| DECEMBRE 2020

LA REVUE DE PRESSE

Défense et intelligence économique

CLUB DÉFENSE - AEGE

JOYEUSES FETES!

Toute l'équipe du club Défense de l'AEGE se joint au pôle veille/publications pour vous souhaiter de bonnes fêtes de fin d'année malgré les circonstances particulières.

L'année 2020 aura été forte en actualité concernant la défense et l'intelligence économique, et pleine de rebondissements. Espérons que 2021 nous réservera de belles surprises et, qui sait, une prise en considération des sujets de guerre économique dans le monde de la défense !

Adam Behillil, Emeryck Edon, Bastien Thérou et Josselin Charpentier

Guerre d'influence française VS Facebook

Depuis le mois de juillet dernier, une nouvelle doctrine appelée "Lutte informationnelle dans le cyber espace" a été mis en oeuvre par nos forces armées, avec comme objectif de lutter contre les campagnes de propagande desservant les militaires français en opérations extérieures. Ces stratégies d'influences biens rodées avaient particulièrement été établies contre ces mêmes offensives bien souvent initiées depuis la Russie.
Facebook a ainsi détecté une centaine de comptes et pages sur son réseau social. Ceux-ci proposaient du contenus de soutien aux armées françaises en Centrafrique et tentaient de limiter l'influence exercée par des comptes gérés depuis la Russie.

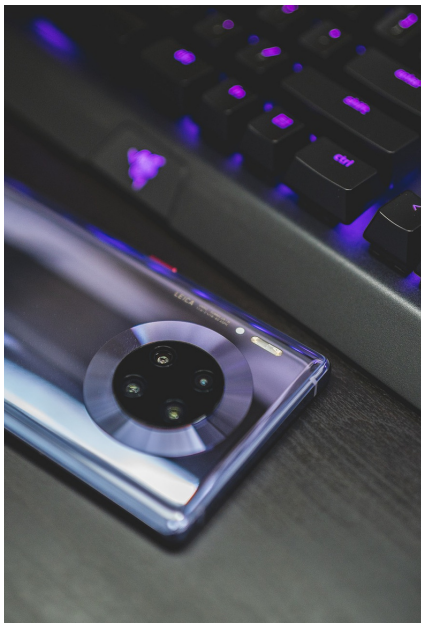
Si notre pays doit se doter de réelles forces dans le combat informationnel, cette lutte ne jouit que d'une faible audience à ce jour. Nos armées doivent continuer de développer ces nouvelles manières de faire la guerre, et réussir à ne pas perdre la bataille face à Facebook.

Huawei veut implanter une usine près de bases militaires stratégiques

Il fut un temps où l'une des principales préoccupations des armées françaises dans le cadre de la lutte contre l'ingérence était l'accroissement rapide des mariages entre jeunes femmes d'origines chinoises et militaires de directions stratégiques bretonnes, selon un rapport du Secrétariat général de la Défense et de la Sécurité nationale (SGDSN)

Aujourd'hui c'est le géant de l'Internet, Huawei, qui souhaite construire une usine à Brumath, dans le Bas-Rhin. Cette dernière doit être consacrée à des solutions technologiques sur les réseaux mobiles.

Si, à première vue, cela ne reste qu'une usine, une question reste en suspens : Huawei a-t-il choisi cet emplacement pour les paysages alsaciens? Car, à quelques kilomètres du terrain, on trouve deux régiments très stratégiques spécialisés sur la guerre électronique mais aussi sur le renseignement d'origine électromagnétique.



A proximité, on trouve aussi le Centre de formation interarmées au renseignement dépendant de la DRM, et un site de la DGSE.

Huawei semble donc avoir particulièrement bien choisi l'emplacement de cette nouvelle usine, à moins que le gouvernement chinois lui ait soufflé des coordonnées GPS. Pékin serait-il en train de placer ses pions?

