# La Lettre de MINERVE

La lettre trimestrielle de Minerve
est éditée par l'Association de l'Enseignement Militaire
Supérieur, Scientifique et Académique

Lettre n° 66 – juin 2025

**Table des matières**



**Rédactrice en chef: ORC Isabelle PRAUD-LION - isabelle.praud-lion@ipl-sas.fr**
**Mise en page : Colonel (ER) Marc LIMON - limonmrc@orange.fr**

# La Lettre de MINERVE

La lettre trimestrielle de Minerve
est éditée par l'Association de l'Enseignement Militaire
Supérieur, Scientifique et Académique

Lettre n° 66 – juin 2025

**Éditorial du Président, le Général de corps d'armée (2S) Olivier GOURLEZ de la MOTTE**
**« Le CYBER : qu'entend-on par Cyber ? »**

Simple préfixe, il signifie la dimension informatique ou de réseau à la notion qu'il introduit. Cependant, il n'est pas aussi banal que cette définition laisse à penser. Comme préfixe, cyber est souvent employé pour alerter sur un risque, avec la cybersécurité, ou vis-à-vis d'une menace, on parle de cyberharcèlement ou de cyberattaque dans l'espace numérique. Même le mot cyberespace n'est jamais utilisé de façon anodine, il introduit en général des problématiques de menaces complexes.

Dans le cyberespace, il est question de malveillance dans l'utilisation de l'Intelligence Artificielle, de transformer les objets connectés comme autant de « portes d'entrée » vulnérables aux intrusions. Or ce monde connecté nous environne de toutes parts, dans notre quotidien et surtout dans le monde des armées. Il est en perpétuelle évolution et intègre des notions nouvelles à des rythmes de plus en plus élevés. Il n'y a pas le choix. Il faut appréhender les risques qu'il présente, mais surtout trouver des parades.

Or le monde numérique détient en lui-même les mesures et contre-mesures pour déjouer les pièges qui nous sont tendus.

Ne nous laissons pas impressionner par ces menaces et cette guerre qui semble ne jamais s'arrêter. Prenons ce « domaine du Cyber » comme un véritable champ de bataille, où nous avons à défendre nos intérêts, déterminer nos centres d'intérêts et nos capacités à les préserver. L'adversaire doit aussi être identifié, sans complaisance. Or il est multiple et variable.

Voilà un univers d'étude qui doit nous motiver. L'acquisition des compétences dans ce domaine et la connaissance des acteurs et armes devient un véritable enjeu, au risque d'être, à notre insu, délogé du terrain de confrontation.

Bonne lecture à vous.

**Mot du Directeur général de Minerve, le Général (2S) Nicolas RICHOUX**

Chers amis,

L'année est déjà bien avancée et l'été approche à grands pas, tandis que Minerve poursuit son chemin dans un environnement changeant. Le Colonel PHELUT vient en effet de prendre le poste de directeur du CEMS-T en remplacement du général CHIGOT, admis en deuxième section. Le CEMS-T, enfin en rythme de croisière, devrait reprendre la place du CCF dans ses bâtiments historiques dès cet été. Aucun changement pour Minerve qui conserve sa permanence privilégiée au cœur de l'Ecole. Notons que notre association bénéficie du soutien actif et réaffirmé du nouveau directeur, qui a annoncé son intention de rejoindre prochainement nos rangs.

Quelques points :

- lors de la dernière Lettre de Minerve, je vous annonçais en avril une conférence sur l'Algérie, avec comme invité l'ambassadeur DRIENCOURT. Celle-ci a malheureusement été annulée par décision du commandement, en raison d'un télescopage supposé avec l'actualité. Nous regrettons fortement cet acte de censure qui nous a été annoncé au dernier moment et qui nous a mis en porte-à-faux vis-à-vis de nos auditeurs fidèles et de notre invité. J'espère que vous voudrez bien tous nous en excuser. Nous ne renonçons toutefois pas à reprogrammer cette séquence, peut-être en fin d'année, tant ce sujet apparait important et on ne peut plus d'actualité ;
- la prise d'armes de fin de scolarité de l'EMSST aura lieu le 16 juin en fin de matinée ;
- je vous annonçais également dans la précédente Lettre une possible soirée « alumni », organisée par l'EMSST au profit des stagiaires. Son objectif est de mettre en réseau les anciens et les nouveaux lauréats de l'EMSST. Cette soirée aura bien lieu le 18 juin prochain avec le soutien actif de Minerve.

Pour le reste, je vous souhaite à tous de belles vacances d'été ensoleillées et je vous donne rendez-vous à la rentrée.

Notez dès à présent la prochaine conférence du 2 d'octobre, qui aura pour thème l'intelligence artificielle. Venez nombreux !

À bientôt !

**Editorial de la Rédactrice en chef**

*Isabelle PRAUD-LION, Officier réserviste citoyen auprès du CCF*

Chers lecteurs,

Cette lettre, vous l'avez compris, a pour thème : le Cyber.

La diversité des contributions permet au moins de se créer une image de cette réalité. Marie KRATZ, Professeur très respectée pour ses travaux dans le monde de la décision économique, nous présente les réflexions en cours sur la couverture des impacts financiers des risques liés aux cyber-attaques pour les acteurs économiques. À cet égard, je dois me faire pardonner car, avec son accord, nous avons bien simplifié la partie statistique de son article.

Les « *honeypots* » du chef de Bataillon EGON, sont un bon exemple du nouveau champ de bataille applicable à des domaines tels que la stratégie et les leurres par exemple en matière de transmission et codage.

Bref, bonne lecture et j'en profite pour vous souhaiter à tous, un très bel été.

**Rédactrice en chef: ORC Isabelle PRAUD-LION -** isabelle.praud-lion@ipl-sas.fr
**Mise en page : Colonel (ER) Marc LIMON -** limonmrc@orange.fr

**Minerve** est soutenue par la **Fondation Crédit Social des Fonctionnaires**

**Nouvelles de l'EMSST : la fin d'année académique**

*Par le Colonel Alexis-Emmanuel LAPACHERIE, directeur de l'EMSST*

La fin de l'année académique 2024-2025 pour les 172 officiers stagiaires de l'EMSST marque l'aboutissement de plusieurs années d'investissement personnel. En effet, certains de nos camarades ont commencé dès 2020-2021, dans les murs de l'EMSST, la préparation du concours du diplôme tactique. Puis, les lauréats des concours de l'École de Guerre Terre et du diplôme technique ont été orientés et sélectionnés, avant de poursuivre leur montée en compétence lors des cours de préparation à la mise en scolarité, toujours au sein de l'EMSST. Enfin, ils ont pu rejoindre leurs établissements de formations pour une à plusieurs années de scolarités intenses.

Cette fin d'année va être clôturée par une prise d'arme le mardi 16 juin puis par une soirée alumni organisée par l'association Minerve et l'EMSST le mercredi 18 juin. Cette soirée, première du genre, vise à rassembler plusieurs générations d'officiers autour de partenaires académiques et économiques pour se retrouver et discuter. La soirée sera organisée autour de pôles par origine de formation ou domaine afin de faciliter les échanges.

Au bilan, l'année 2024-2025 a été particulièrement bien remplie avec des flux importants d'officiers en formation du fait notamment des transformations en cours au sein de l'armée de Terre. L'EMSST a encore renforcé son ingénierie de formation pour offrir à nos officiers lauréats des parcours taillés « sur mesure ». L'EMSST maintient son investissement dans des domaines socles (capacitaire, système d'information, cybersécurité, finances, ressources humaines, langues) et a poursuivi ses « paris » dans des formations novatrices. En effet, restant fidèle à l'esprit de son fondateur le général Sabatier, l'EMSST s'est engagée résolument dans la formation d'officiers dans des domaines en pointe sur le plan technologique tels que l'IA, le quantique, la robotique ou encore les sciences cognitives afin d'offrir à l'armée de Terre les compétences dont elle aura besoin.

