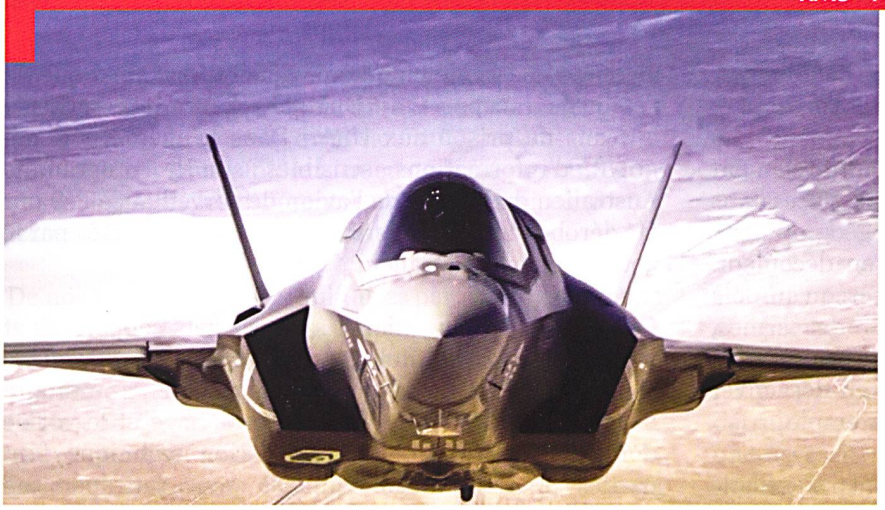
Zeitschrift: Revue Militaire Suisse
Band: - (2018)
Heft: [2]: Numéro Thématique 2

Artikel: Les cyber-attaques, plus grande menace pour les armes modernes?
Autor: Kudelski, André
DOI: https://doi.org/10.5169/seals-823453



Le chasseur à hautes performances F-35 est furtif, donc peu vulnérable aux missiles. Mais qu'en est-il de sa protection contre les virus informatiques ?

Cyber

Les cyber-attaques, plus grande menace pour les armes modernes ?

André Kudelski
Chairman & CEO, Kudelski S.A.

Le cyber espace est devenu un composant conventionnel de la guerre, s'ajoutant aux domaines traditionnels des opérations militaires que sont la mer, la terre, les airs et l'espace. La complexité du développement d'armements et de leurs composants offre des opportunités pour les hackers, qui peuvent infiltrer les tiers dans l'industrie de défense durant le processus de développement de l'arme. Pour le monde militaire, la menace principale vient d'opérations cyber d'états ou de hackers freelances se réclamant d'un Etat, qui accomplissent des activités de collecte de renseignements étendues et très sophistiquées.

La complexité amène de la vulnérabilité

Les armes évoluent et deviennent de plus en plus sophistiquées et létales. Leur développement est long, complexe, coûteux et intègre de plus en plus des composants électroniques et cyber. L'intégration d'éléments d'intelligence artificielle (IA), notamment pour les systèmes d'armes létales autonomes (SALA), ou semi-autonomes augmente la cyber vulnérabilité de ces armes. Grâce à une cyber-attaque, un adversaire pourrait éliminer la menace d'une machine ou d'une arme (ex : avion de chasse ou missile) en la désactivant, sans avoir recours à aucune action cinétique ou, pire, en prendre le contrôle.

Parallèlement, une géopolitique de l'armement est visible, notamment concernant le contrôle des technologies militaires développées dans l'industrie de l'armement. En 2017, la Chine, dans son plan national, a annoncé le développement d'IA qui devrait atteindre le niveau des entreprises américaines d'ici 2020, avec l'ambition de devenir « le premier centre d'innovation de l'IA au monde » d'ici 2030.[1] D'autres pays comme les Etats-Unis et la France établissent aussi des plans nationaux, reconnaissant qu'il s'agit d'une question d'Etat majeure.[2] Vladimir Poutine a même affirmé que la nation « *qui deviendra le leader dans ce domaine (l'IA) deviendra le leader du monde* ».[3]

Le dernier avion militaire américain, le Lockheed Martin F-35 *Lightning* II – soit le programme militaire américain le plus coûteux de son histoire (développement et production estimés à USD 406 milliards)[4] – met en exergue ces problématiques de nouvelles technologies de l'armement et de la complexité de la géopolitique de l'armement militaire. Le F-35, décliné en trois versions, est un avion complexe, qui intègre beaucoup de composants électroniques, permettant à la fois des performances en vol, la collecte et l'échange de données. Cet avion est parmi les plus avancés de sa génération. Néanmoins, ces capacités avancées amènent des problématiques dont les états doivent prendre conscience car elles s'appliquent à tout armement moderne. Par exemple, la maintenance du système, appelé ALIS (*Autonomic Logistics Information System*), est logiquement centralisée aux Etats Unis pour tous les utilisateurs du F-35, américains ou étrangers. A ce jour, plus de dix états ont acheté ou vont acquérir cet avion (Australie, Canada, Corée du Sud, Danemark, Israël, Italie, Japon, Norvège, Pays-Bas, Turquie, et Royaume-Uni).