Photonis : nouveaux rebondissements

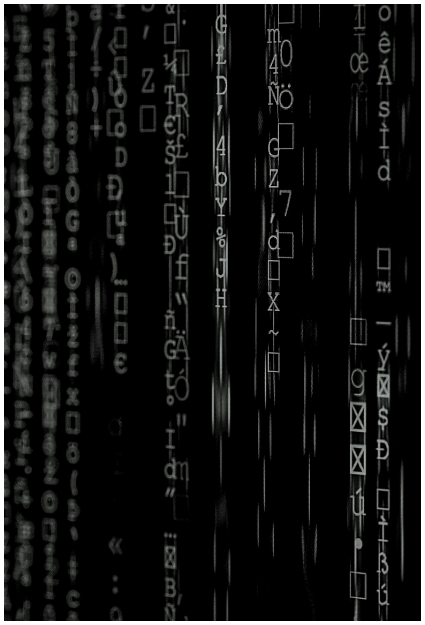
Photonis, pépite française de la vision nocturne, ne devrait finalement pas passer sous contrôle américain. D'abord prêt à une vente, Teledyne a ensuite refusé les conditions posées par le gouvernement francais, avant de revenir sur sa décision et de proposer une nouvelle offre d'achat. Mais cette fois, la décision semble définitive : Photonis devrait rester sous pavillon tricolore.
La ministre des Armées, Florence Parly, a rappelé la "volonté de protection des intérêts stratégiques de la France".

Espérons que cette histoire à rebondissements terminera par un *happy end*. Mais il semble nécessaire que chacun prenne bien conscience que nos entreprises stratégiques sont vulnérables. Des puissances étrangères pourraient à nouveau jouer sur la frilosité des banques françaises en terme d'octroi de crédits afin de relancer l'offensive auprès de nos pépites fragilisées par la crise.

Les Etats-Unis face aux cyber attaques

Une attaque informatique de grande ampleur se déroule aux Etats-Unis depuis le printemps. Celle-ci aurait été mise en oeuvre *via* l'infiltration d'un *malware* dans un logiciel de gestion de réseaux, dont le gouvernement américain est client: Solarwinds. Une *back door* lors d'une mise à jour aurait permis aux attaquants d'infiltrer à la fois les réseaux gouvernementaux ainsi que ceux de très nombreuses entreprises. L'unité de cybersécurité de la Sécurité intérieure à reconnu ne pas avoir à ce jour déterminé l'ampleur des dégâts liés à cette cyber attaque. Un manque de cyber combattants entraine par ailleurs une difficulté à résoudre le problème.

Face à l'ampleur de l'attaque, il est d'ailleurs très probable que les pirates soient liés à un gouvernement. Les Etats-Unis ont accusés le gouvernement russe, bien que Vladimir Poutine ait démenti toute implication. Quoi qu'il en soit, les modes de conflits ont évolué avec les technologies développées ces dernières années.



Cette évènement prouve encore une fois la nécessité d'investir le monde immatériel dans les stratégies étatiques de défense. Cette attaque va coûter des milliards de dollars aux Etats-Unis. Et ils ne sont pas les seuls concernés: l'Agence européenne du médicament (AEM) a elle aussi été visée par une cyberattaque, alors même qu'elle délibère sur les autorisations de vaccins dans la lutte contre la COVID19.

L'Allemagne défends ses intérets

En parallèle des hésitations et revirements incessants du gouvernement francais sur l'affaire Photonis, le Conseil des ministres allemand a lui fait le choix de la clarté et de la fermeté dans la protection d'Hensodt, une ex-filiale d'Airbus.

En effet, le gouvernement va acquérir 25,1% des parts de la pépite européenne du secteur de l'électronique de la défense, soit un investissement d'environ 450 millions d'euros. Berlin a donc choisi de protéger ses intérêts stratégiques face aux investisseurs étrangers, notamment chinois et américains.