que l'informatique pourrait devenir l'une des armes du XXIe siècle. La Chine a créé un corps d'armée de 9,600 hommes affecté au cyberespace. Aujourd'hui l'armée chinoise est régulièrement accusée de vouloir attaquer les systèmes informatiques américains par le *US Secretary of Defense*.
La Grande-Bretagne a annoncé en mai 2011 se doter de capacités offensives en matière de cyberguerre, et plus seulement défensives. Le ministre de la Défense, Nick Harvey, estime que "le cybermonde fera désormais partie du champ de bataille de l'avenir".

Le **HARCÈLEMENT ÉLECTROMAGNÉTIQUE** (***HEM***), aussi appelé **torture électronique**, consiste en l'attaque d'une ou plusieurs personnes de manière répétée, à l'aide de moyens électromagnétiques. Des cas ont été relevés à Cuba, en Chine, en Russie et aux États-Unis dans des attaques ayant visé des diplomates et agents américains et canadiens. Les rayonnements électromagnétiques ont des effets biologiques comme on peut le constater dans la littérature scientifique, ou, par exemple, par une agence de renseignement de la défense américaine.
Par ailleurs, de nombreuses personnes se prétendant victimes de harcèlement ou de torture électromagnétique ne présentent pas de preuves suffisantes pour étayer leurs allégations. Ces dernières sont ainsi qualifiées de "théories de complot".
Les personnes se décrivent comme subissant un harcèlement électromagnétique par des moyens technologiques avancés, qui les visent personnellement. Le symptôme commun est d'entendre des voix dans leurs têtes, les appelant par leur nom, souvent en se moquant d'eux ou d'autres personnes de leur entourage, ainsi que les sensations physiques comme des brûlures.
Les personnes victimes de harcèlement électromagnétique peuvent également être victimes de "stalking", ce qui consiste à être constamment sous la surveillance d'une ou plusieurs personnes (*stalking en groupe*).
Certaines personnes se plaignent d'un bombardement continu d'ondes, sans qu'il n'y ait eu d'intervention physique (opération chirurgicale) sur leur propre personne. Le Dr Allan Frey décrit de telles ondes auditives.

Dans d'autres cas, certaines personnes auraient eu un implant greffé dans leur cerveau, qui amplifiait les ondes. Les expériences de la CIA menées sur la jeune femme Karen Wetmore sont de cet ordre.
Aux États-Unis, une forme particulière est l'enlèvement par extraterrestres (*alien abduction)* où la personne enlevée subit des implants extraterrestres destinés à la surveiller et à la contrôler.

Le projet HAARP est un authentique projet de recherche sur l'ionosphère, existant depuis 1990 et situé en Alaska. Le fait qu'il soit soutenu par l'armée américaine a fait suggérer qu'il s'agirait en fait de recherches sur une arme météorologique, de rupture des communications et réseaux informatiques de l'ennemi et une arme électromagnétique de contrôle mental par ondes et fréquences particulières.

Dans la foulée, se sont surajoutés de nombreux programmes imaginaires de même type : « *RHIC-Edom* » pour fabriquer des assassins par ondes et radiations, « *Monarch* » pour provoquer par hypnose, et stimuli audio-visuels une personnalité multiple et en contrôler l'une d'entre elles.

Les révélations de ces projets, ainsi que la présentation détaillée de ces armes et procédés secrets font l'objet d'une abondante littérature suscitant la formation de communautés, pouvant se réunir en congrès annuel notamment aux États-Unis. Ces groupes peuvent développer une sous-culture et générer une activité commerciale (*leaders auteurs-conférenciers, vente de livres, conférences payantes, vente de méthodes, produits et appareils permettant de se défendre contre le contrôle mental*).
Barrie Trower ex. agent secret a dénoncé l'utilisation de micro-ondes pour contrôler les populations dans une interview en 2012.

En France, les autorités appellent le harcèlement électronique "AGRÉMI", pour Agressions Électromagnétiques Intentionnelles. Mais cette appellation ne concerne que les attaques contre les systèmes informatiques et non contre les personnes.
Toute personne peut par exemple solliciter l'Agence Nationale des Fréquences (*ANFR*) pour la réalisation de mesures de l'exposition aux ondes électromagnétiques.

Aux États-Unis les armes psychotroniques sont mentionnées dans le "space preservation Act of 2001". Il s'agit d'une proposition de loi interdisant l'utilisation dans le cosmos d'un certain nombre d'armes, réelles ou imaginaires. Cette proposition a été déposée par le député démocrate Dennis Kucinich, à la demande de certains de ses électeurs aux influences new Age mais il ne l'a pas rédigé lui-même.

Fin 2016 une trentaine de diplomates en poste à Cuba (*principalement américains mais aussi canadiens*) présentèrent des symptômes physiques allant jusqu'à des lésions cérébrales. Les autorités américaines rendent publics les faits en 2017, parlant d'"attaques soniques", puis en 2018 parlant de micro-ondes.
Des armes à micro - ondes ont été mentionnées pour cette attaque notamment par la CNN.
L'Académie des sciences américaine a finalement conclu que la source la plus plausible de ces attaques était des radiofréquences pulsées et dirigées, radiofréquences qui comprennent les micro-ondes.
En 2018 un diplomate américain en poste en Chine a présenté des symptômes similaires. La presse parle d'"attaques acoustiques".

Le **RENSEIGNEMENT D'ORIGINE ÉLECTROMAGNÉTIQUE** ou ROEM est un renseignement dont les sources d'information sont des signaux électromagnétiques : communications utilisant les ondes (*radio, satellitaire*), émissions d'ondes faites par un radar ou par des instruments de télémesure. Le plus célèbre réseau ROEM est le système Échelon, développé principalement par des États anglo-saxons dans le cadre du traité UKUSA de 1946, et connu du grand public depuis les années 1990. Outre les écoutes téléphoniques, le ROEM comprend donc la surveillance des télégrammes, des télécopieurs, des courriers électroniques et autres sortes de communications électroniques, facilitant l'espionnage industriel et posant d'évidents problèmes de respect de la vie privée.

***Dupuy-de-Lôme*, navire collecteur de renseignements d'origine électromagnétique de la Marine nationale**.

Par extension, le ROEM désigne toutes les activités liées à la collecte et à l'analyse des signaux et à l'obtention de tels renseignements. Le ROEM se définit par opposition au renseignement d'origine humaine (*ROHUM*), au renseignement d'origine source ouverte (*ROSO*), et au renseignement d'origine image (*ROIM*).

Les signaux peuvent être répartis en trois types principaux, et pour chacun il existe un terme :

- renseignement issu de l'interception de télécommunications, COMINT (*Communications Intelligence*).
- renseignement électronique, ELINT (*Electronic Intelligence*) : renseignement obtenu à partir des émissions électromagnétiques hors communications. Cette discipline s'applique principalement pour les émissions radar. Elle permet de caractériser précisément ce qui est physiquement émis par un émetteur. Cette étape est essentielle pour l'identification des signaux et pour les contre-mesures (*brouillage, leurrage*).
- renseignement tiré de signaux d'instrumentation étrangers, FISINT (*Foreign Instrumentation Signals Intelligence*) : écoute de transmissions d'instrumentations installées dans des systèmes aérospatiaux, de surface ou sous-marins étrangers. Par exemple la télémesure d'un système en cours de test, les systèmes de poursuites ou la transmission d'images vidéo d'un drone. Les signaux de télémesure des missiles balistiques intercontinentaux (*ICBM - Telemetry Intelligence ou TELINT*) sont un élément important de contrôle des traités de réductions d'armements.

Le renseignement mesures et signature (*MASINT : Measurement and Signature Intelligence*), diffère au ROEM dans le sens où il concerne les signaux émis involontairement par les systèmes adverses, comme le bruit d'un char ou la cavitation des hélices de navires. À noter que ces signaux peuvent être d'origine électromagnétique ou non.

Le renseignement d'origine électromagnétique doit d'abord être distingué des interceptions de communications (*telles les écoutes téléphoniques*) pratiquées par la police et placées sous la supervision du pouvoir judiciaire. En effet, étant assuré par les services de renseignement, le ROEM n'est pas soumis à autorisation des instances judiciaires.

La confidentialité des communications internationales est pourtant protégée, en théorie, par la Convention des télécommunications internationales (*art. 22*), la Convention de Vienne sur les relations diplomatiques (*1961, art. 27 et 30*), la Déclaration universelle des droits de l'homme (*art. 12 sur la protection de la vie privée*), de même que la Convention européenne des droits de l'homme (*art. 8*) et le quatrième amendement à la Constitution des États-Unis. De plus, un groupe de travail spécifique, visant à protéger les données personnelles dans le domaine des télécommunications, de la Conférence internationale sur la protection des données personnelles, le *International Working Group on Data Protection in Telecommunications* (*IWGDPT*), est mis en place en 1983.

Le ROEM se distingue en outre des interceptions opérées par la police, en ce sens que cette dernière vise normalement une ligne spécifique ou un groupe de lignes, tandis que le ROEM conduit des "pêches" aux communications internationales, et n'a pas besoin que les correspondants interceptés soient supposés criminels.
Le ROEM s'effectue en trois phases : la planification, c'est-à-dire l'identification de l'information demandée par les consommateurs (*ministères, etc.*) ; l'accès et la collecte des données ; enfin le traitement de celles-ci, qui permet leur diffusion ultérieure aux consommateurs intéressés.
La collecte de COMINT ne peut avoir lieu qu'avec l'accès à l'infrastructure de télécommunications, accès obtenu à la fois avec la complicité des opérateurs de télécommunications et à leur insu.
Puisque les informations importantes sont souvent chiffrées, le ROEM demande souvent de recourir à la cryptanalyse. Cependant, l'attaque par analyse du trafic (*qui envoie à qui et le volume du trafic*) produit régulièrement des informations importantes, même si les messages ne peuvent être décryptés. Par exemple, Alice envoie à Benoît une vingtaine de messages chiffrés. Or, Benoît est connu des services secrets, mais pas Alice. Conclusion : Alice a probablement un lien avec Benoît. Elle est donc à surveiller.

Avec la modernisation des méthodes de communications, le ROEM est devenu plus important pour les forces armées et pour le corps diplomatique. Pendant la Première Guerre mondiale, l'armée russe subit une importante défaite par les Allemands lors de la bataille de Tannenberg. La cause principale de celle-ci fut une protection insuffisante des moyens de communications russes. L'entrée en guerre des États-Unis à cette époque est largement attribuée à l'interception et au décryptage du télégramme Zimmermann.

Le ROEM s'est illustré lors de la Seconde Guerre mondiale. La rapidité du *Blitzkrieg* et l'activité des sous-marins allemands ont incité les armées alliées à en améliorer les techniques. Les Britanniques, niant son importance au début de la guerre, perdirent ainsi le *HMS Glorious* en 1940. D'un autre côté, les Polonais parvinrent à mettre la main sur une machine Enigma et commencèrent à travailler au déchiffrement des messages créés par celle-ci. À la suite de l'invasion de la Pologne par l'Allemagne, la machine allemande et les travaux polonais furent repris par les Britanniques. Cette opération, maintenant connue sous le nom d'Ultra, était essentiellement effectuée depuis Station X à Bletchley Park, Alan Turing étant le membre le plus connu de cette équipe. Elle permit plusieurs victoires alliées décisives lors de la Seconde Guerre mondiale, comme la victoire américaine lors de la bataille de Midway (*juin 1942*), et facilita les travaux du nouveau *Special Services Branch*, mis en place en juin 1942 (*au même moment que l'OSS*).

Les Américains, de leur côté, parvinrent à "briser" les messages chiffrés par le code JN-25 japonais. Connaissant les intentions japonaises, l'amiral Nimitz vainquit les Japonais lors de la bataille de Midway, six mois seulement après la défaite américaine à Pearl Harbor. Le décryptage des messages japonais permit aussi d'apprendre le trajet que l'amiral Yamamoto devait prendre, et ainsi d'abattre l'avion qui le transportait en avril 1943.

De 1945 à 1975, la *National Security Agency* (*NSA*) américaine a obtenu systématiquement des principales entreprises de télégraphie (*RCA global, ITT World Communications et la Western Union*) l'accès aux messages circulant par câble. L'interception des télécommunications se faisait au départ par la collecte de copies papier de télégrammes, puis par la remise de bandes magnétiques. Selon la commission Church du Sénat américain (*1975*), la NSA sélectionnait environ 150 000 messages par mois, sur un total de 6 millions de messages par mois, pour en faire un compte rendu (*soit 1 message sur 40*). Des milliers de messages étaient transférés à d'autres agences de renseignement pour analyse. Lew Allen, alors directeur de la NSA, reconnaissait le 8 août 1975, devant la commission Pike, que "la NSA interceptait systématiquement les communications internationales, les appels téléphoniques comme les messages câblés", dont "des messages adressés à des citoyens américains ou émanant d'eux".