Pour autant, les obligations académiques du cycle 2024-2025 ne sont pas encore terminées pour nos officiers qui vont devoir continuer à pâlir sur de noirs bouquins pendant le temps de leur stage estival afin de parachever leurs mémoires de thèse professionnelle ou de préparer leurs immersions à l'étranger.

Le cycle 2025-2026 s'annonce aussi particulièrement chargé avec une nouvelle promotion de 160-170 officiers stagiaires. Les journées de rentrée se dérouleront les mardi 2, mercredi 3 et jeudi 4 septembre 2025 avec, le mardi après-midi, la tenue de la conférence inaugurale de l'EMSST sur le thème « Sciences cognitives et supériorité opérationnelle ».

Je salue et remercie nos officiers stagiaires pour l'exemplarité de leur comportement et la qualité de leurs travaux qui font honneur à l'armée de Terre et contribuent à la réflexion militaire.

**« Gérer le risque cyber : une science en devenir »**

*Par Madame Marie KRATZ, Docteur habilitée à diriger des recherches en Mathématiques appliquées*

Préambule : cet article a été rédigé sur la base de l'article « *Managing Cyber Risk, a Science in the Making* » de M. DACOROGNA and M. KRATZ publié en 2023 dans « *Scandinavian Actuarial Journal* ».

Marie KRATZ est Professeure à *l'ESSEC Business School*, directrice du CREAR (Centre de Recherche en Econo-finance et Actuariat sur le Risque) et de la filière actuariat ESSEC-Sorbonne Université. Également Actuaire Agrégée de l'Institut des Actuaires, elle préside le groupe « Risques Assuranciels, Economiques et Financiers » de la Société Française de Statistique. Ses travaux menés entre la France, Zurich, Singapour, Etats-Unis, Australie et Inde, portent entre autres, sur des risques émergents dont le risque cyber, avec une approche par la théorie des valeurs extrêmes.

**Un risque omniprésent et encore mal compris**

Rançongiciels, piratages massifs de données, interférences dans les processus démocratiques : les cyberattaques s'invitent chaque jour dans notre actualité. Le risque cyber s'impose comme l'un des grands de ce monde hyperconnecté. Contrairement aux catastrophes naturelles, dont les conséquences financières sont tangibles et mesurables, ce risque se distingue par son caractère immatériel, sa complexité et en conséquence, par la difficulté à modéliser son coût. Cette difficulté tient à plusieurs facteurs. D'abord, l'évolution fulgurante technologique devance constamment, celle de nos mesures. Ensuite, le caractère extrême et systémique : nos systèmes sont désormais interconnectés au point qu'une défaillance locale peut engendrer des conséquences globales avec des impacts financiers difficiles à estimer. Enfin, paradoxalement, bien que les systèmes informatiques génèrent désormais des volumes de données colossaux, peu d'informations sont disponibles sur les incidents eux-mêmes, souvent passés sous silence par crainte d'atteinte à l'image. Pourtant, modéliser ce risque est essentiel pour développer notre résilience et apporter des réponses efficaces, qu'elles soient assurantielles, technologiques ou sociétales.

Cet article présente l'approche probabiliste où le phénomène (risque) étudié est considéré comme aléatoire et son impact financier est modélisé par des distributions de probabilité considérées comme des « mesures » de l'aléa. Nous nous intéressons à l'évolution en cours dans ce domaine scientifique, puis présentons rapidement d'autres approches utilisées pour gérer ce risque.

**Le cyberespace : un nouveau champ de conflit**

Le terrain de jeu du risque cyber, le cyberespace, s'articule en trois dimensions indissociables : une couche physique tangible forgée par des infrastructures (câbles, serveurs, satellites), une couche logicielle comprenant systèmes d'exploitation et programmes et une couche psycho-cognitive, constituée d'images, de textes où s'entremêlent idées, émotions, croyances et perceptions.

Cette stratification reflète l'imbrication du virtuel et du réel, brouillant les frontières traditionnelles entre ces deux mondes. Une cyberattaque peut simultanément paralyser des infrastructures critiques, mais aussi manipuler l'opinion publique via les réseaux sociaux.

Cet espace est devenu un véritable théâtre d'opérations, au même titre que les domaines terrestre, maritime, ou aérien. Les grandes puissances y déploient des stratégies de jeux nouveaux, tandis que des groupes criminels organisés y prospèrent dans l'ombre. Ce basculement nous oblige à repenser fondamentalement notre approche de la sécurité, appelant à de nouvelles règles internationales et à une gouvernance repensée de cet espace commun devenu champ de bataille.

**Réinventer la modélisation de l'impact financier du risque cyber**

Dans ce contexte évolutif, les approches conventionnelles de modélisation doivent être complétées par des modèles innovants ou empruntés à d'autres domaines, tels, par exemple, l'épidémiologie pour modéliser la contagion numérique des attaques dans un réseau interconnecté.

Des modèles statistiques fondés sur l'analyse des extrêmes sont également mobilisés pour estimer les pires scénarios des cyberattaques. Ces derniers reposent sur la « théorie des valeurs extrêmes » (EVT), domaine en probabilité et statistique utilisé pour modéliser les événements rares dont les impacts sont catastrophiques. Alors que les approches statistiques classiques s'intéressent au comportement moyen (le cœur de la distribution de probabilités approché par une distribution Gaussienne), l'EVT, elle, s'intéresse aux comportements extrêmes. Elle se base sur trois types de mesures de probabilité (les lois de FRECHET, WEIBULL et GUMBEL) pour caractériser la distribution de probabilités des valeurs extrêmes (en estimant de façon asymptotique, non plus le cœur, mais les queues de la distribution de probabilités). Le statisticien caractérise ainsi le phénomène aléatoire selon un paramètre dit « paramètre de forme » qui caractérise la nature de la queue de distribution et étalonne le phénomène aléatoire par comparaison aux trois lois. On parle de « mesure de la queue de distribution de l'aléa[1] ». Ainsi donc, la nature de la queue de distribution nous permet d'estimer les probabilités d'occurrence d'événements extrêmes.

Nos recherches récentes menées sur la base de données des crimes cyber de la Gendarmerie Nationale, sur la période 2015-2019 et publiées en 2023[2], révèlent un constat frappant : les pertes financières liées aux cyberattaques présentent des "queues" statistiques au moins aussi lourdes que celles liées aux catastrophes naturelles. En termes concrets, cela signifie qu'une cyberattaque majeure pourrait provoquer un impact économique comparable à celui d'un séisme dévastateur. Pour illustrer cette réalité, nos modèles montrent que la différence entre une perte financière moyenne et celle du scénario catastrophe peut atteindre un facteur multiplicatif qui varierait entre 19 et 25. Cette analogie avec les catastrophes naturelles permet de mieux appréhender l'intensité du choc qu'une cyberattaque majeure pourrait provoquer sur les systèmes économiques et sociaux et souligne l'ampleur du défi à relever.

Un autre cadre intéressant pour l'étude des cyberattaques est celui de la théorie des jeux utilisée pour modéliser les interactions stratégiques entre attaquants et défenseurs. Dans cette perspective, chaque partie anticipe les mouvements de l'adversaire et adapte sa stratégie en conséquence. Cette approche permet de simuler des scénarios réalistes et fournit un éclairage tant sur les arbitrages pouvant être effectués en matière de sécurité que sur les points faibles d'un système de protection.

