L'angle mort

Ce qu'une prédiction juste de 2019 nous apprend sur l'échec de la prospective

Que vaut une prédiction juste sur le « quoi » quand on s'est trompé sur le « comment » ? C'est la question la plus utile que je me sois posée cette année. Elle m'a été posée par l'Histoire, qui a de mauvaises manières.

I. La copie de 2019

En juin 2019, avec un camarade, nous publiions dans le cahier de la Revue Défense Nationale consacré au Salon du Bourget une analyse sur les bases aériennes face aux menaces futures. Ni prophétie, ni coup d'éclat : une note d'officiers qui font leur travail, celui de regarder devant.

Nous y écrivions que les mini-drones, presque invisibles au radar, naviguant bas et lentement, permettaient « des attaques surprises, de basse technologie et sans exposer les opérateurs ». Nous rappelions que des drones rustiques emportant des obus de mortier avaient endommagé des bombardiers russes stationnés en Syrie début 2018, lors d'attaques saturantes. Nous alertions enfin sur une prolifération qui faisait passer des capacités autrefois étatiques dans l'arsenal d'adversaires irréguliers.

Relu aujourd'hui, le texte a un mérite : il est daté, signé, publié. Il constitue donc ce que la prospective produit rarement : une pièce à conviction opposable à son auteur. On va s'en servir.

II. Le verdict de l'Histoire

Le 1er juin 2025, l'opération ukrainienne Spiderweb a visé cinq bases aériennes russes, jusqu'en Sibérie orientale, à plus de 4 000 kilomètres du front. 117 drones FPV, du matériel de vidéaste de mariage militarisé. Une quarantaine d'appareils touchés selon Kiev, une vingtaine selon des sources américaines, environ 10 % de la flotte selon Berlin : peu importe la borne retenue, il s'agissait de Tu-95 et d'A-50 que l'industrie russe ne sait plus produire. Le préjudice, estimé par Kiev à plusieurs milliards de dollars, a été infligé par des engins dont le coût unitaire se compte en centaines d'euros : la flotte entière valait le prix d'une berline allemande.

Sur le « quoi », notre copie de 2019 tient. Saturation : validée. Basse technologie : validée. Prolifération : validée au-delà de nos craintes.

Sur le « comment », elle a été pulvérisée.

Car nous raisonnions, comme toute la littérature de l'époque, en couches concentriques : détecter loin, intercepter en profondeur, durcir au centre. La défense comme un oignon. Or Spiderweb n'a percé aucune couche. Les drones n'ont pas franchi de frontière : ils sont entrés en Russie par la logistique civile, cachés dans des cabanons en bois montés sur des camions, conduits par des chauffeurs qui

ignoraient leur cargaison. Ils ont patienté dix-huit mois. Puis ils ont décollé de parkings situés en bordure de piste, pilotés en partie via le réseau mobile russe lui-même.

L'attaque n'est pas venue de l'extérieur. Elle est née dedans, portée par les flux mêmes que la base défendue consomme pour vivre : routes, conteneurs, réseaux télécoms.

C'est ici que la leçon dépasse le militaire. Toute défense en couches suppose un extérieur. Quand la menace emprunte vos propres flux, le périmètre devient une fiction administrative : une ligne qui existe dans les organigrammes et les schémas de zonage, plus dans la réalité.

Les responsables du numérique ont appris cette leçon avant les militaires, et c'est l'ancien responsable de la transformation numérique de l'armée de l'Air et de l'Espace qui vous le dit, avec ce qu'il faut de malice : cela fait quinze ans que les DSI sérieux ont enterré le périmètre. La clé USB dans le parking, le prestataire compromis, la mise à jour logicielle vérolée en amont de la chaîne : le monde cyber a théorisé dès 2010 le « zero trust », ce principe selon lequel aucun flux n'est réputé sûr du seul fait qu'il vient de l'intérieur. Spiderweb, c'est une attaque par la chaîne d'approvisionnement appliquée au monde physique. Les pare-feux ont fait faillite avant les clôtures ; les clôtures n'ont pas voulu le savoir.