De 1945 au début des années 1980, la NSA et le Government Communications Headquarters (*GCHQ*) britannique possédaient en Europe des systèmes d'interception radio HF. Le système le plus perfectionné était le système AN/FLR-9, installé en 1964 à San Vito dei Normanni (*Italie*), à Chicksands (*Angleterre*) et à Karamürsel (*Turquie*). La base de Chicksands devait intercepter d'abord les communications des forces

aériennes des États membres du pacte de Varsovie, mais aussi les communications diplomatiques non-américaines (*unité DODJOCC*), en priorité desquelles les communications diplomatiques françaises.

Le premier satellite d'écoute électronique de type COMINT des États-Unis a été lancé en août 1968 (*Canyon*), rapidement suivi par un second ; sept satellites Canyon ont été lancés entre 1968 et 1977. Chargés d'intercepter les ondes radio ultra-courtes des réseaux interurbains et visant en particulier l'URSS, ils étaient contrôlés depuis Bad Aibling (*RFA*). CANYON devint rapidement l'un des projets les plus importants de la NSA, et fut suivi par une nouvelle génération de satellites (*Chalet*), dirigés depuis Menwith Hill (*Angleterre*). Le premier satellite Chalet a été lancé en juin 1978, suivi d'un deuxième en octobre 1979. Leur nom ayant été publié dans la presse américaine, ils furent alors rebaptisés VORTEX.

Après la dégradation des rapports avec l'URSS et l'élection de Reagan, la NSA obtint en 1982 des fonds et du matériel pour faire fonctionner quatre satellites Vortex à Menwith Hill, construisant alors un nouveau centre d'opérations de 5 000 m. En 1987, à la suite de nouvelles publications dans la presse, ces satellites furent rebaptisés Mercury.

En 1985, Washington donna pour mission à Menwith Hill la collecte des informations en provenance du Moyen-Orient. La base fut récompensée pour ses contributions lors des opérations navales du Pentagone dans le golfe Persique, de 1987 à 1988 (*lors de la guerre Iran-Irak*), puis à nouveau pour son soutien aux opérations Tempête du désert et Bouclier du désert lors de la guerre du Golfe de 1991. Menwith Hill est aujourd'hui le principal site d'espionnage COMINT des États-Unis dirigé contre Israël. De nouveaux satellites ont été lancés en 1994 et 1995.

Parallèlement, une autre classe de satellites ROEM (*Rhyolite, Aquacade, Magnum, Orion*) a été développée par la CIA de 1967 à 1985. Dirigés à partir d'une base située à Pine Gap, en Australie, ils ciblaient la télémesure, les ondes radio très haute fréquence (*VHF*), les téléphones mobiles, les messages des "pagers″ ainsi que les liens de transmission des données informatiques.

Chaque satellite et son appareil de maintenance vaut environ un milliard de dollars. Les principales bases sont Buckley Air Force Base, près de Denver ; Pine Gap, Australie ; Menwith Hill, Angleterre et Bad Aibling, en Allemagne.

Pour des raisons techniques et de coût, selon le journaliste Duncan Campbell, auteur d'un rapport pour le Parlement européen sur le sujet, « *bien que les communications européennes passant sur des ondes radio interurbaines soient hautement vulnérables et puissent facilement être collectées, il est vraisemblable qu'elles sont généralement ignorées. Il est en revanche très hautement probable que les communications qui entrent et sortent d'Europe en passant par les réseaux de communications hertziens des États du Moyen-Orient sont collectées et traitées.* »

La Russie a lancé le 27 septembre 2014 une fusée Proton-M. Le satellite mis en orbite était classifié, souvent présenté comme étant un satellite de télécommunications Loutch qui habituellement ne sont pas l'objet d'un tel secret. Selon le journal russe *Kommersant*, il s'agirait du premier satellite géostationnaire d'écoute électronique de la Russie, de type "Olymp-K" (Олимп (*Olimp*).

Depuis 1971, les États membres de l'UKUSA interceptent systématiquement les communications satellitaires, dirigée par Intelsat (*International Telecommunications Satellite Consortium*). Aux deux premières bases (*Morwenstow, en Cornouailles, et Yakima*) fut rajoutée, à la fin des années 1970, la base de Sugar Grove, en Virginie. Ce système d'interception fut considérablement développé entre 1985 et 1995, en conjonction avec l'élargissement du système de traitement Échelon. Des bases furent construites à Sabana Seca, Porto Rico ; Guam, Pacifique ; SFC Leitrim au Canada ; Kojarena, Australie ; Waihopai, Nouvelle-Zélande ; et Paramaly, à Chypre, en 2000. Les nations de l'UKUSA disposeraient aujourd'hui d'au moins 200 systèmes de collecte par satellite.

D'autres pays intercepteraient aussi ces communications. La FAPSI russe possédait des bases à Lourdes (*Cuba*), et à Cam Ranh au Viêt Nam, mais le président Vladimir Poutine a annoncé en 2001 leur fermeture, afin d'économiser 200 millions de dollars par an et d'améliorer les relations avec Washington (*le Congrès américain avait voté, en mai 2000, en faveur d'une restriction de l'aide financière apportée à la Russie tant que la base de Cuba restait ouverte ; la base vietnamienne, elle, devait être fermée en 2004*) ; la DGSE française et le BND allemand sont soupçonnées de collaborer dans la base de Kourou, en Guyane, qui cibleraient les communications américaines et sud-américaines par satellite. La DGSE aurait aussi des sites en Nouvelle-Calédonie et dans les Émirats arabes unis, tandis que les services de renseignement suisses ont trois bases d'interception COMSAT dans le cadre du programme Onyx, un système lancé en 2000.

De 1990 à 1998, le GCHQ a intercepté les communications terrestres (*fax, courriels, télex et communications informatiques*) entrant et sortant de l'Irlande via la tour hertzienne de Capenhurst, située sur le terrain d'une centrale nucléaire et fonctionnant 24 heures sur 24. Les communications internationales de l'Irlande transitaient alors via le câble de fibres optiques UK-Ireland I, avant d'être transmises à travers le réseau de tours de "relais-radio" hertzien de British Telecom, centralisé dans la tour de la BT à Londres, mais qui passait au-dessus de Capenhurst. Outre des informations sur le terrorisme, la tour de Capenhurst servait à l'espionnage industriel ainsi qu'à l'interception des communications diplomatiques de l'Irlande et des communications personnelles de résidents irlandais notables, à l'aide de listes ciblées de numéros de téléphone ou de systèmes de reconnaissance vocale. La tour ferma en 1998, les liaisons radio ayant été remplacées par un nouveau câble de fibres optiques, qui collectent aujourd'hui les communications internationales transitant par le Royaume-Uni avant de les transmettre au GCHQ à Cheltenham. Une base similaire, plus petite, était installée dans le comté d'Armagh, tandis que les communications commerciales par satellite pouvaient être interceptées par Echelon.

La Cour européenne des droits de l'homme a donné gain de cause, le 1er juillet 2008, aux ONG *Liberty Human Rights*, le *British Irish Rights Watch* et le *Irish Council for Civil Liberties*, qui avaient porté plainte contre le Royaume-Uni et l'Irlande du Nord, en 2000. Les ONG affirmaient que leur droit à la vie privée, garanti par l'article 8 de la Convention européenne des droits de l'homme, avait été violé, notamment du fait d'imprécisions dans la formulation de la loi de 1985 régulant les interceptions de communications (*Interception of Communications Act 1985*).

De 1972 à 1981, le Pentagone intercepta les communications soviétiques sur un câble sous-marin de la mer d'Okhotsk à l'aide du sous-marin USS Halibut (*SSN-587*) et de deux autres sous-marins, l'USS Seawolf (*SSN-575*) puis l'USS Parche (*SSN-683*). Ces navires entraient dans les eaux territoriales soviétiques, localisaient le câble subaquatique, et attachaient sur celui-ci un "pod", un conteneur étanche contenant des systèmes d'écoute de câbles par induction et des bandes enregistreuses. Les bandes enregistreuses étaient récupérées par un sous-marin environ une fois par an. Le *Halibut* reçut une *Presidential Unit Citation* pour ses opérations complexes et très productives en 1972. Selon une personne ayant connaissance des détails du programme : « *la "pêche" issue du programme fournit les seules interceptions non chiffrées des messages du commandement militaire soviétique. Nous avions tout, des informations technologiques aux procédures de commandement, en passant par les habitudes opérationnelles, les localisations habituelles d'unités, les plans, une base pour la cryptanalyse et bien plus*. »

L'opération Ivy Bells fut trahie en 1980 par l'employé de la NSA Ronald Pelton qui en informa le KGB contre le paiement de 35 000 dollars. En 1981, les deux pods fixés sur le câble de la mer d'Okhotsk furent remontés par un navire câblier de la marine soviétique ; une de ces nacelles d'Ivy Bells est maintenant exposée au musée de l'ancien KGB à Moscou.

Une opération d'écoute des câbles situés dans la mer de Barents, elle, n'a jamais été détectée. La mer de Barents étant peu profonde et très patrouillée par la marine soviétique, l'opération ne put commencer qu'après l'entrée en service de l'USS *Parche*, un sous-marin espion bien plus moderne que le *Halibut* et le *Seawolf*. L'opération fut autorisée par le président Jimmy Carter en 1978 et commença en 1979 lorsque le *Parche* installa un pod sur un câble près de Mourmansk. Comme les soviétiques avaient remonté les pods d'Ivy Bells en mer d'Okhotsk, les pods utilisés à partir de 1982 étaient conçus pour se détacher et rester au fond de la mer si les câbles étaient relevés pour inspection. Le programme d'écoute avait reçu le nom de code Manta et l'opération de branchement s'appelait Acetone, codes qui furent ensuite régulièrement changés. Les écoutes en mer de Barents se seraient prolongées sans jamais être détectées jusqu'en 1992.

Ce système avait pour désavantage qu'il s'écoulait plusieurs mois entre le moment où les communications étaient interceptées et le moment où elles étaient analysées, le temps qu'un sous-marin vienne relever les bandes enregistreuses. Une idée qui émergea au milieu des années 1970 était de poser clandestinement un câble sous-marin du branchement d'écoute jusqu'au Japon, où les interceptions pourraient être analysées en temps réel. Par la suite, une idée similaire fut lancée pour le branchement en mer de Barents, avec un câble allant jusqu'au Groenland. Ces projets, estimés à plus d'un milliard de dollars, ne furent jamais mis en œuvre.

En 1986, ces opérations furent élargies à la mer Méditerranée. L'USS Seawolf et le NR-1 mirent sur écoute un câble reliant l'Afrique de l'Ouest à l'Europe à une époque où les États-Unis étaient engagés dans une confrontation avec la Libye.

Il n'y a pas d'informations disponibles sur d'éventuelles opérations d'écoutes ultérieures. Cependant, on peut noter que le rôle du Parche était suffisamment important pour justifier une modification majeure du sous-marin lors d'une grande refonte qui dura de 1987 à 1991 et comprenait notamment l'allongement de 30 m de long de sa coque. Pendant cette période, les missions furent reprises par un autre sous-marin spécialement modifié,

l'USS Richard B. Russell (*SSN-687*). Pendant ses périodes d'activité de 1979 à 1986 et de 1993 à 1998, le Parche a été régulièrement décoré des deux plus hautes décorations collectives que les sous-marins peuvent recevoir.

Les États-Unis seraient le seul pays à avoir développé cette technologie d'interception des communications. À noter qu'en 1985, le USS Baltimore (*SSN-704*) observa un sous-marin soviétique classe Zoulou IV en mer de Norvège s'entraînant à des travaux sous-marins qui pourraient être la mise sur écoute ou le sabotage d'un câble sous-marin.

Au cours des années 1990, les câbles en fibre optiques ont de plus en plus remplacé les satellites de télécommunications pour transmettre les communications internationales. Or, ces câbles sont beaucoup plus difficiles à intercepter que les transmissions des satellites qui utilisent des ondes radio.

En 1999, le public apprit que l'USS Jimmy Carter (*SSN-23*), le dernier sous-marin de la classe Seawolf, la classe de sous-marins nucléaires la plus récente de l'US Navy, allait être réaménagé en vue d'opérations de renseignement clandestin, pour un coût de 400 millions de dollars. Un an et demi plus tard, le coût de la conversion du Jimmy Carter était estimé à un milliard de dollars, dans le but, entre autres, de mettre sur écoute les câbles à fibres optiques. Le Jimmy Carter a été lancé en 2005.

Selon un article du Wall Street Journal, la NSA aurait au moins expérimenté la mise sur écoute d'un câble sous-marin à fibre optique au milieu des années 1990. Les résultats auraient été mitigés, pas tant à cause de la difficulté à placer une écoute mais plutôt en raison du volume important de données interceptées dans ce type de câble très haut débit, qui rend difficile le tri pour en tirer les communications présentant un intérêt pour les services de renseignement.