Au sein de la théorie des jeux, l'intelligence artificielle intervient dans la modélisation du risque cyber. Elle transforme radicalement la capacité des joueurs (attaquants comme défenseurs), en temps quasi réel, grâce à des algorithmes d'apprentissage automatique. Contrairement aux approches classiques qui reposent sur des règles prédéfinies, cette approche dynamique autorise les joueurs à adapter leur stratégie en fonction des schémas émergents reconnus ou de nouvelles menaces détectées. Elle ouvre ainsi la voie à une détection plus précoce et à une gestion proactive des incidents, notamment dans des environnements complexes ou en constante évolution.

**Les défis du secteur assurantiel**

Le monde de l'assurance, en quête de nouveaux relais de croissance, observe avec attention ce nouveau champ de risques. Cependant, l'assurance reste étonnamment timide pour offrir une couverture financière cyber, réticence en partie due à la difficulté de quantification des pertes, à la crainte de pertes systémiques et à l'absence de données partagées. Les PME, fortement exposées, peinent à obtenir des couvertures qu'elles jugent inadaptées, trop chères ou assorties d'exclusions importantes. Nombre d'entre elles renoncent à s'assurer, augmentant leur vulnérabilité et par extension, celle de l'écosystème économique tout entier.

Cependant, des solutions émergent : garanties modulables adaptées aux besoins spécifiques de chaque organisation, modèles probabilistes sophistiqués pour mieux évaluer l'exposition au risque et surtout, coopération étroite entre assureurs et experts en cybersécurité. Cette dernière approche s'avère particulièrement prometteuse, permettant d'ajuster la couverture en fonction des mesures de protection mises en place et d'inciter ainsi à l'adoption de bonnes pratiques.

**De la cybersécurité à la résilience**

Le terme « résilience » s'est imposé dans notre vocabulaire, parfois au point de perdre sa substance. Appliqué au domaine cyber, il mérite une définition précise. La cyber-résilience représente bien plus qu'une simple protection : c'est la capacité d'une organisation à anticiper les cybermenaces, résister aux attaques, maintenir ses fonctions vitales en période de crise et rebondir efficacement après le choc.

Ce concept ne se limite donc pas à la prévention, mais englobe aussi la réponse, la gestion de crise afin de limiter les dégâts et la capacité d'adaptation même en mode dégradé. La cyber-résilience repose ainsi sur plusieurs piliers : une gouvernance adaptée, une culture du risque partagée, une redondance des systèmes critiques, une communication de crise préparée, et des exercices réguliers de simulation d'incident.

C'est un changement de paradigme fondamental, qui implique une démarche d'amélioration continue de gestion des risques, constamment adaptée à l'évolution permanente des menaces et des technologies. Cela nécessite de former les personnes, de renforcer les partenariats avec les prestataires de cybersécurité, d'investir dans la veille technologique et de bâtir une stratégie de continuité d'activité robuste.

**Une mobilisation collective indispensable**

L'ampleur du défi cyber exige une réponse coordonnée entre les différents acteurs : chercheurs, assureurs, experts en sécurité, entreprises ou États. C'est uniquement par la mise en commun des expertises, le partage des données et la construction de cadres communs que nous pourrons apprendre à gérer ce risque complexe et dynamique.

L'expérience des dernières décennies en matière de risques naturels, industriels ou financiers montre que, malgré leur complexité, ces risques peuvent être cartographiés, mesurés, modélisés et gérés par des dispositifs adaptés. Il en ira de même pour le risque cyber, avec ses spécificités.

Domaine passionnant d'une science en devenir, c'est grâce à l'investissement coordonné dans la transparence des données et les synergies à bâtir entre les acteurs, conjugués aux travaux des scientifiques, que nous gagnerons en résilience dans le monde numérique, parfois instable et qui, désormais, façonne notre quotidien.

---

1- Pour plus de détails techniques, on pourra se référer aux chapitres des livres :

- M. KRATZ (2019). *Introduction to Extreme Value Theory. Applications to Risk Analysis & Management. In Matrix Book Series, vol. 2 - 2017 MATRIX Annals - Mathematics of Risk. E. WOOD, D. de GIER, J. PRAEGER, C.E. and Tao T. SPRINGER.*

- M. DACOROGNA and M. KRATZ (2020). *Moving from Uncertainty to Risk : The Case of Cyber Risk. In Cybersecurity, in Humanities and Social Sciences. A Research Methods Approach. Edited by* H. LOISEAU, D. VENTRE, H. ADEN. WILEY - ISTE.

2- M. DACOROGNA, N. DEBBABI, M. KRATZ (2023*). Building up cyber resilience by better grasping cyber risk via a new algorithm for modelling heavy-tailed data, European Journal of Operational Research,* 311, p. 708-729.

**« Le pot de miel et le pot de fer ; une tactique de défense dans le cyber champ de bataille »**

*Par le Chef de Bataillon Mathieu EGON, Stagiaire EMSST 2024-25, Master spécialisé Cybersécurité et Cyberdéfense à Télécom Paris*

Le cyberespace est un champ de bataille permanent. La plupart du temps l'objectif des attaquants est de pénétrer un système de défense adverse et l'objectif des défenseurs est de repérer, empêcher ou repousser ces attaques. Ce champ de bataille ressemble par bien des aspects au siège d'un fort du moyen-âge. Une des différences des cyber-forts avec leurs aïeux est la possibilité d'utiliser des « honeypots » (pots de miel).

Les types de cyber-attaques étant aussi nombreux qu'il est permis d'être inventif, nous pouvons les regrouper dans la métaphore du château-fort. Pour voler des objets ou détruire une partie du fort, l'attaquant peut chercher à passer par le pont levis en se camouflant dans le flux[1], escalader les murailles[2], attaquer en force avec un bélier[3], utiliser un espion / traitre pour ouvrir la grille[4]... Une fois que le point d'entrée est concrétisé, l'attaquant devra trouver les plans, préparer une sortie, accéder à des zones plus sensibles[5], se camoufler pour ne pas être repéré, passer à l'acte et s'exfiltrer.

Le concept du pot de miel, « *honeypot* », est de laisser une ressource délibérément vulnérable, conçue pour attirer les attaquants. Une fois entré dans le système, l'attaquant doit être attiré par ce leurre, ce qui permet de voir s'il y a un danger et, dans ce cas, de lui faire perdre du temps, lui donner de mauvaises informations à voler et de se renseigner sur lui.

Plusieurs type d'honeypots existent. De manière basique « laisser trainer » de faux documents classifiés sur un réseau et voir qui va les lire, permet de faire remonter la présence d'attaquants ou de ne rien faire du tout. Cela peut avoir un but pédagogique en interne et relever des présences non désirées. Un faux serveur permettra également de voir si un attaquant le scanne ou cherche à se connecter ; allant même, avec plus d'interaction jusqu'à recréer des simulations plus complexes et réalistes, avec des systèmes qui échangent des flux d'informations entre eux. En somme on crée un second donjon dans le château, avec des gardes et des serviteurs qui sortent et rentrent, de la musique... Le comportement des attaquants et leurs techniques sont ainsi identifiés et étudiés alors que la protection est concentrée sur le reste du réseau. Une entreprise peut également créer des honeypots de production, leurres fonctionnant comme les vraies machines. L'espoir étant qu'un attaquant s'en prenne au pot de miel le plus visible et vulnérable plutôt qu'à l'outil de production.

Analyser une attaque en cours va permettre de chercher à identifier l'attaquant : cerner ce qui l'intéresse réellement mais aussi quels outils et techniques il utilise afin de mieux spécifier nos règles de détection. Adapter nos outils défensifs à son attaque, rechercher d'autres traces de son passage dans les journaux d'évènements empêche une attaque plus large. À l'issue d'une attaque détectée, un rapport précis sur les outils et les vulnérabilités exploitées liste des recommandations pour prévenir de futures attaques similaires.