Or le système ALIS offre aux hackers des opportunités de faire des attaques de l'« homme du milieu » (*man-in-the-middle - MITM*) qui permettraient d'avoir accès au système de management de la maintenance de l'appareil, aux systèmes des missions, ainsi qu' aux clés cryptographiques utilisées dans chaque appareil en service.[5]

1 MOZUR Paul. «Beijing Wants A.I. to Be Made in China by 2030», *The New York Times*, Jul 20, 2017https://www.nytimes.com/2017/07/20/business/china-artificial-intelligence.html

2 FAURE Juliette. «L'intelligence artificielle peut-elle nous gouverner», *Diploweb*, Jan 24, 2018 https://www.diploweb.com/L-intelligence-artificielle-peut-elle-nous-gouverner.html

3 VINCENT James. «Putin says the nation that leads in AI 'will be the ruler of the world'», *the Verge*, Sep 04, 2017 https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world

4 TURNER Julian. «The $1 trillion question: is the F-35 project too big to fail», Airforce Technology, Jul 16, 2018 https://www.airforce-technology.com/features/f-35-project/

5 KÜMMERLING Pascal. «Le F-35, une machine à broyer la concurrence européenne», *24 Heures Blog*, Oct 05, 2017 http://psk.blog.24heures.ch/archive/2017/10/05/le-f-35-une-machine-a-broyer-la-concurrence-europeenne-864465.html

Par ailleurs, ces systèmes de centralisation de données, dans un contexte de clouding, permettent l'accès aux données collectées par les armes qu'elles soient des avions, tanks, bateaux, missiles ou tout autre élément ayant des sondes. Les données sont *in fine* stockées dans un serveur, mettant en exergue le lieu géographique où ces données sont et les risques qui en découlent. Une réflexion plus poussée peut imaginer qu'au-delà de l'accès d'un tiers à des données sur des armes, un Etat ayant conçus une arme et ayant accès à des données durant son utilisation, pourrait en désactiver potentiellement le service à distance par exemple.

Les risques de fuites de données (data leak) ont par exemple poussé Israël à créer un système complet de maintenance avec des firewalls pour s'assurer qu'aucune donnée ne quitte leur territoire. Cette décision, avec le stockage de pièces de rechange, permet d'augmenter son autonomie et son indépendance en cas de conflit.[6] A noter que l'Etat d'Israël a une notion de doctrine militaire très précautionneuse lorsqu'il s'agit de tout élément qui pourrait venir limiter sa capacité d'autonomie et d'indépendance qui s'explique par le géopolitique de la région.

Les maîtres des APT et de la rétro-ingénierie

La Chine et la Corée du Nord ont été longtemps accusées de cyber intrusions pour espionner et voler des données à des Etats occidentaux et Asiatiques dans les domaines de l'aéronautique et de la défense. Deux campagnes de menace persistante avancée (Advanced Persistent Threat - APT) nommées « Titan Rain » et « Byzantine Hades », ont permis l'exfiltration massive d'informations top secrètes. En octobre 2017, des plans de navires militaires de l'entreprise Daewoo ont été dérobés à travers des cyber-attaques.[7] La méthodologie utilisée durant ces différentes attaques attribuerait ces opérations à la Chine et la Corée du Nord.

Les avions militaires américains ont un attrait particulier pour la Chine car ils ont toujours été la référence en termes de performances et d'expériences positives sur de nombreux théâtres d'opérations. En 2015, Edward Snowden révélait notamment que cette dernière avait volé des plans du F-35.[8] En mars 2016, un groupe de hackers chinois plaidaient coupable pour le hacking d'entreprises américaines de défense, comme Boeing, pour le vol de plan et de propriété intellectuelle du F-35, du chasseur Lockheed Martin F-22 *Raptor* (le première avion de chasse de cinquième génération) ainsi que de l'avion de transport C-17. Un des hackers a été condamné à 4 ans de prison aux USA.[9] Dans la même période, 30GB d'informations sensibles sur le programme Australien du F-35 et de l'avion de surveillance P-8 ont été dérobés à une entreprise de défense contractée par le gouvernement australien.[10]

Grâce à la rétro-ingénierie, à des projets coopératifs et à des transferts technologiques, la Chine peut produire la majorité de ses systèmes d'armements militaire de manière autonome. Ainsi, l'espionnage et le vol de données de projets et d'information technique font parties de la stratégie chinoise pour rattraper son retard dans le domaine des technologies militaires les plus avancées. Le deuxième porte-avion chinois, basé sur le premier qui était une rénovation d'un bâtiment de deuxième main des années 80 acheté à l'Ukraine en 1998, est un bon exemple de rétro-ingénierie. Basé sur ce navire non terminé, la marine chinoise a planifié de lancer en 2020 son premier porte avion « fait maison », doté de technologies de pointe.