ANNEXE 8

Faisceau hertzien (*FH*) : comment ça marche ? points positifs et négatifs

L'ADSL et la fibre sont les moyens de connexions les plus connus. Parfois coûteux, inaccessibles en zone rurale ou montagneuse, non fiables ou au débit ralenti, il peut être intéressant de porter sa réflexion vers une autre technologie. **La technologie du Faisceau Hertzien (*FH*) est une bonne solution lorsque les besoins du professionnel en matière de connectivité doivent être plus puissants, en zones géographiques à risques ou "blanches".** On détaillera ici, son mode de fonctionnement, les facteurs perturbateurs, ses avantages et ses inconvénients, son utilité pour les professionnels ou encore son histoire. Le faisceau hertzien (*FH*) est proposé par des fournisseurs au sein de leurs offres et services.

Le faisceau hertzien est une technologie permettant la transmission d'informations et de données d'un point A à un point B par l'intermédiaire d'ondes radioélectriques, dont les fréquences sont comprises entre 1 et 86 Ghz. Ce dispositif "sans fil" peut être rapproché du wifi domestique et dispose de nombreux avantages. Cette technologie s'améliore continuellement, stimulée par de nombreuses recherches scientifiques. Le signal source (*vidéo, audio, données, texte, etc*.) à retransmettre est transposé en fréquence par modulation. L'opération de modulation transforme le signal d'origine en bande de base, par un signal modulé dit "à bande étroite", dans une bande passante définie et conforme aux normes exploitées.

En février 2013, le gouvernement a partagé son ambition de croissance, notamment au travers du développement du numérique sur le territoire. Pour cela, le Président de la République a alloué un budget annoncé de 20 milliards d'euros sur les 10 ans à venir afin d'accroître l'accès au très haut débit. L'objectif du gouvernement est de proposer à horizon 2022, un accès à une connexion internet d'au moins 30 Mb/s à toute la population française, surtout en zones rurales et difficiles d'un point de vue topographique. Pour ce faire, l'état souhaite notamment s'appuyer sur le faisceau hertzien (*FH*).
Afin de préciser les besoins et les enjeux deux cahiers des charges ont été conçus. Un datant de 2013 et l'autre de 2015.

Le faisceau hertzien semble être le moyen de communication parfait pour les connexions avec les objets mobiles : les automobiles, les trains, les bateaux, les avions, les satellites, les piétons etc. Cette technologie est intéressante notamment dans le cadre de la diffusion d'un émetteur à plusieurs récepteurs.
Par exemple, à l'échelle d'une ville, il paraît plus intéressant et moins coûteux de mettre en place un seul émetteur et une antenne chez chaque particulier, plutôt que de les relier les uns aux autres avec un câble.

Une onde radioélectrique moins coûteuse - Ces ondes radioélectriques sont focalisées et concentrées grâce à des antennes directives. Afin que les ondes arrivent à bon port lors de longues distances géographiques, le trajet hertzien entre deux équipements d'extrémité est la plupart du temps sectionné en plusieurs tronçons ou "bonds", grâce à des stations relais. On peut opposer le faisceau hertzien à la fibre optique qui demande d'importants travaux de génie civil et nécessite un support physique entre l'émetteur et le récepteur.

Une technologie "sans fil" - Le faisceau hertzien grâce à sa technologie "sans fil", ne requiert pas d'acceptation des propriétaires des terrains traversés. En effet, dès lors que l'ARCEP a validé l'installation de la connexion entre deux antennes relais aucune autre demande n'est requise.
Le faisceau hertzien semble être une des meilleures solutions pour développer l'installation d'internet au sein de secteurs topographies difficiles tels que les zones de montages, rurales etc.
Le faisceau hertzien peut être considéré comme un pont radio en bande réservée, soit une fréquence radio privée et certifiée par l'ARCEP. Des antennes directives converties au numérique peuvent effectuer le relai. A contrario, la fibre utilise une bande passante, plusieurs usagers peuvent la partager. Aussi, les "points" intermédiaires dans les réseaux de fibre sont plus nombreux. Ces deux éléments amenant plus de latence.

L'installation d'un faisceau hertzien est proposée par des opérateurs de réseaux. Une étude de terrain et de faisabilité est alors nécessaire :

1. En fonction de l'adresse de l'entreprise concernée, un premier pronostique de faisabilité peut être prononcé ainsi qu'un budget prévisionnel ;

2. À la suite d'un premier accord de principe, l'opérateur se rend sur le terrain afin d'effectuer une étude approfondie ;
3. Une fois la faisabilité du projet confirmée, la commande est alors déployée dans un délai de 8 à 20 semaines, en fonction de l'opérateur.

Le tarif de l'installation du faisceau hertzien est bien entendu calibré en fonction du projet, il inclut :

- Les frais d'accès aux services : les frais du déploiement et du raccordement de l'antenne ;
- Un abonnement mensuel : variable en fonction du débit, du réseau de l'opérateur et de la zone géographique de l'entreprise.

Pour élaborer avec précision l'ingénierie de liaisons hertziennes en vue directe, il convient de suivre la recommandation UIT-R P.530-8 (*ou supérieure*), laquelle définit les paramètres de propagation les plus significatifs.

Calcul du bilan de liaison

La station émettrice rayonne, traversant le territoire afin d'atteindre le récepteur. L'énergie que la station déploie décroit au fur et à mesure qu'elle avance vers le récepteur. Il est donc important d'étudier le trajet parcouru et de veiller à adapter les éléments qui l'entourent et qui peuvent affecter son déploiement.

Les caractéristiques des équipements d'extrémité à prendre en compte pour le calcul du bilan énergétique sont :

- Puissance d'émission : c'est la puissance du signal que l'équipement hertzien peut délivrer. Elle est couramment comprise entre 20 et 30 dBm.
- Seuils de réception : définis par rapport à un taux d'erreur binaire donné (*TEB = 10^{-3} ou 10^{-6}*), ils traduisent la capacité pour le récepteur à traiter le signal affaibli après propagation (*vis-à-vis du bruit thermique*). Dépendant de la bande de fréquences, du débit et du type de modulation, ils sont généralement compris entre −70 et −95 dBm.
- Pertes de branchement (*guide d'onde, connectique*…) : pour les équipements ne présentant pas d'antennes intégrée, il est nécessaire de relier par un câble coaxial ou un guide d'onde l'émetteur/récepteur à l'antenne. Ces déports induisent des pertes linéiques de 1 à plusieurs dB, auxquels s'ajoutent les pertes dues aux connecteurs et autres éléments de branchements.
- Gain de l'antenne : les antennes, principalement paraboliques, apportent un gain de puissance (*de l'ordre de 25 à 45 dB*) d'autant plus grand que leur diamètre est important. La directivité du faisceau augmente avec la bande de fréquences et les diamètres de l'antenne.

L'obtention du bilan de liaison repose sur le constat simple : la station distante doit recevoir un signal tel qu'elle puisse le retranscrire avec un taux d'erreur acceptable, au regard des exigences de qualité de la liaison. Le bilan de liaison, sommation de la puissance émise et de tous les gains et les pertes rencontrés jusqu'au récepteur, doit donc être tel que le niveau de signal reçu soit supérieur au seuil de réception.

Cependant, si les caractéristiques d'émission/réception du FH jusqu'à l'antenne peuvent être connus avec précision, il est en revanche impossible de connaître à tout instant les caractéristiques du milieu traversé par les ondes.

Étant donné les conditions fluctuantes de propagation qui peuvent dégrader voire interrompre occasionnellement la liaison, on définit en réception les marges de fonctionnement permettant de remplir ces critères :

- Marge au seuil : pour compenser la majorité des pertes occasionnelles de puissance (*évanouissements non sélectifs*) que subit le signal, la réception se fait avec une marge appelée "marge uniforme" ou "marge au seuil". C'est la puissance que l'on pourra perdre par dégradation des conditions de propagation sans perdre pour autant affecter les performances la liaison.
- Marge sélective : comme déjà indiqué, le signal ne subit pas qu'un affaiblissement au cours de la propagation. Il subit également des distorsions. Cela complique encore la tâche de réception. Pour traduire la capacité d'un équipement à traduire correctement un signal entaché de distorsion (*superposition du signal direct avec ses répliques retardées*), on introduit une marge dite sélective, qui découle de la caractéristique de signature du récepteur.

La présence d'un perturbateur (*par exemple une autre liaison émettant sur une fréquence trop proche*) peut également amener une dégradation du seuil effectif du récepteur, et réduit par conséquent ces marges.

Des dispositifs permettent d'améliorer la disponibilité et la qualité des liaisons, aussi bien vis-à-vis des aléas de propagation que de la fiabilité des équipements. Il est par exemple possible de doubler la liaison mais il existe des moyens moins lourds et moins coûteux.

Il est possible d'opter pour une configuration d'équipement dite de "veille active" (*Hot-stand-by*), afin de pallier les éventuelles défaillances de matériels. On peut également ajouter une "diversité" : il s'agit d'un deuxième canal distinct à la liaison. À l'émission, en cas de défaillance de l'émetteur, on bascule automatiquement sur un

deuxième émetteur, de secours. Celui-ci est donc inactif la majeure partie du temps. En réception, les deux récepteurs reçoivent. L'équipement choisit automatiquement la voie par laquelle le signal est le meilleur. En cas de panne, l'un des deux chemins reste toujours disponible, et permet le dépannage sans interruption de la liaison.

Diversité d'espace et de fréquence

En introduisant une diversité on peut tirer parti des phénomènes d'interférence évoqués plus tôt :

- Diversité d'espace : un des principaux problèmes déjà mentionné concerne la présence d'un rayon réfléchi en plus du rayon direct qui entraîne la formation d'interférences dans le plan vertical des antennes de réception. La puissance mesurable présente donc des pics de sur-champ et des creux de sous-champ suivant un axe vertical. L'idée est de placer une deuxième antenne de réception distante de la première d'une demi-frange d'interférence, ou d'un multiple impair de celles-ci, de manière que les champs principaux et de diversité soient corrélés en opposition. Le champ combiné permet ainsi de s'affranchir très largement des instabilités du champ dues aux réflexions ou aux trajets multiples.
- Diversité de fréquence : l'idée est semblable à celle de diversité d'espace. Il s'agit également de combiner deux champs dont les déphasages sont complémentaires. On exploite cette fois-ci les différences de propriétés de propagation des ondes de fréquences voisines. On émet ainsi de façon redondante sur un deuxième couple de fréquences, préférentiellement sur une polarisation croisée.
- Diversités mixtes et hybrides : il est possible également de proposer des configurations mêlant les deux types de diversité précédents. On peut ainsi émettre à deux fréquences différentes sur les deux antennes de diversité d'espace (*on parle alors de diversité quadruple*). Il est également possible de placer une seule antenne croisée d'un côté, et de profiter de la diversité d'espace en réception de façon dissymétrique (*diversité triple*).

La diversité de fréquence présente l'avantage de ne nécessiter qu'une seule antenne. Les efforts sur les structures portantes sont donc moindres ; leur taille peut également être moindre. En revanche, une fois données les hauteurs d'antenne, l'écart optimal en fréquence est fixe. Cette exigence n'est pas toujours compatible avec les plans de fréquence imposés par ailleurs. Elle présente également un rendement spectral faible

La diversité d'espace nécessite deux antennes (*y a-t-il la place sur le pylône correspondant à l'espacement voulu ?*) mais leur taille est souvent moindre. Par ailleurs, la méthode présente l'avantage d'une plus grande souplesse, et de performances généralement supérieures. Elle est de plus économe en fréquences, ressource ô combien rare.

Les fournisseurs sont nombreux, et vous proposent un accompagnement expert afin de déployer cette offre. En plus d'apporter un diagnostic, un conseil, l'installation du matériel et de sa mise en place, les fournisseurs se proposent en général de gérer la partie administrative avec l'ARCEP.

Par exemple :

- Bouygues Telecom Entreprises
- Orange
- Iris64
- Triad
- ADW Network
- Alcatel-Lucent

Premier ellipsoïde de Fresnel. Il s'agit d'un volume présent dans l'espace qui permet de mesurer l'atténuation que peut apporter un obstacle (*colline, immeuble ou encore montagne*) lors de la propagation d'une onde.

Toutes les conditions d'utilisation des réseaux sont recommandées et définies par l'UIT-R.