Ces *honeypots* sont donc des éléments essentiels de l'arsenal défensif. Les défis de la création d'honeypots reposent sur la difficulté d'avoir un système suffisamment réaliste pour attirer les attaquants. Par conséquent, l'arbitrage coût et bénéfice de chaque dispositif est essentiel. L'arrivée de l'intelligence artificielle pour identifier les comportements des attaquants, ajuster en temps réel le comportement du piège pour le rendre plus crédible, créer des réseaux coordonnés plus difficiles à distinguer des vrais réseaux, devrait rendre ces systèmes de plus en plus efficaces.

---

1- Ce sera du phishing par exemple, le fait d'être invité par un utilisateur qui ouvre un lien frauduleux, ou l'utilisation d'une identité falsifiée. De même la requête SQL permet de manipuler une base de données en insérant du code malveillant dans un formulaire de connexion par exemple. Si on rajoute « TOTO*OR 1=1// » dans un emplacement de mot de passe, le site attaqué lira le code : « *TOTO*OR 1=1//, choisir la condition toujours vraie 1=1* » et donnera accès au site.

2- Utilisation d'une faille 0 *day* (exploit inconnu pour le moment) existante dans un réseau ou un logiciel.

3- Attaque par force brute, ou en testant des annuaires de mots de passe comme RockMe qui comprend 1 milliard de mots de passe usuels.

4- Utilisation d'une clef USB pour ouvrir une porte dérobée (*backdoor)*.

5- Augmenter des privilèges, en se faisant passer pour un administrateur par exemple.

**« Cybersécurité des drones : l'équilibre fragile entre innovation et efficacité »**

*Par le Chef de bataillon Emanuel LE GUEN, stagiaire EMSST 2024-2025,- DT SI option cybersécurité, en mastère spécialisé cyber sécurité des opérateurs de services essentiels à Télécom Sud Paris*

Les drones, grâce à un rapport coût/efficacité favorable, sont devenus les symboles d'un nouveau visage du champ de bataille. Qu'ils soient utilisés pour le renseignement, le ciblage ou les frappes létales, ces engins volants – parfois de conception artisanale – jouent un rôle décisif aux niveaux tactique, opératif et stratégique. Mais à mesure qu'ils gagnent en autonomie, en puissance et en connectivité, une autre menace grandit : celle des attaques « cyber-électroniques » (dans le champ électromagnétique et le cyberespace). Dans ce contexte, la cybersécurité des drones peut-elle suivre le rythme de l'innovation technologique sans compromettre l'efficacité opérationnelle acquise par cette agilité qui les caractérise tant ?

Les drones modernes intègrent désormais des systèmes complexes de communication, de géolocalisation, d'intelligence artificielle et de pilotage à distance. Leur sophistication technique les rend plus efficaces mais aussi plus vulnérables. En Ukraine, plusieurs cas disponibles en sources ouvertes montrent que les liaisons radio et GPS de drones militaires ont été brouillées ou détournées par des moyens de guerre-électronique russes. Certains engins ont même été « retournés » contre leurs opérateurs, preuve d'un piratage actif des systèmes embarqués ou d'une prise de contrôle via le spectre électromagnétique. Ces opérations illustrent comment la multiplication des drones sur le champ de bataille augmente l'empreinte numérique d'une force et par conséquent sa « détectabilité » et sa surface d'attaque.

Par ailleurs, la guerre en Ukraine met en lumière une autre faiblesse : la dépendance aux composants, technologies et protocoles civils. De nombreux drones, civils comme militaires, reposent sur des circuits ou des logiciels issus du commerce grand public. Cela multiplie les risques de failles non maîtrisées, voire de portes dérobées insérées lors de la fabrication. Le segment des drones légers (inférieurs à 25kg et par essence plus produits car moins couteux) repose particulièrement sur des technologies grand public très répandues (majoritairement Wifi®, ELRS®, bandes radio *Industrial, Scientific and Medical*[1] (ISM) pour les supports de communication, MAVLink® et Occusync® pour les protocoles de commandes et de retours vidéo) avec des mécanismes de sécurité qui reposent sur des algorithmes de chiffrement symétriques maitrisés (AES, 3DES, ChaCha20). Un chiffrement robuste tel qu'il doit l'être dans le milieu militaire, repose notamment sur la capacité à gérer les clés de chiffrement dans le temps (renouvellement, révocations, autorités de certification…) et ces infrastructures de gestion à distance comme les *Public Key Infrastructure*[2] (PKI) se prêtent peu à un usage tactique réactif et discret.

Sécuriser un drone militaire ne va pas sans coût. Les protocoles de chiffrement, les pare-feux embarqués, les systèmes de détection d'intrusion sont autant d'éléments qui viendront ralentir le temps de réponse, augmenter les débits, diminuer les rayons d'action et ralentir les cadences de production. Dans un contexte de guerre où l'innovation tactique se fait à grande vitesse, les délais de certification et les contraintes techniques imposés par la cybersécurité peuvent gêner la réactivité.

Cependant, renforcer la cybersécurité de ces engins ne doit pas être envisagé comme une option, comme un choix entre faire vite ou faire bien. Si le dilemme entre déployer vite des systèmes performants mais imparfaits ou bien attendre des garanties de sécurité au risque de perdre l'initiative opérationnelle semble légitime, la réponse l'est tout autant : « les deux mon général ».

Car des pistes d'équilibre existent. L'approche dite de « *security by design* », qui consiste à intégrer la cybersécurité dès la phase de conception, gagne du terrain. Bien intégrée, elle évite l'ajout de couches logicielles ou de composants électroniques gourmands en ressources computationnelles et énergétiques. Les mécanismes de chiffrement tels que le PSK (*Pre Shared-Key*) ou l'IBE (*Identity-BasedEncryption*) sont des variantes cryptographiques plus adaptées aux systèmes fermés ou déconnectés. Malgré un coût supplémentaire, l'utilisation accrue de la fibre optique a fait également ses preuves afin de s'affranchir des contraintes électromagnétiques et de diminuer ainsi la surface numérique d'attaque.

De même, des collaborations internationales, notamment au sein de l'OTAN (STANAGs 4774 / 4778, 4586 et 4621), visent à établir des normes communes pour la cybersécurité des systèmes autonomes. Cette bataille normative qui accroît non seulement la cybersécurité mais aussi l'interopérabilité doit être menée autant sur le segment des drones militaires que sur celui des drones civils - largement dominé par le marché chinois à ce jour (DJI notamment) - mais se fait actuellement à un tempo désynchronisé du besoin opérationnel.

Ainsi, le champ de bataille numérique impose donc une double exigence : innover vite, mais sécuriser mieux. Les drones ne sont plus seulement des armes volantes : ce sont des cibles mouvantes dans un espace de guerre cyber-électronique où chaque faille technique peut valoir une défaite tactique. L'avènement des essaims de drones va rendre la problématique d'équilibre entre performance et protection d'autant plus urgente à régler. Et dans cette opposition communément établie entre réactivité et sécurité, la solution ne consiste pas forcément à faire un choix entre l'un ou l'autre à condition d'investir suffisamment tôt et de façon suffisamment déterminée le champ de la recherche et du développement.

---

1-ISM : gamme de fréquences radio réservée au niveau international pour des usages non commerciaux.

2- PKI : ensemble de technologies, de politiques et de services permettant de gérer des clés cryptographiques.

**« Par-delà les frontières de l'esprit : le billet de cyberpsychologie »**

*Par un officier stagiaire EMSST 2024-2025, Ecole des Psychologues Praticiens*

L'évolution technologique militaire, depuis les premiers chars sumériens jusqu'aux drones modernes, témoigne d'une quête constante d'amélioration des capacités humaines et tactiques. Néanmoins, les innovations récentes portent des enjeux liés à la dépendance technologique, à la vulnérabilité aux cyberattaques et à des questions éthiques et juridiques fondamentales. En effet, l'intégration de l'intelligence artificielle (IA) et de robots humanoïdes sur le champ de bataille est porteur de défis complexes. Ces machines pourraient un jour combattre au côté des soldats, voire agir de manière indépendante, ce qui soulève des interrogations profondes sur le plan moral, technique et psychologique.