La Chine est ainsi accusée de voler des données militaires confidentielles, afin de pouvoir répliquer des designs et des technologies de pointe, comme des radars, des moteurs ou des *softwares*. Ceci permet de rattraper un retard de manière bien plus rapide que l'investissement de millions en R&D durant des décennies, sans l'assurance d'atteindre son objectif. Le résultat est que le dernier avion militaire chinois, le *Chengdu* J-20, intègre des éléments qui étaient apparemment volés du F-22 américain, le premier avion de cinquième génération du monde, et du MiG 1.44 russe, un projet qui n'a jamais atteint le stade de la production. Bien qu'une ressemblance visuelle puisse être mise en avant, comme avec le *Shenyang* J-31, qui ressemble étroitement au F-35, il est difficile d'évaluer les composants et les éléments internes de ces avions afin d'établir si oui ou non, ils sont vraiment le fruit de rétro-ingénierie.

Pourquoi les avions militaires ?

Disposer d'avions militaires performants est un avantage stratégique crucial. La suprématie aérienne reste en effet un élément vital sur le champ de bataille, comme l'ont encore démontré la guerre du Golf de 1991 (Opération DESERT STORM) et ou celle d'Irak en 2003 (Opération IRAQI FREEDOM). Durant ces guerres, la coalition, menée par les Etats-Unis, a disposé d'une domination totale du ciel grâce à leurs avions militaires incorporant des technologies avancées. La coalition a utilisé une approche de guerre en réseau (*network centric warfare*). Cette approche a permis une prise de

6 KÜMMERLING Pascal. «Le F-35, une machine à broyer la concurrence européenne», *24 Heures Blog*, Oct 05, 2017 http://psk.blog.24heures.ch/archive/2017/10/05/le-f-35-une-machine-a-broyer-la-concurrence-europeenne-864465.html

7 CHOI Haejin. «North Korea hacked Daewoo Shipbuilding, took warship blueprints: South Korea lawmaker», *Reuters*, Oct 31, 2017 https://www.reuters.com/article/us-northkorea-missiles-cybercrime/north-korea-hacked-daewoo-shipbuilding-took-warship-blueprints-south-korea-lawmaker-idUSKBN1D00EX

8 PAGANINI Pierluigi. «Chinese hacker admitted hacking US Defense contractors», *Security Affairs*, Mar 24, 2016 http://securityaffairs.co/wordpress/45597/intelligence/china-hacked-us-defense-contractors.html

9 WORLAND Justin. «Chinese Man Sentenced to Prison for Trying to Hack Boeing», *Time*, Jul 14, 2016 http://time.com/4405934/chinese-hacking-boeing/

10 AFP. «F-35 Stealth Fighter Data Stolen in Australia Defence Hack», *Securityweek*, Oct 12, 2017 http://www.securityweek.com/f-35-stealth-fighter-data-stolen-australia-defence-hack

décision qui utilisait la collecte de données et le partage d'informations pour obtenir un avantage concurrentiel sur le champ de bataille, disposant du processus de prise de décision le plus rapide, le mieux adapté pour intégrer et synchroniser les différentes unités et services (forces terrestres, aériennes et navales).

De nos jours, les experts militaires parlent de cinquième génération de chasseurs aériens qui intègrent les fonctionnalités les plus avancées du marché comme une signature furtive (une surface équivalente radar très faible), une super manœuvrabilité (poussée vectorielle), une avionique avancée (systèmes électroniques), la fusion des données (création de données au travers de senseurs et le partage de celles-ci) et des capacités multi-rôles (accomplir diverses missions).[11]

Le développement d'avions militaires et de drones aux capacités avancées permettra la mise en œuvre d'une suprématie aérienne pour les années à venir, particulièrement dans les prochains points chauds de la planète. Ils seront également un important support pour les éléments de projection de la puissance (power projection) dans la mise en œuvre de tactiques empêchant l'accès à des zones spécifiques (Anti-Access/Area Denial - A2/AD), par exemple dans la mer de Chine méridionale ou sur la ligne en neuf traits (Nine-Dash Line), ligne de démarcation où Pékin affirme détenir une souveraineté territoriale sur les mers Jaune et du Japon en ce qui concerne la Corée du Nord.

D'où les actes de cyber-attaques visant l'armement et spécifiquement le domaine aérien. Ces évolutions mèneront à une logique simple où le coût/bénéfice de pirater une arme sera plus avantageux que de la détruire par des méthodes traditionnelles. Il y a donc une nécessité pour les gouvernements de concevoir des avions de combat qui, dès leur phase de design et de conception, sont à même de faire face aux cyber-attaques et d'investir dans leurs capacités technologiques et humaines de sécurité des opérations (OpSec) pour identifier les informations critiques à protéger afin d'éviter leur diffusion et de réduire leur exploitation.

A. K.

11 DE BRIGANTI Giovanni. "F-35 Reality Check Ten Years On - Part 1: 'Fifth-Generation' and Other Myths", *Defense-Aerospace*, May 09, 2012 http://www.defense-aerospace.com/article-view/feature/135080/f_35-reality-check-10-years-o-%28part-1%29.html

Le F-35 C est la version développée pour l'US Navy, disposant d'ailes pliables ainsi que d'un train d'atterrissage renforcé. Plus lourd que la version A des forces aériennes, il doit renoncer à l'emport d'un canon interne. Photo © US Navy.