1. Pour que les ondes puissent correctement se propager de la station émettrice au récepteur, il est important de veiller au dégagement de la zone de liaison. Le relief, la végétation ou encore le bâtit peuvent causer des pertes d'émission. L'énergie la plus importante est contenue dans la zone appelée "premier ellipsoïde de Fresnel". A cet effet, l'étendue de cette zone - concentrée sur quelques dizaines de mètres - doit être dégagée.
2. Il est aussi primordial d'étudier les conditions climatiques et atmosphériques de la zone traversée par l'onde. Les rayons ne se déploient pas en ligne droite mais se calent aux zones disposant d'un fort indice électromagnétique, soit les couches de l'atmosphère les plus denses. Ce que l'on appelle aussi la réfraction atmosphérique. Les fortes précipitations peuvent aussi perturber la propagation de l'onde. A cet effet, lors des études de terrain préalables il est important de mener des études statistiques afin d'anticiper le déplacement de l'onde en fonction de la courbure de la terre, et des changements climatologiques.

La réfraction atmosphérique - Ce phénomène optique se produit lorsque la trajectoire d'une lumière est non rectiligne du fait de la variation de la densité de l'air avec l'altitude.

Faisceau hertzien (*FH*) : quels facteurs peuvent perturber leur propagation ?

Les facteurs pouvant perturber la propagation des faisceaux hertziens sont liés à celles des ondes radios.
Lors de la propagation de l'onde hertzienne, trois types d'éléments peuvent la perturber :

1. Son rayonnement en espace libre, impliquant la difficulté parfois à pallier la présence d'obstacles sur son chemin ;
2. Les variations aléatoires climatologiques, les hautes précipitations pouvant perturber son parcours ;
3. Les interférences, les perturbations électromagnétiques, les brouillages ou encore la réflexion principale ou de multi-trajets.

Pour les FH de fréquence supérieure à 8 GHz, les précipitations entraînent des pertes également considérables, d'autant plus que le taux de précipitations (*en mm/h*) et la fréquence sont élevés. De plus, la phase de ces précipitations influence également l'atténuation du signal. Ainsi la neige, qui a une très petite constante diélectrique, a beaucoup moins d'influence que des gouttes de pluie de même masse. La neige fondante, d'autre part, allie le large diamètre des flocons et le coefficient de la pluie pour créer un obstacle plus important que les deux séparément que l'on nomme la "bande brillante". Ainsi le passage d'une onde de 10 cm dans cette bande rencontre de trois à trente fois plus d'atténuation que dans la pluie sous la bande.
En France, l'intensité de pluie qui est atteinte ou dépassée 0,01 % du temps varie, selon la région, de 22 à 60 mm/h sur l'année moyenne. Ce phénomène de précipitations est donc dimensionnant dans l'ingénierie des liaisons dont la bande de fréquences est supérieure à 8 GHz. Il réduira la longueur possible du bond pour des exigences de disponibilité données. L'onde est également partiellement dispersée sur la polarisation croisée (*phénomène de transpolarisation*). Atténuation et transpolarisation sont plus marquées pour un signal en polarisation H (*horizontale*).

Le signal reçu est la somme du signal principal, et de tous les signaux réfléchis (*sur le sol, la végétation, et surtout les étendues d'eau*). Les interférences générées entre tous ces signaux entraînent des sur-champs et des sous-champs parfois extrêmement importants mais également des distorsions (*évanouissements sélectifs*).
La réflexion principale est le phénomène dominant de multi-trajets. Il existe cependant d'autres cas d'importance.

- Les réflexions multiples dans une couche de guidage, le conduit atmosphérique jouant un rôle semblable à un guide d'onde : l'onde "rebondit" sur les "bords" du conduit.
- La scintillation : lors du survol d'une forêt par exemple, une partie de l'onde se propage à travers les arbres, subissant de fortes transpolarisations, et déphasages. Le champ d'interférence résultant est très instable.

Faisceau hertzien (*FH*) : quelle est son utilité pour les professionnels et les entreprises ?

De nombreux opérateurs proposent un service de mise en place de faisceau hertzien, notamment Bouygues Telecom Entreprises, ADW Network ou encore Orange.
Les professionnels et entreprises ayant recours à ce type de technologies sont motivés par un accès Internet Très Haut Débit, dont les locaux sont situés en "zone blanche", soit un lieu qui n'est pas éligible à la fibre optique et où l'ADSL ne suffirait pas.
La technologie du faisceau hertzien (*FH*) permet aussi de limiter l'enveloppe budgétaire allouée à la construction d'un réseau de communication relié à Internet, contrairement à la fibre optique. Le faisceau hertzien semble être une technologie économique et facile de mise en place. Le faisceau hertzien ne demande pas de travaux de grande ampleur, les coûts d'installation d'un faisceau hertzien sont en moyenne dix fois moins élevés que ceux utilisés dans le cadre de l'installation de la fibre optique.

Avantage et inconvénient d'un faisceau hertzien *(FH)*

Les avantages sont :

- Sans fil et robuste ;
- Très haut débit - jusqu'à 2 Gbits/s ;
- La transmission de tous les types de flux (*voix, data, vidéo*) ;
- Travaux moins coûteux - meilleur rapport qualité/prix par rapport à la fibre ;
- Installation facile, rapide et évolutif : 4 à 5 jours pour installer la liaison hertzienne ;
- Une connexion pour tous - au sein de zones topographiques difficiles et éloignées.

Les inconvénients d'un faisceau hertzien, ceux des moyens radio :

- Les ondes sont sensibles aux masquages et obstacles tels que le relief, la végétation et les bâtiments ;
- Liaison perturbée en cas de fortes intempéries, comme la pluie, la réfractivité de l'atmosphère et aux phénomènes de réflexion ;

- Les paraboles doivent avoir une vue directe ;
- La confidentialité et sa traçabilité - il est possible de pouvoir intercepter une communication car l'information est transmise en "espace libre". Dans ce cas, un système de cryptage peut être mis en place entre l'émetteur et le récepteur.

L'histoire des faisceaux hertziens (*FH*)

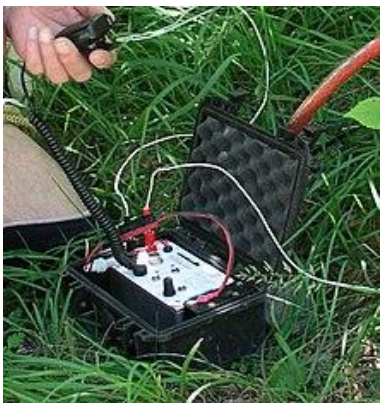
- **1931** : après de multiples recherches, une première liaison entre Calais et la ville Douvres est effectuée en 19 centimètres (*~1,57 GHz*) sur 40 kilomètres de long.
- **1942** : l'ANTRC, fabrication du premier faisceau hertzien (*FH*) aux États-Unis, anciennement appelé VHF, puis "câble hertzien".
- **1944** : cette technologie fut transmise aux français en dotation à l'époque du débarquement.
- **1944 - fin des années 80** : mise en service pour les transmissions des forces, pour ensuite servir à la D.O.T. (*Défense Opérationnelle du Territoire*)
- **Pendant les années 60** : la technologie se développe pour donner vie à 3 nouvelles gammes de faisceaux hertziens. Chacun de ces appareils répond à des besoins spécifiques, les faisceaux hertziens de l'Avant (*QR-MH-8*), de descente de site (*QR-TH-3*) ou bien de franchissement de coupures ou encore des grandes unités (*ARIANE ou GR-MH-11*). Afin de pouvoir respecter les besoins de confidentialité nécessaires à l'époque de la guerre froide, le RITA de l'armée de terre française a été mis en place. Cet appareil a permis par le chiffrement de jonction, de respecter un degré de discrétion acceptable.
- **Pendant les années 70** : France Telecom fait l'usage des faisceaux hertziens pour des besoins régionaux.
- **2006 - 2010 - 2012 et 2014** : les conditions de l'utilisation sont réglementées et revues par les autorités.
- **En 2014**, les conditions d'utilisation de la bande de fréquences 24,5-26,5 GHz (*26 GHz*) par les faisceaux hertziens ont été revues pour s'aligner sur le plan de fréquence de la recommandation européenne n° T/R 13-02. Elles permettent un spectre radioélectrique plus large, pour augmenter les débits sur les réseaux.
- **Février 2013** : le Plan France Très Haut Débit a été initié par le Président de la République.
- **2018** : l'Institut Fraunhofer a permis d'atteindre un débit de 40 Gbit/s pour 1 km de distance, ce qui en fait une avancée scientifique car quasiment équivalente à la puissance de la fibre optique.
  Par exemple, l'ADSL en France propose un débit de 6 Mbit/s, soit un total de 6 000 fois moins.

Ces recherches menées par l'Institut Fraunhofer a aussi mis en valeur la haute résistance du faisceau hertzien (*FH*) face aux conditions climatiques extrêmes qui peuvent parfois dégrader et perturber la qualité du signal entre l'émetteur et le récepteur.

Record mondial - La plus longue liaison réalisée au monde est celle qui relie Port Soudan au Soudan à Taif en Arabie Saoudite, réalisée en 1979 par la société italienne Telettra, sur une distance de 360 km à travers la mer Rouge entre les stations de Jebel Erba, altitude 2 179 m (*20°44'46,17" N 36°50'24,65" E, Soudan*) et Jebel Dakka, 2 572 m (*21° 5'36,89" N 40°17'29,80" E, en Arabie Saoudite*). Cette liaison fut construite sur la bande de 2 GHz, avec quatre antennes de 4,60 m de diamètre dans chaque station, montées sur des tours de 112 m de hauteur. Elle a permis la transmission de 300 communications téléphoniques plus un signal de télévision, en analogique (*FDM*).

ANNEXE 9

Système de transmission par le sol


Système Nicola, système de transmission par le sol.

Un **système de transmission par le sol**, abrégé **TPS** (***T**ransmission **P**ar **S**ol*) et parfois appelé "tellurophone" (*de tellurique*), est un système de communication en milieu souterrain utilisant des ondes électromagnétiques transmises par le sol continu.

Le TPS, le système Nicola, le système FAUCHEZ… sont tous des systèmes de radiocommunication utilisés notamment :

- en spéléologie, en particulier pour les opérations de secours ;
- pour des applications militaires ;
- pour des applications radioamateurs ;
- pour des mines souterraines.

Nicola est un système émetteur/récepteur BLU super hétérodyne. Il permet une liaison radio entre deux postes à travers plusieurs centaines de mètres de roche calcaire, en exploitant la conductivité électrique du sol. Il permet ainsi une grande simplification des opérations de secours spéléologiques en offrant un moyen de communication entre le sous-sol et la surface très simple à mettre en place.

La Télégraphie Par le Sol (*TPS*), inventée en 1917, a une portée d'environ 3 km. L'émetteur injecte dans le sol, entre deux piquets métalliques distants d'une centaine de mètres, un "courant vibré" commandé par le manipulateur de signaux Morse. La réception s'effectue entre deux autres piquets métalliques distants également d'une centaine de mètres. Extrêmement faible, le signal capté entre ces piquets doit être amplifié avant d'être transmis au casque d'écoute.

En 1874, c'est la première transmission radio dans le sol par le colonel Pilsoudski ingénieur Russe.

- En France, en 1901 : essais de transmission radio dans le sol au Vésinet près de Paris, par Eugène Ducretet.
- En France, en 1915 à Meudon près de Paris : mise au point de transmission radio par le sol pour des applications militaires durant la Première Guerre mondiale. Par Perot, professeur à l'école Polytechnique, le capitaine Jouaust et le lieutenant Labrouste (*car les fils de téléphone sont fréquemment coupés entre les tranchées*).
- Les transmissions radio par le sol sont très répandues sur le front entre les tranchées pendant la Première Guerre mondiale aussi bien en radiotéléphonie (*et en radiotélégraphie pour des distances de plusieurs kilomètres*).
- En France, en 1927 dans les mines de Bruay : essai de transmission radio souterraine sur la bande des 160 mètres par des radioamateurs (*8DU l'abbé Jules Galopin, F8JF Charles Pépin, F8JN Robert Marcelin et le SWL Edmond Aubry qui sera F8DU*). Essais d'antenne dipolaire, d'Antenne cadre, d'antenne long-fil et essais d'électrodes dans le sol.

Les plans de chaque génération de Nicola appartiennent au domaine public.

Gouffre Berger 1987-1988 - C'est à la suite de deux opérations de secours au Berger que l'idée de disposer d'un moyen de communication plus simple que le fil émerge. Albert Oyhançabal, conseiller technique de l'Isère, supervise alors une série d'essais du système Molefone mais les résultats ne sont pas jugés satisfaisants.