Dès l'Antiquité, les mythes grecs et les automates conçus par les ingénieurs d'Alexandrie témoignaient d'une fascination pour les machines imitant la vie humaine. À la Renaissance, Léonard de Vinci s'est inspiré de ces concepts pour créer des automates mécaniques, tandis que la littérature, avec des œuvres comme « Frankenstein », exprimait déjà des craintes face au progrès scientifique. Ce roman, inspiré du mythe de Prométhée, anticipe les préoccupations modernes sur l'intelligence artificielle et la robotique.

Aujourd'hui, les avancées technologiques de sociétés telles que *Boston Dynamics*[2] ou encore *Tesla* et les promesses reposant sur son robot Optimus, tendent à brouiller la frontière entre l'homme et la machine. Aussi, la militarisation de ces robots soulèverait d'importants enjeux éthiques. Ces machines intelligentes, capables d'apprendre et d'interagir, affecteraient la perception du combat, qui pourrait devenir plus déshumanisé. La présence de robots armés autonomes sans contrôle humain direct menace le principe fondamental de réciprocité morale, posant aussi la question de la responsabilité.

L'anthropomorphisme joue un rôle crucial dans cette dynamique. A terme, les soldats pourraient ainsi percevoir les robots comme des compagnons d'armes, surtout lorsque ceux-ci affichent des comportements ou des expressions proches de l'humain, comme c'est aujourd'hui le cas avec le robot AMECA. Cette proximité peut créer un effet paradoxal appelé « vallée de l'étrange », concept développé par le roboticien japonais Masahiro MORI en 1970[3].

Au combat, le soldat est sans cesse soumis à l'incertitude et doit prendre des décisions qui ont souvent pour objet l'ouverture du feu et pour conséquence la mort d'êtres humains. Ce sont ses émotions et son instinct, dans le feu de l'action, qui lui indiquent la marche à suivre lorsque les procédures et les règlements ne donnent plus de réponse. Dans ce contexte, la fraternité d'armes est une condition essentielle de l'action collective, construisant ainsi l'esprit de corps.

Aussi, l'attachement émotionnel des soldats à leurs compagnons robots ainsi humanisés pourrait avoir des implications tactiques importantes. La perte d'un robot « frère d'armes » pourrait avoir un impact émotionnel inattendu, similaire à la perte d'un collègue humain, surtout si les interactions ont été conçues pour renforcer cette perception d'humanité. Peut-on vraiment parler de fraternité d'armes quand une des parties est une entité programmée, sans conscience, ni émotions véritables ? Devront-ils être considérés comme de simples outils, ou leur intelligence et leurs capacités émotionnelles simulées entrent-elles dans une autre catégorie ?

Pour anticiper ces transformations, la formation militaire pourrait avoir tout intérêt à évoluer en intégrant des aspects opérationnels et psychologiques liés à l'interaction homme-machine. Dit autrement, il sera vraisemblablement nécessaire de passer de la seule robotisation à une véritable cobotique[4] afin d'intégrer les interdépendances entre soldats et robots intelligents pour préserver la cohésion du groupe, la résilience des soldats et leur santé mentale.

L'évolution technologique militaire ne se limite plus à la simple amélioration des outils de combat. Elle bouleverse la nature même de la guerre, en introduisant des entités artificielles capables d'agir et de réagir de manière autonome. La relation entre l'homme et la machine aura sans nul doute à être repensée, afin de préserver les valeurs humaines dans un environnement de plus en plus technologique. La réflexion sur l'avenir de la guerre et la place des robots dans ce nouvel écosystème demeure donc une priorité pour construire un cadre adapté, sûr et éthique.

---

1- La cyberpsychologie vise la compréhension des processus psychiques qui se développent lorsque l'homme entre en interaction avec des technologies (Internet, numérique, jeux vidéo, robots, etc.).

2- Le robot-mule « Spot » a notamment pu être expérimenté par les élèves de l'Ecole Militaire Interarmes en 2021.

3- D'après ce concept, plus une entité non-humaine ressemble à un être humain, plus les petites imperfections qui la caractérise deviennent inquiétantes et génèrent un sentiment de malaise chez l'être humain. Le terme de « vallée » fait référence ici à une zone dans laquelle chaque progrès fait vers l'imitation humaine amènera, passé un certain seuil de réalisme, une acceptation plus grande.

4- La cobotique correspond à la coopération entre un homme et un robot. La robotique collaborative est une technologie qui utilise la robotique, la mécanique, l'électronique et les sciences cognitives pour assister l'homme dans ses tâches quotidiennes.

**« Légitime cyberdéfense »**

*Par le Chef d'escadron Maxime SERRES, stagiaire EMSST 2024-2025, École des Mines de Nancy, Mastère spécialisé attaque et défense des systèmes informatiques*

À l'aune de la publication de son plan stratégique[1] pour la période 2025-2027 pour une Nation cyber-résiliente, l'ANSSI (Agence Nationale de Sécurité des Systèmes d'Information) soutient que l'action publique cyber requiert une évolution dans la gouvernance et la coordination des acteurs. Attardons-nous ici sur les principaux éléments constitutifs de l'organisation de l'État en matière de cyberdéfense et sur les enjeux du secteur.

**Connaissance et anticipation**

Le pilier renseignement cyber est essentiellement armé par les membres du premier cercle du renseignement[2]. Eux-mêmes sont appuyés par des entités subordonnées de second rang comme le CRAC (Centre de Recherche et d'Analyse Cyber) pour la DRM (Direction du Renseignement Militaire) ou le CALID (Centre d'Analyse et de Lutte Informatique Défensive) pour le COMCYBER (Commandement de la cyberdéfense).

Notamment axé sur la lutte contre la cybercriminalité, un maillage territorial irrigue les régions. Il comprend en particulier le réseau des CSIRT (centre de réponse aux incidents) et des équipes spécialisées de la Gendarmerie Nationale.

Ces entités ont pour objectif d'être en mesure de caractériser et de qualifier la menace. En termes d'analyse (aussi appelée *cyber threat intelligence*) la finalité réside dans la collecte d'indices et la production de documentation, comme ce fut le cas dernièrement concernant le groupe APT28[3] (groupe russe d'acteurs malveillants).

**Besoin en coordination**

L'exigence de coordonner l'écosystème cyber national au regard de la menace en perpétuelle évolution a été pointée du doigt par un rapport d'information du Sénat[4] de 2022 sous le prisme de la Loi de Programmation Militaire (LPM) 2024-2030. En effet, les actions civilo-militaires du domaine de la cyberdéfense se sont étoffées et diversifiées ces 15 dernières années.

Le C4 (Centre de Coordination des Crises Cyber) mis en œuvre suite à une proposition décrite dans la revue stratégique de cyberdéfense[5] de 2018 est un mécanisme interministériel qui répond à cette observation. Les déclinaisons opérationnelles du C4 (dont le C4 stratégique, le C4 technique et le C4 restreint) agissent en partenariat avec l'ANSSI.

La valorisation du travail de l'ensemble des acteurs de la cyberdéfense par une fine coordination est essentielle alors que le secteur est intensément soumis à des évolutions technologiques de rupture (cryptographie post-quantique, intelligence artificielle, maîtrise de l'information...).

**Impératif de souveraineté**

Parmi les priorités, dans le contexte actuel d'une grande instabilité géopolitique, l'ANSSI identifie également la nécessité de resserrer les rangs autour des acteurs français et européens de la cybersécurité. L'agence défend une vision autonome de la sécurité et de la stabilité du cyberespace au niveau international.