L'alerte n'était d'ailleurs ni seulement américaine, ni seulement civile. Dès 2008, Éric Filiol, ancien militaire devenu chercheur en cyberdéfense, théorisait avec ses co-auteurs l'attaque par les interdépendances : dans la revue spécialisée MISC début 2008, puis dans cette même Revue Défense Nationale en mars 2009, sous un titre qui dit tout, « Cyberguerre : de l'attaque du bunker à l'attaque dans la profondeur ». Sa thèse constante : une infrastructure critique ne se réduit pas à sa dimension technique, elle comprend ses composantes humaines et externes, et l'attaquant rationnel choisit le chemin au coût le plus faible, qui passe rarement par la porte blindée. Ses travaux ultérieurs iront jusqu'à formaliser mathématiquement la recherche de ce chemin optimal, en adoptant la vision de l'attaquant et non celle du défenseur. Autrement dit : la théorie de Spiderweb dormait dans nos propres bibliothèques, en français, depuis quinze ans.

III. Les sept ans

Deuxième leçon, plus dérangeante que la première, car elle ne concerne pas l'adversaire mais nous-mêmes : le délai.

Reconstituons la chronologie. 2018 : des drones artisanaux endommagent des bombardiers russes en Syrie ; le signal est public, documenté, commenté. 2019 : nous l'écrivons noir sur blanc dans une revue de référence, parmi d'autres auteurs qui alertent dans le même sens. 2025 : Spiderweb démontre le scénario à échelle industrielle, puis l'automne voit des essaims de drones non identifiés fermer des aéroports et survoler des bases en Europe. 2026 : l'actualisation de la loi de programmation militaire ajoute 1,6 milliard d'euros à la défense antiaérienne et antidrone, crée un cadre juridique pour neutraliser les drones au-dessus des sites vitaux, et le service d'infrastructure de la défense lance les premiers chantiers de durcissement passif des bases : couverture des aéronefs hors hangars, filets, camouflage.

Soyons justes : la lutte anti-drones active a progressé entre-temps, fortement accélérée par la préparation des Jeux de Paris 2024. Mais protéger un ciel d'événement pendant quelques semaines et durcir durablement des emprises sont deux problèmes différents. Le second, le moins spectaculaire, celui des abris, des filets et de la dispersion, attend 2026 pour ses premiers chantiers.

Sept ans entre l'analyse publiée et la ligne budgétaire. Et encore : il a fallu que l'Histoire fasse la démonstration elle-même, en direct et en 4K, pour que le circuit s'accélère.

Qu'on me comprenne bien : je ne blâme ni les décideurs de 2019, ni les états-majors, qui arbitrent sous contrainte entre cent menaces documentées. Le problème n'est pas la mauvaise volonté. Le problème est structurel : la prospective française ne manque pas de visionnaires, elle manque d'un circuit de conversion. Nous produisons des alertes comme d'autres produisent des rapports annuels : abondamment, sincèrement, et pour l'étagère. L'alerte vieillit sept ans dans le circuit ; l'adversaire, lui, itère en sept semaines. Spiderweb a été conçue, testée et exécutée en dix-huit mois, soit moins de temps qu'il n'en faut chez nous pour faire converger une expression de besoin.

J'ai passé une partie de ma carrière dans le numérique de défense, où ce différentiel de tempo porte un nom : la dette. Dette technique quand on repousse la modernisation, dette prospective quand on repousse la décision. Dans les deux cas, les intérêts sont composés, et c'est toujours l'événement qui présente la facture.

IV. Vade-mecum de la prospective utile

Alors, que faire ? Puisque cet essai s'est ouvert sur notre propre copie, tirons les règles de nos propres erreurs. Cinq règles, chacune avec son application défense et son miroir numérique, car c'est le même muscle qui travaille.

Règle 1 : ne pas analyser la menace, la jouer. Nous avions identifié le drone ; nous n'avions pas joué la partie adverse jusqu'au bout, celle qui cherche le chemin le moins défendu, donc le plus improbable. C'est toute la différence entre l'analyse et le wargaming : l'analyste décrit une capacité, le joueur adverse cherche à gagner avec, et il trouve des chemins qu'aucune note d'état-major n'aurait osé écrire. Un wargame honnête aurait fait partir les drones du parking du supermarché voisin, pas de l'horizon radar. Encore faut-il respecter la condition qui fait tout : donner au camp rouge le droit de gagner, et à ses trouvailles un débouché ailleurs que dans un compte rendu. La France a d'ailleurs créé en 2019 sa Red Team Défense, chargée de faire imaginer par des auteurs de science-fiction les menaces de 2030 à 2060. La même année que notre article : preuve que l'imagination était au rendez-vous. C'est la suite du circuit qui ne l'était pas, et les règles 3 et 5 disent pourquoi. Miroir numérique : le test d'intrusion procède du même esprit, à condition de ne pas le réduire à un exercice de conformité annuel dont le périmètre est négocié à l'avance, c'est-à-dire à une fiction de plus.