- **Juillet 1996** : une autre tragédie survient au gouffre Berger : quatre Hongrois et deux Anglais sont dans le gouffre Berger lorsque de fortes pluies tombent en surface. Du 10 au 17 a lieu une opération de secours qui se solde par le décès d'un Hongrois, Torda Istvan, et d'une Anglaise, Nicola Dollimore, proche amie de Graham Naylor. Les autres membres de l'expédition sont sauvés de justesse. À la suite de cette tragédie, Nick Perrin, le compagnon de Nicola, ainsi que les membres de leur club, offrent une somme d'argent à la SSSI qui propose d'utiliser cette somme pour développer un système de radio. L'idée de la "Fondation Nicola", qui plus tard deviendra l'"Association Nicola", est née.
- **1996-1997** : la SSSI définit les besoins en transmission pour les secours et consulte les spécialistes radioamateurs français, anglais et suisses pour finalement définir les spécifications générales de ce que sera Nicola 1.

À la suite de la réunion de janvier, et très rapidement, Graham Naylor, Paul Riceet Paul Mackrill travaillent sur la mise au point et la fabrication du matériel radio, qui s'appelle système NICOLA et dont le principe est celui des Suisses, adapté dans une optique de production en série. De nombreux essais (*Bournillon, Gournier, TQS, gouffre Berger*) seront réalisés par des bénévoles de la SSSI, de l'ADRASEC 38 et des spéléologues isérois. Dès le début, au sein de la fondation et de la SSSI, il est décidé de développer un système radio dont les plans seront du domaine public pour éviter tout brevet et rendre le système accessible à tous les acteurs du secours spéléologique.

- **Début 1998** : article dans la revue Spéléo Magazine.
- **Été 1998** : première utilisation lors d'une opération de secours réel dans le gouffre Berger.
- Discussions avec le SSF pour lui transférer la technologie du système Nicola afin de le fabriquer en petite série au profit de tous les départements de France.
- **Novembre 1998** : l'utilisation du système Nicola lors d'un exercice dans la Dent de Crolles montre le gain de temps important qu'il est possible d'obtenir.
- **Décembre 1998** : article de Jacques Gudefin dans "Info SSF" nº 51.
- **Janvier 1999** : le préfet de l'Isère reconnaît l'importance du développement du système Nicola et félicite la SSSI ainsi que l'ADRASEC 38.

Utilisation du système Nicola pour communiquer depuis la surface avec un groupe de spéléologues situé dans la grotte des Chamois (*Alpes-de-Haute-Provence*).

- **Février 1999** : Collaboration avec la Gendarmerie nationale pour la mise au point du système Nicola II, qui sera très vite utilisé par les PGHM de Grenoble et Oloron-Sainte-Marie.
- **Juin 1999** : publication des circuits de deuxième génération (*système Nicola II*) dans le journal CREG. La technologie est donc mise dans le domaine public. Cette version utilisant des circuits CMS (*composants montés en surface*) permet la fabrication en série (*CREGJ 38*).
- **Juin 1999** : "Info SSF nº 53" annonce la disponibilité du system Nicola pour les spéléo-secours départementaux.
- **Été 1999** : recherche de 3 spéléologues perdus dans la Dent de Crolles avec l'aide du système Nicola.
- **Courant 1999** : réunion technique en Angleterre dans le Derbyshire de tous les spécialistes de la radio souterraine. Échanges techniques et essais entre HeyPhone, Nicola et Molefone.
- **Novembre 1999** : l'autorisation de mise sur le marché du système Nicola est émise par l'Autorité de régulation des télécommunications grâce au soutien du colonel Papalardo du groupement de gendarmerie de l'Isère. Sans son intervention, les démarches auraient pris plusieurs années...
- **Novembre 1999** : secours au gouffre des Vitarelles. Le PGHM de Grenoble, engagé dans le réseau en crue des Vitarelles pourra, grâce à Nicola, communiquer avec la surface.
- **Décembre 1999** : la Revue l'Express publie un article sur le système Nicola.
- **Courant 2000** : opération "Highest and deepest" de communication entre le gouffre Berger et le Mont Blanc.
- **Août 2001** : création de l'association Nicola et dépôt de ses statuts auprès de la préfecture de l'Isère.

Le développement du système Nicola dans sa troisième version touche à sa fin (*août 2008*). Cette nouvelle version devrait apporter les améliorations suivantes :

- Conception numérique autour d'un circuit FPGA.
- Choix de la fréquence : Nicola 2 ne peut utiliser que la fréquence de 87 kHz. Nicola 3 pourra, lui, choisir sa fréquence dans la plage 20−190 kHz.
- Envoi de textes, comme les SMS, en utilisant une très faible bande passante. Lors de l'utilisation de Nicola dans des conditions karstiques difficiles, lorsque la qualité de la liaison ne permet pas de parler, il devrait être possible d'envoyer/recevoir des textes.
- Mode nomade : permet à un spéléologue en mouvement sous terre de recevoir tous les messages émis par les autres postes Nicola.
- Boîtier : plus petit, complètement étanche.
- Connexion Bluetooth permettant d'émettre et recevoir en utilisant les oreillettes du commerce ainsi que de lier Nicola à des PDA, Smartphones, etc.

Fonctionnement par rayonnement électrique. Le courant électrique dans une plage 20 à 190 kHz est généré dans le sol par deux électrodes qui terminent un dipôle électrique d'une longueur comprise entre de deux fois 20 mètres à deux fois 80 mètres. Une électrode est plantée sur une des parois et l'autre électrode est plantée sur la

paroi opposée ou bien une électrode est plantée au sol et l'autre électrode est plantée au plafond. Cela pour profiter de la plus grande tension entre les deux électrodes.

Dans le système de Jean Jacques FAUCHEZ "F6IDE". Le courant électrique dans la bande radioamateur des 1,8 MHz ou dans la bande radioamateur des 137 kHz est généré dans le sol par une antenne dipôle d'une longueur comprise entre de deux fois 30 mètres à deux fois 80 mètres isolé du sol.

Ainsi, le système Fauchez permet une liaison radio entre plusieurs postes à travers plusieurs centaines de mètres de roche calcaire. Il permet ainsi une grande simplification des opérations de secours spéléologiques en offrant un moyen de communication entre le sous-sol et la surface très simple à mettre en place.

ANNEXE 10

QU'EST-CE QUE LE "MÉTAVERS".

"Métavers" est le successeur de l'internet mobile présenté par Mark Zuckerberg (*cofondateur du site et du réseau social Facebook*) en juillet 2021. Peu après, le 18 octobre 2021, Facebook a annoncé le recrutement de quelque 10.000 personnes en Europe sur les cinq prochaines années pour développer ce nouvel univers virtuel.

Le terme "métavers" est une simple contraction des mots "méta" (*qui fait référence à une vision d'ensemble*) et "univers". Il est issu de romans de science-fiction du début des années 90, décrivant des mondes virtuels dans lesquels les individus peuvent interagir, souvent à l'aide d'accessoires comme des casques de réalité virtuelle. Ainsi, tout monde virtuel dans lequel un individu est invité à se créer un double numérique peut être considéré comme un "métavers".

Le "métavers" étant un terme générique faisant écho à un monde virtuel, il peut prendre de nombreuses formes. Sur le papier, un simple forum en ligne - et bien sûr un réseau social - sont des "métavers", dans la mesure où ils réunissent des "doubles virtuels" des internautes dans un univers parallèle où ils peuvent se rencontrer. Mais le "métavers" tel qu'il est imaginé par Facebook est plus ambitieux. En lieu et place d'une simple page Web ou application, l'entreprise souhaite se rapprocher des romans de science-fiction en équipant ses utilisateurs de ses casques de réalité virtuelle Oculus, marque rachetée en 2014 pour 2 milliards de dollars.

Selon les ambitions de Mark Zuckerberg, qui espère démocratiser cette nouvelle plateforme dans les cinq prochaines années, tous les domaines pourraient être concernés. Il souhaite ainsi que les utilisateurs de Facebook ou Instagram puissent désormais se retrouver sous forme d'avatars, dans des mondes virtuels en 3D, pour échanger dans un bar imaginaire, assister à un concert en ligne, ou se réunir pour une réunion professionnelle.

En septembre 2019, Facebook avait dévoilé Facebook Horizon, un réseau social en réalité virtuelle, remplaçant Facebook Spaces, annoncé en 2017. Des projets qui en restent au stade de version bêta, au même titre que la déclinaison professionnelle baptisée Workooms et présentée en août 2021.

Si Facebook est le premier des GAFAM (*acronyme des géants du Web* : ***G**oogle / Alphabet, **A**pple, **F**acebook / Meta, **A**mazon et **M**icrosoft*) à présenter de telles ambitions pour le grand public, de nombreuses plateformes sont en réalité des "métavers", bien qu'elles n'utilisent pas la réalité virtuelle. La plus illustre d'entre elles est Second Life, un univers entièrement créé en 3D au début des années 2000 qui connut un immense succès à cette époque. Comme c'est aujourd'hui le cas sur les réseaux sociaux, on y trouvait des publicités, des événements organisés par des marques, mais aussi des internautes rémunérés, par exemple en commercialisant des vêtements virtuels. Ironiquement, la fin de Second Life fut précipitée par le succès… de Facebook.
Plus récemment, le jeu vidéo "Fortnite ". D'abord présenté comme un simple jeu de combat, il s'est transformé en lieu de rencontres virtuelles. Comme Second Life des années plus tôt, Fortnite a réuni les internautes pour des concerts virtuels, mais également pour faire la promotion de films, de séries ou de produits en tous genres.

Plusieurs raisons font que le concept de "métavers" revient dans l'actualité. D'abord l'attrait des géants du Web pour ce formidable relais de croissance économique, avec des mondes virtuels qui n'oublient pas d'importer les publicités du monde réel, à l'image de ce que l'on retrouve dans Fortnite.
Autre raison majeure : la démocratisation des casques de réalité virtuelle, désormais accessibles, bien que peu utilisés par le grand public. Pour Facebook, évoquer le "métavers" permet de faire la promotion de sa marque Oculus, tout en faisant émerger dans l'actualité des sujets qui font oublier ses nombreux déboires actuels.
La pandémie de Covid-19 et ses conséquences en matière de confinement ou de télétravail n'est probablement pas étrangère à l'intérêt des géants du numérique et de la publicité pour le "métavers".

Raphaël Grably - Le 18/10/2021

Le monde virtuel, prendrait-il l'ascendant sur le monde réel ? Anne Roumanoff s'est penchée, avec un certain humour, sur le sujet dans sa chronique "Rouge vif". Dans ce qui suit, l'humoriste fait état du changement de nom du groupe Facebook, "MÉTA" (*comme par hasard*), et surtout de l'influence des réseaux sociaux dans nos vies, "le virtuel et le réel" :

« L'amitié virtuelle est moins fatigante que l'amitié réelle. Sur Facebook, pour présenter ses condoléances, c'est pratique, il suffit de cliquer sur une icône prière et, si on souhaite s'investir dans une relation numérique amicale, on peut même ajouter : "Je pense fort à toi." Les amis virtuels, on ne les aide pas à déménager.

Confortablement installé sur son canapé, on clique sur la photo de leurs cartons encore emballés en ajoutant : "Courage !!!" Si l'on veut se débarrasser d'un ami virtuel encombrant, on clique sur "Ne plus être ami" et c'est fini.

Pas besoin, comme dans la vraie vie, de "Oui, oui, on va déjeuner. Quand ? Bientôt, je te dis ça très vite." On peut tous être beaux virtuellement grâce aux filtres. En quelques clics, on peut s'amincir la taille, s'enlever les rides et se rajouter des muscles. Le lifting numérique est gratuit et ne fait pas mal. Le souci, c'est qu'on s'habitue à cette version améliorée de soi-même, alors quand on croise son vrai reflet dans la glace on regrette qu'il n'y ait pas de filtre dans le miroir de la salle de bains pour se lisser le teint.

Les likes virtuels nous aident à supporter le réel. Dans la vraie vie, quand on change de coiffure, tout juste si nos proches le remarquent. Si l'on publie une photo sur Instagram en postant "new hair, new life", on reçoit aussitôt une avalanche de commentaires aussi simplistes qu'enthousiastes qui nous caressent l'ego : "Trop belle", "Magnifique !", "Wouah". Ensuite, on va vite liker les commentaires positifs pour encourager nos admirateurs numériques.

La vie virtuelle de notre "moi" est merveilleuse. On passe des vacances sublimes dans un endroit magnifique en mangeant des plats délicieux. Devenu paparazzi narcissique et reporter virtuel de l'unique sujet qui nous passionne, "moi", on met en scène sa vie rêvée, que l'on décline à l'infini : "Moi à la plage, moi au restaurant, moi et mon amoureux, moi et mes amis…" Le temps pourri, les moustiques, les engueulades, les gosses insupportables, ce n'est pas "instagramable", alors on n'en parle pas. Parfois on se photographie, quelquefois on se filme mais, toujours, on compte les likes.