Cet objectif ne pourra être atteint qu'en s'affranchissant des liens fonctionnels qui font de la France et de l'Europe des colonies numériques[6]. La forte dépendance aux produits dématérialisés extra-européens est le moteur de cette forme de colonisation dont les services d'infonuagique (ou *cloud computing*) sont d'une importance cruciale[7].

Ainsi, en tant que haut représentant reconnu de la communauté cyber au niveau national comme international, l'ANSSI se fixe pour horizon stratégique d'accroitre la résilience française dans le domaine de la sécurité informatique. L'agence, appuyée par les Armées et portée par les hautes instances républicaines, articule son action en cinq points : défendre, connaître, partager, accompagner et réguler.

Néanmoins, malgré l'effort porté sur l'orchestration des entités cyber publiques, les défis restent de taille (insatiabilité normative, numérisation à outrance, recrutement en personnel compétent) et ne pourront être relevés qu'en conservant un cap rationnel.

---

1- ANSSI 2025, Plan stratégique 2025-2027 de l'ANSSI.

2- IHEMI 2019, Organisation étatique de la gestion de crise cyber par Martial Le GUEDARD.

3- Centre gouvernemental de veille, d'alerte et de réponse 2025, Ciblage et compromission d'entités françaises au moyen du mode opératoire d'attaque APT28.

4- Présidence du Sénat, 24 mai 2023, Rapport d'information , par Olivier CADIC et Mickaël VALLET.

5- Secrétariat général de la défense et de la sécurité nationale, 18 février 2018, Revue stratégique de cyberdéfense.

6- Le GRAND CONTINENT, 7 avril 2025, Le pouvoir de dire non, Dominique de VILLEPIN.

7- Le FIGARO 25 avril 2025, Le coût colossal de la dépendance européenne au numérique américain, Jean KEDROFF.

**« Un exemple de cyber attaque par émanations électromagnétiques : attaque Echo TEMPEST avec *trojan* matériel »**

*Par un stagiaire EMSST 2024-25, Master 2 Cybersécurité Université de Rennes*

La majorité du matériel informatique employé pour traiter de sujets cyber, quel que soit le niveau de classification, est d'origine étrangère. Or l'utilisation au quotidien de matériel en provenance de pays concurrents n'est pas sans risque. L'article ci-après (s'appuyant sur les deux articles scientifiques de référence[1]) montre l'importance de contrôler minutieusement tous nos périphériques même les plus anodins pour limiter les risques de compromissions. Les lieux ne pouvant pas appliquer le zonage TEMPEST rigoureusement, comme les postes de commandement tactiques, sont une cible probable.

L'attaque TEMPEST est une forme d'attaque par canaux auxiliaires sur les appareils électroniques. Un attaquant cherchant à récupérer des informations sur une cible (e.g. un écran) va capter et interpréter les variations du champ électromagnétique produites par celle-ci pour reconstituer l'information recherchée. Cette attaque est passive, l'attaquant ne fait « qu'écouter » l'environnement électromagnétique s'appuyant sur cette faille de sécurité connue depuis le milieu du 20ème siècle. Ces émissions naturelles générées par nos appareils électroniques sont généralement confinées dans ces appareils par un blindage qui va réduire la probabilité de réussite d'une telle attaque.

L'attaque Echo TEMPEST est une forme avancée de la première version. L'approche « Echo » ajoute une dimension active à cette exploitation, en injectant des signaux spécifiques afin de provoquer des fuites, puis en analysant les échos de ces perturbations. Cette technique connue de la NSA (*National Security Agency*) depuis plusieurs années a été popularisée grâce à internet et les vidéos de Michael OSSMAN[2].

**Principe de fonctionnement**

Dans cette variante, l'attaquant aura préalablement piégé le périphérique par un cheval de Troyes (*trojan)* matériel, grâce à un dispositif inséré physiquement, dans ou à proximité, du système cible, afin de faciliter ou d'amplifier les émanations électromagnétiques mais uniquement lorsque l'attaquant le décidera.

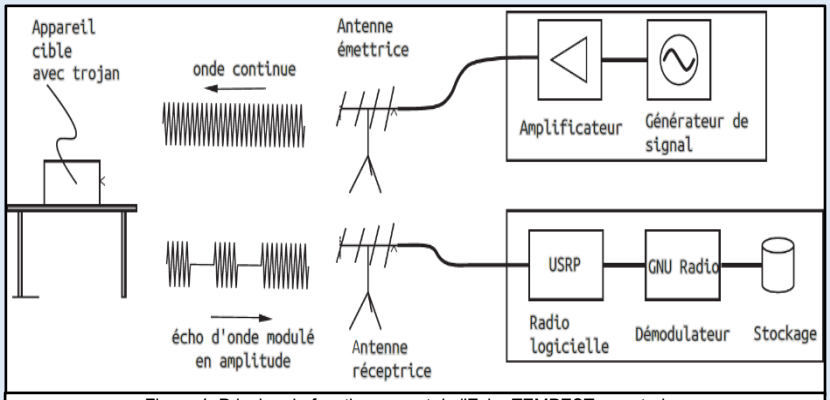



Figure 1: Principe de fonctionnement de l'Echo TEMPEST avec trojan

Ce *trojan*, souvent de taille réduite, pouvant être intégré dans un câble, un connecteur ou un circuit imprimé, a plusieurs fonctions :

- il reçoit l'onde émise ;

- il change d'état lorsqu'un signal passe sur le système piégé, ce qui en modifie l'impédance ;

- il renvoie à l'attaquant un signal modulé en amplitude selon les variations de l'impédance.

Ainsi, lorsque l'attaquant émettra une onde radio spécifique en direction de l'appareil piégé, il recevra un écho de cette onde, modulée en amplitude, en fonction des variations de l'impédance provoquée par le *trojan*.

Ces variations d'impédance sont le reflet de l'activité électrique du périphérique et donc, des informations qui y transitent.

**Cas d'application : clavier USB Low-Speed**

Les claviers USB ne sont pas la cible des attaques TEMPEST, car dans l'état actuel, ils génèrent trop peu d'émanations électromagnétiques. Cependant, lorsqu'un utilisateur tape une touche d'un clavier piégé par un *trojan* :

-Les trames USB génèrent des transitions électriques spécifiques sur les fils dédiés à la transmission des données ;

-Ces transitions modifient l'impédance du système ;

-Couplées à un signal injecté, elles créent un écho modulé en amplitude ;

-L'analyse du spectre des échos par l'attaquant lui permet de reconstituer les trames et ainsi les frappes effectuées.

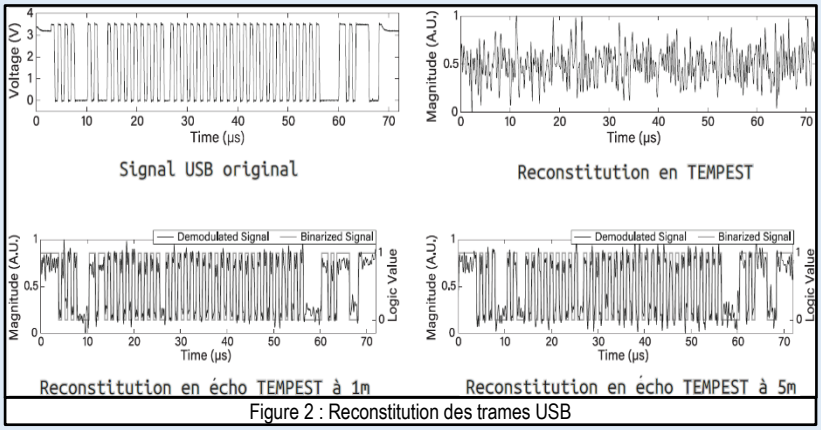



Figure 2 : Reconstitution des trames USB

Les captures de signal ci-contre (Fig.2) montrent que la capture en TEMPEST passif ne permet pas de retrouver le signal USB original. Alors qu'en Echo TEMPEST, le signal est aisément identifiable jusqu'à 5 mètres. Ensuite plus l'attaquant s'éloigne de la cible, plus l'écho sera faible, avec pour conséquence : perte d'informations et besoin de davantage de temps d'analyse pour reconstituer les informations.