Règle 2 : dater ses prédictions et fixer le rendez-vous de relecture. Une prospective sans échéance de vérification est une opinion avec une mise en page. L'auto-fact-check doit être institutionnel : chaque document prospectif devrait naître avec sa date de relecture obligatoire et son critère de succès observable. Défense : relire les livres blancs et revues stratégiques à mi-parcours, publiquement, en assumant les écarts. Numérique : tout schéma directeur devrait contenir la liste de ses propres paris, avec la date à laquelle on saura s'ils étaient bons. Celui qui refuse cette clause vous dit quelque chose sur la confiance qu'il place dans son propre document.

Règle 3 : mesurer le délai alerte-décision, et rien d'autre. On évalue la fonction prospective au nombre d'études produites, jamais au temps qu'il faut pour qu'une alerte devienne une décision dotée de crédits. C'est l'unique indicateur qui compte, et il est mesurable : date de première alerte documentée, date de la décision, écart. Sept ans dans notre cas. Défense comme numérique : tant que ce chiffre n'est pas suivi en comité de direction, la prospective reste un centre de coût culturel, un

supplément d'âme.

Règle 4 : traquer l'angle mort conceptuel avant l'angle mort factuel. Notre erreur de 2019 n'était pas un manque d'information, tout était public ; c'était un cadre hérité, le périmètre, qui formatait ce que nous étions capables d'imaginer. Les faits manquants se cherchent ; les concepts manquants ne se voient pas, précisément parce qu'on pense avec. D'où une pratique : importer régulièrement les cadres d'un autre domaine et regarder ce qu'ils révèlent. Le zero trust appliqué à la protection des emprises physiques aurait fait gagner des années. Inversement, la dilution et le durcissement, vieilles règles de l'art aérien, auraient épargné bien des architectures numériques centralisées autour d'un unique point de défaillance.

Règle 5 : brancher la prospective sur un circuit de décision court. Une cellule prospective qui remet ses travaux à une chaîne hiérarchique de sept étages produit de la littérature : brillante, et inutile. Il faut un canal court vers l'autorité qui décide et qui paie, et un droit de tirage rapide pour expérimenter sans attendre le cycle budgétaire. Défense : c'est l'esprit des dispositifs d'innovation type défis ouverts ou battle labs, à condition que la sortie d'expérimentation débouche sur un marché, pas sur un rapport. Numérique : c'est toute la différence entre une DSI en « mode produit », qui livre en continu, et une DSI en cycle en V, qui livre des promesses.

Rendez-vous pris

Une dernière chose, et c'est la plus importante : cet essai s'applique sa propre règle 2.

J'affirme ici que la menace née des flux internes (logistique, sous-traitance, réseaux civils) deviendra le mode d'action dominant contre les infrastructures militaires et critiques, et que les défenses périmétriques continueront d'absorber l'essentiel des budgets pendant encore des années, parce qu'elles se voient, se visitent et s'inaugurent.

Rendez-vous en 2033 pour la relecture. C'est dans sept ans. Le délai standard, vous disais-je.

BDSN

L'article de 2019 : « Les bases aériennes de l'Armée de l'air face aux défis des menaces et opérations futures », cahier RDN du Salon du Bourget 2019, defnat.com. Faits cités : opération Spiderweb (juin 2025, bilans contrastés selon Kiev, Washington et Berlin) ; actualisation de la LPM 2024-2030 (présentée le 8 avril 2026, promulguée en août 2026) ; chantiers de durcissement des bases lancés en 2026 par le service d'infrastructure de la défense ; Red Team Défense lancée fin 2019 par l'Agence de l'innovation de défense. Sur l'attaque indirecte : P. Evrard et É. Filiol, MISC n°35 (janv. 2008) et n°36 (mars 2008) ; É. Filiol et F. Raynal, « Cyberguerre : de l'attaque du bunker à l'attaque dans la profondeur », Revue de Défense nationale et sécurité collective, mars 2009 ; É. Filiol, chapitre in D. Ventre (dir.), Cyberguerre et guerre de l'information, Hermès-Lavoisier, 2010 ; C. Gallais et É. Filiol, Journal of Information Warfare, vol. 16 n°1, 2017.