Dans le monde virtuel, le business est réel. Facebook n'est pas une œuvre caritative, mais une entreprise commerciale qui veut toujours en savoir plus sur nos centres d'intérêt pour vendre nos données à des annonceurs qui nous envoient des publicités ciblées. Trois milliards et demi d'utilisateurs, 1 milliard d'euros en Bourse. "Tout ce qui est gratuit se paie", on a lu ça quelque part. Peut-être sur Instagram.

Ce qui se passe dans le virtuel a un impact dans le réel. Les fake-news influent sur les élections, les algorithmes nous confortent dans nos opinions, les ados harcelés sur les réseaux peuvent décider d'en finir, mais on oublie tout ça en regardant la vidéo d'un chat qui tombe dans l'eau. Tout est sur le même plan, tout se mélange dans un immense magma d'images que l'on fait disparaître d'un coup d'index sur l'écran.

Facebook a changé de nom. Mais "notre mission reste la même, il s'agit toujours de rapprocher les gens". C'est Mark Zuckerberg qui l'a dit. Il paraît qu'une révolution technologique s'annonce. Grâce aux lunettes à réalité augmentée, bientôt on aura un avatar qui pourra assister à des réunions de travail en 3D et faire du shopping dans des magasins virtuels. Encore plus de virtuel, le projet est bien réel. Cela pose bien des questions : ce qui est virtuel est-il réel ? Le réel est-il forcément vrai ? La réalité doit-elle être sans filtre ? Vous avez trois heures. »

ANNEXE 11

Antoine de Saint-Exupéry

Saint-Exupéry est un personnage connu de tous, et avec lui c'est tout l'imaginaire nostalgique des premiers temps de l'Aéropostale qui ressurgit, et reprend vie.

Qui aujourd'hui ne connait pas le nom d'Antoine de Saint-Exupéry ? Saint-Exupéry, anachorète du Cap Juby, pilote de ligne et de raid, pilote de guerre, aventureux jusqu'à la limite du possible, poète magnifique, mêlant sans cesse l'action de l'esprit à celle du corps et qui semble voué à naviguer parmi les étoiles… au-delà de ce 31 juillet 1944, jour de sa disparition en mer Méditerranée, au large des Calanques de Marseille, lors d'une mission de reconnaissance à bord de son Lockheed Lightning P38.

Son expérience de pionnier de l'aviation et de pilote de guerre lui donnera toute la légitimité pour délivrer son principal message : « ***C'est par le dépassement de soi que l'on devient un Homme*** ».

Saint-Exupéry, ou mieux, "Saint-Ex", a été présenté comme un "paladin", un "chevalier errant" comparable aux héros de la guerre, car il faisait partie d'une nouvelle génération d'aviateurs attelée à une besogne immense, la création de l'Aéropostale. Il est également qualifié de "camarade le plus exquis" et de "pilote le plus casse-cou de la ligne", c'est à la fois un "enfant" et un "héros" dont l'aspect le plus pur serait encore le "côté insouciant". Son surnom de "Pique la lune" lui est resté, non seulement en raison de son nez en trompette mais aussi d'une tendance certaine à se replier dans son monde intérieur.

En janvier 1936, Antoine de Saint-Exupéry le héros médiatique, échappe à Saint-Exupéry l'écrivain. Il est entré dans les représentations collectives tout armé d'un courage légendaire, d'un sourire désarmant, chevalier ou paladin déjà sacrifié à l'idéal qu'il devait, à son corps défendant, incarner. L'aviateur tentera de nuancer cette image dans le récit qu'il fera de son aventure pour *L'Intransigeant (avion ainsi baptisé sur la photo ci-contre)*, qui le publiera sous le titre de *Prison de sable*, en six épisodes à la une du 30 janvier au 4 février 1936. Tout au long de ce texte, il répétera inlassablement que son aventure n'a rien de courageux, ni même de douloureux : « *Rien n'est exact des réflexions que l'on m'attribuera sur ce supplice. Je ne subirai aucun supplice*. » Il dira aussi à quel point affronter un danger lui semble un exercice sans grandeur : « *Il ne s'agit pas de vivre dangereusement. Je ne comprends pas cette formule. Ce n'est pas le danger que j'aime. Je sais ce que j'aime. C'est la vie*. » Son errance désespérée dans le désert, Saint-Exupéry la décrit comme "un conte de fées un peu cruel" qui lui aura surtout révélé son attachement aux hommes, et à la vie. Mais ce ne sont pas les paroles que l'on attend d'un héros du détachement : son récit n'affectera pas une image médiatique déjà figée, il est trop tard pour cela. En janvier 1936, Saint-Exupéry est définitivement devenu, bien malgré lui, un héros stéréotypé de l'aviation, dont la figure partagée, déjà statufiée, n'a pas été forgée dans ses propres textes, mais dans un discours médiatique qui, dès l'origine, lui a échappé.

Antoine de Saint-Exupéry, né à Lyon le 29 juin 1900, est fasciné dès son plus jeune âge par les avions. Il fait son baptême de l'air à 12 ans à l'aérodrome d'Ambérieu-en-Bugey. Malgré des résultats scolaires médiocres, le jeune Antoine se consacre à l'écriture et remporte le prix de narration de son lycée.

Fils de Jean de Saint-Exupéry et de Marie de Fonscolombe, il est le troisième enfant d'une famille de cinq (*le second à partir de la droite, sur cette photo*). Son père Jean de Saint-Exupéry décède d'une attaque en 1904. Sans ressources, Marie emmène ses enfants dans le Midi, hébergés dans le château de son père, Charles de Fonscolombes, à La Molle. Elle leur lit des livres magnifiques dont les Contes d'Andersen, auxquels Antoine restera attaché toute sa vie. Elle leur enseigne la peinture, qu'elle pratique en amateur, et la musique.

En 1907 Charles de Fonscolombe, son grand-père, décède. Marie et les enfants sont accueillis à Lyon par leur tante Madame de Tricaud. Antoine de Saint-Exupéry partage sa vie entre l'appartement de la place Bellecour et le château de Saint-Maurice de Rémens où il situe l'univers fabuleux de son enfance, celui des jeux et des

découvertes, celui des premières expériences scientifiques aussi : il imagine un système d'arrosage à vapeur et avec l'aide du menuisier du village il construit une "bicyclette volante" qui ne volera jamais. Surveillés avec discrétion par une mère particulièrement affectueuse, les enfants continuent leur apprentissage du dessin et de la musique et présentent au public occasionnel des saynètes qu'Antoine met parfois en scène.

À la sollicitation de leur grand-père Fernand de Saint-Exupéry, qui souhaite avoir près de lui ses petits-fils, en 1909 Antoine et son frère François quittent l'univers de leur première enfance pour continuer leurs études au collège Jésuite de Notre Dame de Sainte-Croix au Mans. Antoine est un élève moyen. La vie d'interne le désole : « *Quand on est un petit garçon au collège, on se lève trop tôt. On se lève à six heures du matin. Il fait froid. On se frotte les yeux et on souffre à l'avance de la triste leçon de grammaire.* » Autant dire que les vacances au château de Saint-Maurice sont une aubaine. Surtout qu'à quelques kilomètres se trouve un terrain d'aviation où des constructeurs lyonnais essaient leurs aéroplanes. Antoine se plait auprès des pistes et dans les hangars où il est fasciné par les moteurs. Laissant croire qu'il avait l'autorisation de sa mère, en juillet 1912 Antoine de Saint-Exupéry convainc un de ces aviateurs de le prendre au bord de son appareil, un Berthaud-Wroblewski (*photo de l'appareil à droite*).

En 1914 Antoine de Saint-Exupéry est pensionnaire à Villefranche-sur-Saône et ensuite à la Villa Saint-Jean de Fribourg. Il se lie d'amitié avec Charles Sallès, Marc Sabran et Louis de Bonnevie. C'est pendant cette période qu'il lit énormément et qu'il découvre Balzac, Dostoïevski et Baudelaire entre autres. Malgré de bonnes appréciations en physique, en philosophie et en musique, Antoine est parmi les derniers de la classe.
En 1917 Antoine de Saint-Exupéry subit une épreuve qui le marque profondément : son frère François est emporté par un rhumatisme articulaire avec des complications cardiaques. François nomme Antoine son exécuteur testamentaire. Vingt ans plus tard celui-ci note dans un texte poignant ce qu'il avait ressenti à la mort de son frère : « *Il me confierait sa tour à bâtir. S'il était père, il me confierait des fils à instruire. S'il était pilote de guerre, il me confierait ses papiers de bord. Mais il n'est qu'un enfant. Il ne confie qu'un moteur à vapeur, une bicyclette et une carabine.* »
Cette même année Antoine de Saint-Exupéry obtient son bac et monte à Paris pour préparer le concours de l'Ecole Navale. Il fait ses classes préparatoires au Lycée Bossuet, puis au Lycée Saint-Louis. Accueilli très chaleureusement par une cousine de sa mère, Yvonne de Lestrange, il est introduit dans les milieux mondains et littéraires les plus huppés de la capitale où il fait la connaissance de ceux qui font la pluie et le beau temps des lettres françaises, André Gide, Gaston Gallimard, Jacques Rivière, Jean Prévost ou Jean Paulhan. Il est invité chez les Saussine (*leur fils sera son ami et il sera amoureux de leur fille*) et fait la connaissance de Louise de Vilmorin, sa future fiancée. En compagnie de ces jeunes gens et de ces jeunes filles de bonne famille, Antoine de Saint-Exupéry fréquente les théâtres et les expositions. Il lit la littérature d'avant-garde et il a avec ses amis des discussions passionnées entre autres sur les écrits de Pirandello (*écrivain italien, poète, nouvelliste, romancier et dramaturge*).

Cependant, c'est la guerre. Paris est bombardé par les armées allemandes qui se trouvent à proximité. Antoine de Saint-Exupéry parvient à tromper la vigilance des surveillants qui les conduisent dans un abri et monte sur le toit de l'école d'où il admire le spectacle des avions qui lancent des bombes, les tirs de l'artillerie antiaérienne, les explosions. Le spectacle lui paraît "féérique".
En 1919, Antoine de Saint-Exupéry passe l'examen d'entrée de l'Ecole Navale et échoue à l'oral. Il envisage de devenir architecte et s'inscrit aux cours de l'Académie de Beaux-arts.
En 1921 il est appelé sous les drapeaux pour effectuer son service militaire. Ayant choisi l'aviation, il est affecté au deuxième régiment d'aviation de Strasbourg puis à Casablanca. Le 23 décembre 1021, il obtient son brevet de pilote militaire au Maroc et en janvier 1922, il est promu caporal à Istres. Ensuite, il vole sur plusieurs bases françaises et monte en grade. À la suite de son premier accident d'avion au Bourget, le 1er mai 1923, cela se traduit par une fracture du crâne. Il est démobilisé et ne se remet à voler qu'en 1926 pour effectuer le transport du courrier entre Toulouse et Dakar. C'est Didier Daurat, directeur de l'Aéropostale qui l'engage pour convoyer du courrier au-delà des mers. C'est à ce moment qu'il publie son premier livre, "L'Aviateur". Suivent de "Courrier sud" (*1929*), "Vol de nuit" (*1931*) et surtout "Terre des hommes" (*1939 - Récompensé par le prix de l'Académie Française la même année*), ouvrages qui relatent la vie de Saint-Exupéry, ses vols et ses rencontres avec les hommes. Jusqu'en 1939 Antoine De Saint-Exupéry effectue de très nombreuses liaisons pour l'Aéropostale où il a rencontré Jean Mermoz et Henri Guillaumet. Par la suite, il écrira "Pilote de guerre" (*1942, il y a donc 80 ans*), "le Petit Prince" (*1943 – son plus grand succès*), puis "Correspondance 1930-1944".

Voici un extrait de "Pilote de guerre"

« Nous sommes fin mai, en pleine retraite, en plein désastre. On sacrifie les équipages comme on jetterait des verres d'eau dans un incendie de forêt. Comment pèserait-on les risques quand tout s'écroule ?... En trois semaines, nous avons perdu dix-sept équipages sur vingt-trois. Nous avons fondu comme une cire... Nous savons bien que l'on ne peut faire autrement que de nous jeter dans le brasier, si même le geste est inutile. Nous sommes cinquante, pour toute la France. Sur nos épaules repose toute la stratégie de l'armée française ».

Voici maintenant la description de "correspondance 1930-1944"

Buenos Aires, septembre 1930. Antoine de Saint-Exupéry, chef d'exploitation de l'Aeroposta Argentina, fait la connaissance de Consuelo Suncín Sandoval, la jeune veuve salvadorienne de l'écrivain Enrique Gómez Carrillo. Après quelques semaines de vie commune en Argentine, ils choisissent de se marier en France auprès de la famille de l'aviateur.