Cependant, il est facile de reconstituer un texte même lorsqu'il manque une partie des lettres. Ainsi, même une attaque dans des conditions non optimales peut permettre une récolte d'informations partielle.

Dans cet exemple, l'émetteur et le récepteur sont au même endroit. Ceci oblige l'attaquant à disposer des deux dispositifs.

En revanche, bien qu'une telle attaque ne soit pas aujourd'hui prouvée, on peut envisager d'avoir une source générant l'onde incidente (un téléphone portable piraté par exemple) à proximité du périphérique piégé avec un *trojan*. Dans ce cas l'attaquant ne dispose que du récepteur ce qui le rend plus discret.

**Les points forts de la technique « Echo TEMPEST »**

- En dehors de toute stimulation électromagnétique de l'attaquant, le câble ne rayonne pas. C'est l'onde émise par l'attaquant qui sera en grande majorité réfléchie et créera l'écho. Ceci rend l'attaque plus difficilement détectable ;
- Un *trojan* disposé lors de la conception du périphérique est pratiquement imperceptible ;
- L'attaquant maitrise la distance de l'attaque en jouant sur la puissance de l'onde incidente ;
- Possibilité de capturer les émanations recherchées pour une reconstitution à posteriori ;
- Réalisable jusqu'à 5 mètres avec du matériel radio logiciel, standard et peu onéreux accessible sur le net.

**Difficultés techniques**

- Nécessité de connaître précisément le protocole cible (*timing USB*, topologie du bus) ;
- Isolation des échos utiles dans un environnement.

**Contre-mesures**

- Protection physique (cage de Faraday) ;
- Détection d'ondes radio (analyseur de spectre, capteurs dédiés) ;
- Vérification matérielle des câbles et périphériques ;
- Utilisation de protocoles USB plus récents nécessitant, de la part de l'attaquant, une capacité d'échantillonnage du signal importante pour la reconstitution.

**Conclusion**

L'Echo TEMPEST avec *trojan* matériel représente un vecteur d'attaque subtil mais redoutablement efficace. Les principes physiques exploités sont simples et nécessitent peu de compétences techniques. Ces travaux mettent en lumière l'importance de la maitrise de la *supply chain* dans les milieux traitant des informations sensibles. L'attaque vise aussi bien des périphériques USB, des périphériques vidéo (écrans), des enceintes intelligentes (pour écouter les sons captés par le micro), que des systèmes plus complexes comme un module de chiffrement. Elle combine ingénierie matérielle, traitement du signal et compréhension fine des protocoles.

Ce type de prélèvement d'information par du matériel standard et peu couteux reste limité. Mais quelles seraient les capacités d'un acteur étatique avec des moyens d'envergure nettement supérieure ? Par exemple, dans le cas du clavier USB, un tel acteur a la capacité d'entrainer des algorithmes de type *machine learning* (apprentissage automatique) pour détecter et interpréter les faibles variations de signal lorsque la distance de capture n'est pas optimale. Cela permet de générer des probabilités de contenu élaboré malgré les erreurs et pertes durant la capture.

En 2023 des chercheurs japonais ont reconstitué des trames de clavier USB en exploitant la technique de l'écho TEMPEST sans *trojan*. Leurs tests ont été réalisés en chambre anéchoïque. L'augmentation de la sensibilité des appareils de mesure, couplée à l'intelligence artificielle, permettrait la reconstitution de frappes faites sur un clavier dans un environnement électromagnétique perturbé sans avoir besoin d'insérer un *trojan*. Bien que la technique doive encore être améliorée, tout périphérique pourrait redevenir source de compromission comme lors de l'émergence de l'attaque TEMPEST et ce, quel que soit le degré de sécurité de l'approvisionnement en matériel.

---

1- 2019, *International association cryptologic research (TCHES vol.2019 n° 4) « Electromagnetic Information Extortion from Electronic Devices Using Interceptor and Its Countermeasure* » Masahiro Kinugawa, Daisuke Fujimoto and Yuichi.

- 2023, *IEEE Transactions on Electromagnetic Compatibility, IEEE, vol.65, no.3 « Echo TEMPEST : EM Information Leakage Induced by IEMI for Electronic Devices* », Shugo Kaji, Daisuke Fujimoto, Masahiro Kinugawa, Yuichi Hayashi.

2- 2014, Michael Ossmann *The NASA Playset*- YouTube.

**« Menace cybernétique : pourquoi généraliser l'analyse et la gestion des risques à tous les projets numériques ? »**

*Par leChef d'escadron Serge TARNAGDA stagiaire EMSST 2024-2025, Mastère Spécialisé en Cybersécurité et Cyberdéfense, Télécom Paris – Institut Polytechnique de Paris*

**Face à la diversité et à la complexité des formes de conflictualité actuelles, la résilience numérique s'impose comme une nécessité impérieuse**

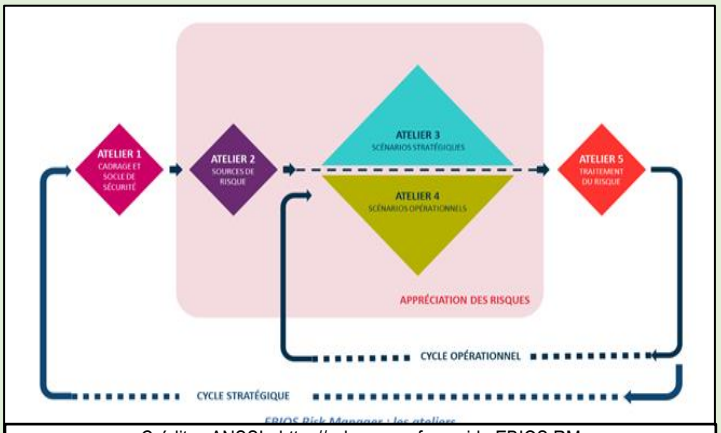
Dans les armées, la transformation numérique s'accélère, irrigant toutes les strates du combat moderne. Systèmes d'information, capteurs, objets connectés militaires, intelligence artificielle embarquée : autant d'opportunités opérationnelles, mais aussi de nouvelles surfaces d'attaque.

Pourtant, nombre de projets numériques, y compris ceux développés en interne, ne font pas toujours l'objet d'une analyse des risques. Par manque de temps, de ressources ou de sensibilisation, ces projets peuvent avoir des vulnérabilités critiques dès leur conception. Dans un contexte géopolitique dégradé, les cyberattaques récentes contre des armées et des industriels de défense mettent en lumière combien ces failles numériques peuvent, à elles seules, compromettre la supériorité opérationnelle.

**EBIOS Risk Manager : une méthode structurante, au service des opérations**

Dans ce contexte, la méthode Expression des Besoins et Identification des Objectifs de Sécurité – Risk Manager (EBIOS RM), développée par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) et vivement recommandée par le commandement de la cyberdéfense (COMCYBER), s'impose comme un cadre pragmatique, adaptable et efficace. Compatible avec les standards internationaux, telle que la norme ISO 27005[1], elle peut être mise en œuvre avec l'aide de l'outil MAITRISK disponible dans les armées. EBIOS RM propose cinq ateliers qui facilitent une analyse collaborative du risque numérique, au service de décisions éclairées et opérationnelles.