Mais la vie conjugale du couple sera un parcours bien chaotique, malgré tout ce qui les réunit et en premier lieu leur imaginaire commun, peuplé d'étoiles, de petits animaux et de toutes sortes de trésors. L'aventureux "Tonio" attend de son épouse une attention et un réconfort de tous les instants que le tempérament de celle-ci, éprise de liberté et douée d'une irréductible fantaisie, ne peut lui apporter continûment.

Mais Antoine et Consuelo ne se délieront jamais de leur alliance, pourtant soumise à des polarités contradictoires. Sacrée à leurs yeux, elle les réunira dans les moments les plus difficiles, jusqu'à New York où l'écrivain se trouve exilé entre 1941 et 1943. Et la promesse réciproque d'un amour inconditionnel leur permettra de supporter, non sans souffrance, l'éloignement et l'inquiétude, lorsque l'engagement militaire de l'écrivain les rendra inévitables jusqu'à la fin tragique de juillet 1944.

Ces années sont aussi celles de l'écriture du Petit Prince, une fable qui illumine, en leur donnant son sens le plus profond, ces lettres souvent déchirantes d'émotion, où alternent la grâce et le désarroi, la défiance et la lumière. Un jeune prince voyageur, une rose et son globe : nous y sommes ! « *Il était une fois un enfant qui avait découvert un trésor* », écrit Antoine de Saint-Exupéry dans sa première lettre à Consuelo. « *Mais ce trésor était trop beau pour un enfant dont les yeux ne savaient pas bien le comprendre ni les bras le contenir. Alors l'enfant devint mélancolique.* »

Autres citations parmi de nombreuses autres de Saint-Exupéry

- « *Pour ce qui est de l'avenir, il ne s'agit pas de prévoir mais de le rendre possible* ».
- *« La beauté du corps est un voyageur qui passe, tandis que la beauté du cœur est un ami qui reste ».*
- *« Dans la vie, il n'y a pas de solution ; il y a des forces en marche ; il faut créer et les solutions suivent ».*
- *« La guerre, ce n'est pas l'acceptation du risque. Ce n'est pas l'acceptation du combat. C'est à certaines heures pour le combattant, l'acceptation pure et simple de la mort ».*
- *« Un sourire est souvent l'essentiel. On est récompensé par un sourire ».*
- *« Le merveilleux d'une maison, c'est qu'elle forme dans le fond du cœur ce massif obscur d'où naissent, comme des eaux de source, les songes »* (*dans "Terre des hommes" – 1939*).

Pendant la seconde Guerre Mondiale il cherche à s'engager pour piloter un avion de combat moderne aux côtés des Alliés. En 1939, il sert en tant que capitaine dans l'armée de l'air. Il reçoit la Croix de guerre avec palme, est fait Officier de la Légion d'Honneur et cité à l'ordre de l'armée de l'air le 2 juin 1940. Il partira en novembre 1940 pour New York où il y arrivera le 31 décembre 1940. Il a l'objectif de faire entrer en guerre les Américains, mais ne sera pas compris. Par la suite, De nombreux accidents et sa mauvaise santé le font mettre "en réserve de commandement". On lui confie des missions mineures d'inspection aérienne et de cartographie en vue du débarquement en Provence. C'est au cours d'une de ces missions, le 31 juillet 1944, que son avion, un Lockheed Lightning P38, disparaît au-dessus de la Méditerranée. Saint-Exupéry est reconnu "Mort pour la France".

Un an plus tôt est paru "Le Petit Prince", son œuvre la plus connue et la plus traduite dans le monde après la bible, un conte poétique et philosophique. Le narrateur est un aviateur en panne dans le Sahara : il va rencontrer un petit prince qui s'interroge sur l'absurdité du monde des adultes. Qui n'a pas lu au moins une fois cette œuvre ?

Son nom est un des plus célèbres au monde, et surtout présent un peu partout autour de nous, principalement en France :

- le billet de 50 francs de la Banque de France a porté son effigie ;
- la base aérienne 113 de Saint-Dizier est base aérienne "Commandant Antoine de Saint-Exupéry" ;

- l'aéroport international de Lyon est baptisé "Antoine de Saint-Exupéry" ;
- la gare SNCF TGV de Lyon est suivie de son nom, "Antoine de Saint-Exupéry" ;
- un des porte-conteneurs de la compagnie maritime CMA CGM a été baptisé "Antoine Saint-Exupéry" (*200.000 tonnes – 400 m de long – 20.600 conteneurs...*) ;
- une petite commune de Gironde, près de Langon, s'appelle "Saint-Exupéry" ;
- de nombreux collèges et lycées portent son nom…"Antoine de Saint-Exupéry" ;
- de nombreux lieux publics (*rues, avenues, places*…) également…"Antoine de Saint-Exupéry".

Pour en savoir plus : https://fr.wikipedia.org/wiki/Antoine_de_Saint-Exupéry

Saint-Exupéry : sa dernière mission

Dernières photos de lui dans son P38 ce 31 juillet 1944 (*au décollage de Bastia*), jour de sa disparition au large de Marseille. Sa mission était de prendre des photos de Grenoble avant le débarquement de Provence. Le trajet probable depuis Bastia apparait sur cette carte. Le dernier contact radio a été établi au-dessus du Massif du Vercors, sur le retour vers la Corse. Son avion disparaîtra du contrôle radar américain à 14h30 à l'approche de la Côte d'Azur.

1998 : une gourmette attribuée à Saint Exupéry retrouvée dans les filets d'un chalutier au large des calanques de Marseille

2004 : découverte des débris de l'avion

Lookheed Lightning P38 :

- envergure = 15,85 m – longueur = 11,52 m
- poids max en charge = 9.798 kg - charge max offensive = 1.450 kg
- vitesse max = 635 km/h - plafond pratique = 13.400 m
- distance franchissable pleine charge = 800 km
- 2 moteurs Allison V-1710-91 de 1.425 chevaux chacun
- 1 canon de 20 mm et 4 mitrailleuses de 12,7 mm
- équipement photo en soute avant.

ANNEXE 12

1912, il y aura bientôt 110 ans.

Roland GARROS va obtenir son premier très grand succès à Angers, en juin 1912. Le Grand Prix de l'Aéroclub de France couronnait le vainqueur du circuit d'Anjou. Il s'agissait d'accomplir sept fois et en deux jours, le dimanche 16 et le lundi 17 juin 1912, le triangle Angers-Cholet-Saumur, soit un peu plus de 1.100 kilomètres. Roland GARROS, qui se présente avec son Blériot personnel (*il a depuis longtemps mis un point d'honneur à ne voler que sur ses propres machines*), est opposé aux trente-trois meilleurs pilotes du monde, soutenus par tous les moyens possibles des firmes industrielles les plus puissantes du monde. Si quelques courageux ont pris leur envol malgré le vent et la tempête, GARROS resta bientôt le seul en l'air avec le jeune BRINDEJONC-DES-MOULINAIS qui, malheureusement pour lui, a franchi la ligne d'arrivée en dehors du temps réglementaire. Roland GARROS est donc le seul à terminer les épreuves du premier et du deuxième jour. Les journalistes ne l'appellent plus désormais que "le champion des champions".
Autodidacte du pilotage, il a obtenu son brevet de pilote (*le n°147*) en juillet 1910. Il est aussi le premier à traverser la Méditerranée en septembre 1913.

Affecté au Camp Retranché de Paris, il met au point le premier système de tir à travers l'hélice, par la pose de déflecteurs en acier sur les pales. En avril 1915, il est le premier à abattre un avion, seul dans un monoplace, et crée le principe du chasseur. Le 18 du même mois, touché par la DCA, il est contraint de se poser à Hulste (*Belgique*) occupé par les Allemands. Après de multiples tentatives d'évasion, il parvient à s'échapper le 15 février 1918 avec le lieutenant Anselme MARCHAL. Le 2 octobre 1918, Roland GARROS remporte sa quatrième et dernière victoire en combat aérien. La veille de ses 30 ans, le 5 octobre, cinq semaines avant l'Armistice, à l'issue d'un combat contre des Fokker D.VII, son SPAD explosait en l'air avant de s'écraser sur le territoire de la commune de Saint-Morel, dans les Ardennes, non loin de Vouziers où il est enterré.

En 1927, le stade devant accueillir la finale de la Coupe Davis est baptisé en son honneur sous l'impulsion de son ami Emile LESIEUR, président du stade français de tennis auquel Roland GARROS avait adhéré en 1906.

Pour mieux connaître la vie et les nombreux exploits de Roland GARROS, orientez-vous vers Wikipédia : https://fr.wikipedia.org/wiki/Roland_Garros

ANNEXE 13

VŒUX du Président pour 2020

Cher(e)s adhérent(e)s et ami(e)s de la Chapelle mémorial de l'aviation.

Je voudrais tout d'abord vous présenter à tous, mes vœux les plus chaleureux ainsi que ceux de notre conseil d'administration, pour l'année 2022.

Malgré les contraintes sanitaires, nous avons pu effectuer notre AG au restaurant *La Détente* qui a été pour la majorité une grande joie de se retrouver comme vous pouvez le lire dans le compte rendu.

Parlons de l'extension de la chapelle, le dossier est accepté par les instances administratives et nous avons confié le dossier à la commission syndicale du Haut-Ossau pour nous faire une évaluation du coup par leurs spécialistes afin de chiffrer et de savoir où ça nous mènera.

Nous aurons le jeudi 12 mai 2022 le rassemblement du collectif CASSIC pour la visite de la chapelle, la remise du drapeau de l'ANATC, le dépôt de gerbe devant la stèle puis repas. Nous vous enverrons les papiers pour cette rencontre en janvier.

La chapelle et l'association de l'AETA Béarn (*section des Arpètes*) étudient la possibilité d'utiliser notre "mess" pour leur réunion de CA : un accord est à l'étude.

Au cours du printemps 2022, nous organiserons l'inauguration de la stèle OPEX qui est finie et nous en profiterons pour faire un repas tous ensemble.

La réalisation de la plaque des pionniers novateurs est en cours : il faudra définir l'endroit de la pose.

Nous avons vendu 142 livres "Pau aérodrome", il nous en reste 38, je remercie toutes les personnes qui ont œuvré pour ce livre.

Je reviens des établissements CANCE où a eu lieu la réunion pour la présentation finale de la maquette de la stèle Louis BLERIOT avec les représentants des établissements de formation aux métiers de l'industrie métallurgique et afin de définir le rôle de chacun pour la réaliser. Bernard et les ingénieurs de chez CANCE ont fait un excellent travail, j'en remercie tout ces acteurs qui œuvrent pour la réussite de ce projet.

Je vous souhaite avec le conseil d'administration de joyeuses fêtes de fin d'année et surtout la santé.

Amicalement, votre président.
Noël Potier

Amicale de la Chapelle Mémorial de l'Aviation et du Camp Guynemer
www.aviation-memorial.com
Président : Noël POTIER, téléphone 06 18 04 18 83
Contact La Chapelle : contactchapelle@free.fr

ANNEXE 14

Mémorial Louis BLÉRIOT

Louis BLÉRIOT dessina en 1908 puis perfectionna d'Issy-les Moulineaux à Pau, avec son École de pilotage et ses Ateliers, le "Blériot XI" : le plus durable concept mondial de monoplan monomoteur à hélice, sur un dessin de cellule qui est aujourd'hui encore exactement le même, pour cette formule d'aéronef, toujours aussi géniale jusqu'à l'Airbus A 380, pourtant tout-électronique et à réaction.

Ceci n'est que peu ou pas inscrit dans la mémoire populaire mondiale et ses débuts connurent… l'incrédulité générale.

Ce que le SMAPP de Pau se met en devoir de corriger, aux côtés de l'ACMA et de la DGAC, face à l'Histoire indélébile de l'Aéronautique Mondiale, sur l'emplacement même des faits historiques établis : voir le Blériot XI… face au Flyer 3.

Cette Grande-première traversée aérienne de la Manche en juillet 1909, ne fut pas une promenade de plaisance sans aucune aide d'appoint, car son avion dépassa très vite le bâtiment de la Marine Nationale Française sensé l'accompagner ; au point que Louis BLÉRIOT a cru avoir "raté l'Angleterre" n'ayant plus de repère aux 2/3 du trajet, et se vit perdu corps et biens dans l'immensité du ciel…

Bernard TREY NAVARRANNE - *Architecte en chef DPLG. Pilote (ACB 1947)*

Le Mémorial Louis Blériot sera érigé sur le site aéroportuaire de Pau-Pyrénées.

Le mémorial Louis BLÉRIOT (*maquette ci-dessus*) sera installé sur le site aéroportuaire de Pau-Pyrénées. L'emplacement sera dans l'axe de l'aérogare à l'entrée du parking n°1.

L'étude du projet est réalisée par le bureau d'étude de notre mécène Christian CANCÉ (*Nay*). Un second partenaire est ajouté, Métal ADOUR possédant des ateliers mieux équipés.
La réalisation sera réalisé par le lycée immaculé-conception et celui des métiers Beau Frêne de Pau.

Colonel Jean ADIAS

Né le 21 octobre 1921 à Pau ; décédé le 10 août 2020 à Gan (*Commune des Pyrénées Atlantiques*).

Il commence sa prestigieuse carrière de pilote à l'aviation populaire en 1937. Il est breveté le plus jeune pilote de tourisme de France en 1937. Reçu en 1938 au concours pour rentrer à l'école de formation des Sous-Officiers à Istres. Il y avait 2000 candidats pour 80 places : il est classé 23ème. Puis le 25 novembre 1939, il est engagé volontaire pour la durée de la guerre. Breveté pilote militaire en 1940, il choisit le bombardement. Il rejoint pour sa formation le centre d'instruction de Marrakech, sur Bloch 210 baptisé le "Cercueil volant", car de nombreux accidents ont eu lieu en raison de la fragilité de ses moteurs. Affecté en 1941 à la 25ème escadre de bombardement basée à Tunis-el-Aouina, il participe à la campagne de Tunisie contre l'Afrika Korps du Maréchal Rommel.

Le caporal-chef ADIAS quitte l'activité fin 1942 et est rappelé comme sergent, en mai 1943, à Aix-en-Provence à la 1ère région aérienne. Après un bref séjour au Maroc, à Kasba-Tadla et Casablanca, il rejoint en avril 1945, le centre de pilotage d'Orangeburg aux Etats-Unis pour une nouvelle formation. Au cours d'un vol de surveillance côtière dans le golfe du Mexique, avec son instructeur américain, il repère le sillage d'un sous-marin allemand qui s'apprête à attaquer un convoi de pétroliers. Après avoir informé le commandant du convoi, le sous-Marin, un U-230 sera coulé par l'escorte du convoi.
A son retour des USA en février 1946, il est sergent-chef et est affecté à l'école des mitrailleurs-navigateurs-bombardiers à Cazaux puis, en novembre 1947, au groupe de liaisons aériennes 50, à Ivato sur l'Ile de Madagascar, lors de l'insurrection malgache, épisode sombre de la colonisation française. A cette époque héroïque, digne des années 1914-1918 disait-il, le bombardement se faisait encore en larguant des bombes de 50kg par la porte latérale. Les manipulations sont difficiles et les risques d'explosion en vol omniprésents. Il est nommé sergent le 1er mars 1949.

En octobre 1952, alors qu'il est adjudant-chef, il est volontaire pour un premier séjour en Indochine, à Tan-Son-Nhut, avec le groupe de transport 2/63 "Sénégal". Ce groupe de transport, équipé de DC-3 Dakota, assure le ravitaillement des postes isolés par le Viêt-Minh et prend une part active aux opérations de la Plaine des Joncs et de Cochinchine. Nommé sous-lieutenant le 1er janvier 1954, il repart à Vientiane pour un second séjour en Extrême-Orient.

Le 20 novembre 1953, débute l'opération Castor. Une armada aérienne de 160 Dakota déverse sur les zones de largage de Dïen-Biên-Phu plusieurs bataillons de parachutistes et des tonnes de matériel. Un terrain improvisé par le Génie sera utilisé intensivement jusqu'au jour où la DCA et les obus de mortier le rendront impraticable. Il faudra alors larguer les charges à très basse altitude afin d'accroître la précision du largage tout en augmentant les risques pour l'intégrité de l'aéronef et de son équipage.
Il participe à cette bataille en effectuant 105 missions au-dessus de la cuvette de Dïen-Biên-Phu entre janvier et mai 1954 date du cesser le feu. Il termine la guerre d'Indochine avec un total de 724 missions de guerre en 3187 heures de vol.

Il passe une année à l'Escadrille d'instruction des troupes aéroportées à PAU et est volontaire pour partir en Algérie. Après un court séjour à Tunis-el-Aouîna, en octobre 1956, le Lieutenant ADIAS est affecté à Colomb-Béchard, au groupe saharien de reconnaissance et d'appui 78 "Tindouf", sur trimoteur Junkers JU52 "Toucan", avec pour mission l'interception et la destruction des caravanes de fellagas venant de Lybie ou du Rio-Oro. En septembre 1957, il rejoint Maison Blanche au groupe de transport 3/62 "Sahara", sur DC-3 Dakota puis sur Nord 2501. Le 1er janvier 1960 il est nommé capitaine.

Il termine la guerre d'Algérie en 1962 avec 429 missions de guerre en 1150 heures de vol. Il est affecté en juillet 1962, à l'Escadron Aérien de Recherche et de Sauvetage 99 à Toulouse Francazal sur quadrimoteur Lockheed L749 "Constellation". Il participe à de nombreuses missions de sauvetage terrestre et maritime dans le monde entier et sauve ainsi un nombre important de vies humaines. Nommé commandant, il prend ensuite le commandement de cet escadron et en décembre 1967, devient chef des Moyens Opérationnels de la base aérienne 101, ce qui revient à un commandement d'escadre, cas unique pour un officier sorti du rang.
Après sa demande de mise à la retraite comme officier de réserve active avec le grade de lieutenant-colonel, il est affecté à la base aérienne 118 de Mont-de-Marsan qui administre le Centre air de perfectionnement et d'information des réserves de PAU dont il prend le commandement.

Le 04 octobre 1983, il est admis à l'honorariat avec le grade de colonel. Il est donc libéré de ses responsabilités de réserviste mais il pratique toujours une intense activité dans les domaines associatifs et de l'aviation civile, en étant instructeur et pilote-largueur. Il pilote aussi dans de petites compagnies aériennes.

Ainsi, au cours de sa carrière entièrement vouée à l'aviation, le colonel Jean ADIAS a effectué plus de 38000 heures de vol sur 134 types d'avions différents qui vont du "Pou du ciel" de 25 chevaux au quadrimoteur Lockheed "Constellation" développant 10.000 chevaux. Il totalise 1241 missions de guerre en 4629 heures de vol.

Deux faits exceptionnels marqueront à jamais le début de sa jeune carrière d'aviateur.

- En 1936, alors qu'il est interne au collège de Betharram, après la conférence prononcée par Jean MERMOZ, il est désigné pour déjeuner à sa table, en face de cette icône de l'Aérospatiale qu'il admire tant.
- En 1939, il est copilote du capitaine Antoine de Saint EXUPÉRY pour un aller-retour Toulouse-Francazal / Le Bourget, sur Bloch 210.

Il est titulaire de nombreuses décorations et distinctions françaises et étrangères :

- Commandeur de la Légion d'honneur (*1977*)
- Médaille Militaire (*1950*)
- Grand-Croix de l'Ordre National du Mérite (*2019*)
- Croix de guerre avec 6 citations à l'ordre de l'Armée (*palmes*)
- Croix de la Valeur militaire avec 2 étoiles de vermeil, 3 d'argent et 1 de bronze
- Médaille de l'aéronautique (*1965*)
- Officier de l'Etoile de la Grande Comores (*1950*) et Chevalier de l'Ordre de l'Etoile d'Anjouan (*1953*)
- Mérite militaire Thaï (*1954*)

ANNEXE 15

Un peu d'humour

Quoi de mieux que la campagne, la nature, rencontrer ceux qui la façonne… se détendre... En attendant la très prochaine balade champêtre, voici quelques "blagounettes du cru".

LE TOUT NOUVEAU COQ

Un bon gros paysan a acheté un nouveau coq, trouvant le sien trop vieux pour "satisfaire" toutes ses poules.
Alors quand le jeune coq arrive dans la basse-cour, le vieux coq vient le trouver et lui dit :
« *Salut jeunot, tu sais que j'approche de la fin, alors si tu veux, tu pourrais me laisser quelques poules…* »
Le jeune coq stupéfié, lui répond : « *Ah non ! Tu as fait ton temps pépé, maintenant c'est mon tour, je prends toutes les poules...* »
Mais le vieux coq, malin, lui demande : « *Alors je te propose une course : le premier arrivé à la clôture, là-bas aura toutes les poules mais tu me laisses quand même 1 mètre d'avance, ok ?* »
Le jeune coq, costaud et en pleine forme comparé au vieux coq qui se tenir à peine sur ses pattes, répond : « *OK, papy, pas de problème, eh... eh... eh* » ... Bref, le jeune coq est persuadé de ne faire qu'une bouchée du vieux !
La course commence….
Le paysan voit son jeune coq courir après le vieux coq, s'empresse de saisir son fusil, et mitraille le jeune coq en gueulant :
« *Putain, ça fait le 5ème coq que j'achète, et c'est le 5ème coq pédé !* »

LE SALON DE L'AGRICULTURE

C'est un couple de paysans qui débarquent à Paris pour le salon de l'agriculture. La femme veut en profiter pour faire ses emplettes chez Tati.
Là, elle essaye un très joli short comme on n'en trouve pas ailleurs, mais hélas impossible de rentrer dedans. Elle essaie un chouette bermuda élastique, mais malgré tous ses effort… ce n'est pas sa taille.
Le mari, qui a toujours un mot gentil pour sa pépettes : « *Tu ne trouveras rien… t'as le cul large comme une batteuse !* »
Après une journée bien remplie, ils se retrouvent à l'hôtel. Comme il a une petite envie le bonhomme commence à tripoter sa germaine, qui se retourne en disant : « *Tu ne penses pas que j'vais mettre la batteuse en route pour un si petit épi ?* »

LE TECHNOCRATE EUROPÉEN

C'est un technocrate européen qui a décidé que dorénavant, tous les oeufs de poule devraient être datés du jour de ponte. Naturellement, on fait procéder à des inspections surprises…
Dans une petite fermette du fin fond de la Corrèze, un inspecteur de la D.G.C.C.R.F. ramène sa fraise : « *Bonjour madame. Je suis inspecteur de la répression des fraudes. Je suis venu constater si vous procédiez bien au marquage du jour de ponte sur tous les œufs que vous vendez.* ».
Immédiatement, elle répond : « *Ah ben ça oui mon gars. Ben sûr qu'y sont datés mes œufs. Tiens, regardes…* »
Alors l'inspecteur regarde les oeufs, et constate que sur chaque oeuf est inscrit : *Aujourd'hui… Aujourd'hui… Aujourd'hui…*

LE VIEUX PAYSAN GAGNE À LA LOTERIE

Eugène, un vieux paysan gagne à la loterie nationale et tout content va au bar fêter ça avec ses copains.
Il leur dit : « *Allez, tournée générale !* »
Et puis demande à ses amis : « *J'aimerais faire un cadeau à ma femme mais je n'ai pas d'idée.* »
« *Offre-lui une télévision couleur.* »
« *Oh mais elle en a déjà une.* »
« *Eh bien une machine à laver alors.* »
« *Oh mais elle en a déjà une aussi.* »

La liste s'allonge sans pour autant aboutir à une solution. Alors, en ayant assez, l'un d'eux lui dit malicieusement :
« *Je sais, offres lui un balai à chiotte, tu verras c'est bien pratique.* »
Naïf, le pauvre paysan répond alors :
« *Oh ben oui c'est une bonne idée car elle n'en a pas.* »
Eugène quitte le bar et va acheter son balai, et l'offre à sa femme. Quelques jours plus tard, les amis d'Eugène lui demandent : « *Alors ta femme était contente de son cadeau ?* »
« *Oui elle était contente de son balai. Elle s'en est servie trois jours mais finalement elle est revenue au papier, elle trouve ça plus pratique !* »

DANS UN PETIT VILLAGE DES CÉVENNES

Cela se passe dans un petit village isolé des Cévennes. Marie Vanachier est la doyenne de ce village et vit dans sa petite maison avec son vieux bouc bien aimé, rescapé de son ancien troupeau.
Or, un jour d'hiver, Marie se rend compte que son bouc a pris froid et tousse affreusement. Complètement paniquée, elle appelle le vétérinaire du coin pour une consultation.
Le vétérinaire examine donc le bouc et dit à Marie : « *Bien voilà, ton bouc a une bronchite aiguë et il faudrait absolument qu'il soit continuellement tenu au chaud. Or je vois qu'il est dans ton étable non chauffée. Il faut absolument que tu trouves une solution.* »
Mais Marie n'est pas très riche, et elle ne peut pas se permettre de chauffer l'étable, ni de chauffer rien du tout pendant la nuit. Elle répond donc au vétérinaire :
« *Bon, pendant la journée, je le garderai dans la cuisine, mais je ne sais pas ce que je vais faire pour la nuit…. Je ne vois qu'une solution : il viendra dormir dans mon lit, ainsi il sera bien au chaud.* »
Le vétérinaire : « *Oui Marie, c'est une solution, mais … et l'odeur ?* »
Marie réfléchit quelques instants puis répond : « *Ha, tant pis, … Il n'aura qu'à s'habituer!* »