**Les 5 ateliers EBIOS RM : une dynamique au service des forces.**




Crédits : ANSSI - https//cyber.gouv.fr – guide EBIOS RM

1. Cadrage et socle de sécurité : définir le périmètre à protéger, identifier les évènements redoutés associés aux biens essentiels recensés et estimer la gravité de leur impact sur la mission.
2. Sources de risque : identifier les compétiteurs crédibles et leurs objectifs de haut niveau, en intégrant les spécificités des menaces étatiques, hybrides ou asymétriques.
3 Scénarios stratégiques : réaliser des scénarios de haut niveau qui sont autant de chemins d'attaques que pourrait emprunter une source de risque pour atteindre son objectif.
4 Scénarios opérationnels : à partir de chaque scenario stratégique, décrire des scénarios d'attaque réalistes, tenant compte des vulnérabilités exploitables et des modes d'action adverses.
5. Traitement du risque : proposer et arbitrer des mesures de sécurité adaptées aux environnements contestés, aux contraintes de mobilité et aux déploiements en coalition afin que le chef décide in fine, en connaissance de cause, si le risque résiduel est acceptable en l'état, tolérable sous contrôle ou inacceptable.

**Un levier de résilience à systématiser dans tous les projets numériques militaires**

Aujourd'hui largement employée dans les programmes d'armement ou les systèmes classifiés, EBIOS RM pourrait utilement devenir un réflexe méthodologique étendu à tous les projets numériques des forces, y compris les systèmes métiers, applications mobiles ou solutions collaboratives interconnectées.

Cette généralisation constituerait un levier structurant pour :

- ancrer une culture commune de gestion du risque numérique au sein des forces ;
- garantir la résilience de toutes les capacités numériques, quel que soit leur niveau de criticité initial ;
- passer d'une posture réactive à une posture proactive, en anticipant les attaques dès les phases de conception.

**Conclusion : EBIOS RM, un facteur de supériorité dans la guerre de l'information**

En intégrant EBIOS RM dès la phase amont de tout projet numérique, les armées renforceront leur capacité d'anticipation, de résilience et de supériorité dans les champs informationnel et cybernétique. Face à une conflictualité hybride durable et de plus en plus débridée, où l'adversaire exploite toutes les vulnérabilités, y compris les plus indirectes, cette démarche s'impose comme un impératif stratégique, puisqu'elle garantit une prise de risque mesurée, et assumée.

---

1- ISO 27005 : norme internationale fournissant des lignes directrices pour la gestion des risques liés à la sécurité de l'information.

**« Cyberdéfense et gestion de la chaîne logistique (*Supply Chain*) : synergies cruciales pour un futur résilient »**

*Par le Capitaine Sandie ROHRBACHER, stagiaire EMSST 2024-2025, master spécialisé management industriel, projets et Supply Chain, à CentraleSupélec*

Et si la prochaine défaite stratégique ne venait ni d'un code malveillant, ni d'un missile hypersonique, mais d'un composant non traçable dans une chaîne d'approvisionnement ? Cette fragilité de la chaîne logistique nécessite une protection accrue sur son intégralité. À l'heure où la guerre hybride brouille les lignes en redéfinissant les contours du conflit contemporain, l'interaction entre cyberdéfense et *Supply Chain* n'est plus un luxe intellectuel : c'est un impératif opérationnel. Plus qu'une simple synergie, cette intégration est essentielle pour renforcer la résilience de l'industrie de défense et sécuriser les opérations militaires.

**La *Supply Chain* : point d'entrée discret des menaces numériques**[1]

Dans l'imaginaire collectif, les cyberattaques sont traditionnellement perçues comme une menace ciblant des infrastructures critiques : systèmes d'armement, réseaux de commandement, ou satellites. Pourtant, la réalité des conflits modernes s'étend au-delà de ces espaces visibles, s'immisçant dans les recoins parfois négligés des chaînes d'approvisionnement. Ce vaste réseau, mêlant flux physiques, financiers et informationnels, constitue un point d'entrée facile pour des agressions numériques.

Cette vulnérabilité, accentuée par l'interdépendance croissante avec les fournisseurs, souvent internationaux, positionne la *Supply Chain* comme une cible de prédilection. Une attaque visant un sous-traitant, apparemment anodin, peut suffire à compromettre la disponibilité d'un système opérationnel critique, soulignant la nécessité d'une vigilance constante pour circonscrire les menaces potentielles. Dans ce nouveau paysage de menaces, les acteurs de la défense doivent non seulement sécuriser leurs « bastions numériques » mais aussi protéger leurs arrières logistiques, où la frontière entre civil et militaire devient de plus en plus floue.

Du côté des industriels, KNDS[3], un des leaders européens de l'armement terrestre a mis en place, dès 2021, la technologie de GATEWATCHER pour mieux se préparer et répondre aux défis de la cybersécurité dans sa chaîne d'approvisionnement, en assurant une surveillance proactive (stratégie d'anticipation visant à minimiser les risques), une protection des données, et en renforçant les compétences de ses employés.

**Coopérer entre les cultures[4] : de la cybersécurité à la cyber-résilience logistique**

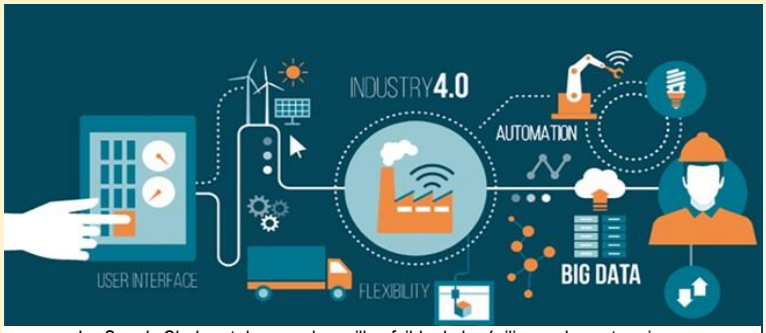
L'intégration de la cyberdéfense et de la gestion de la *Supply Chain* ne se limite pas à la mise en place de protocoles techniques, mais nécessite une transformation organisationnelle et cognitive radicale. Les acteurs de la défense doivent commencer à considérer la *Supply Chain* non plus comme une fonction de support, mais comme une infrastructure stratégique, soumise à des menaces asymétriques. Pour ce faire, il est crucial de décloisonner les cultures professionnelles.

Le défi[5] réside dans la capacité à faire dialoguer des domaines qui traditionnellement ne se parlent guère : le vocabulaire de la cyberdéfense, centré sur le code et les vulnérabilités, doit rencontrer le langage logisticien, composé de délais et flux. Favoriser des échanges, organiser des exercices conjoints de cybercrise entre logisticiens et experts en cybersécurité, élaborer des cartographies des dépendances et fragilités critiques, sont autant d'initiatives nécessaires pour bâtir une culture commune de la résilience.

Il s'agit donc de tirer parti des expertises variées pour accueillir une vision collective, essentielle à la préparation face aux cyberattaques avec les outils modernes : apporter une vraie connaissance cyber aux logisticiens afin de se protéger efficacement d'attaques pernicieuses, ou à défaut de les contourner.

**La dimension humaine : construire une résilience collective**

Au-delà des enjeux techniques, l'élément humain est au cœur de cette synergie entre cyberdéfense et gestion de la *SupplyChain*. L'intégration de la cybersécurité dans le quotidien des équipes est primordiale : une communication fluide, des formations et la sensibilisation aux hypothèses de menace, sont indispensables.




La *Supply Chain* est devenue le maillon faible de la résilience des entreprises.
Source ; ITSocial

Les partenaires externes, tels que les fournisseurs et sous-traitants, doivent également être intégrés dans cette démarche collaborative, avec des normes de cybersécurité établies dans les contrats.

Cette approche collective ne se limite pas à une seule entreprise ou technologie, mais tisse un réseau de confiance indispensable pour renforcer la résilience face aux cyberattaques. En unissant leurs efforts, tous les acteurs de cette chaîne peuvent se préparer à un environnement incertain ce qui est d'autant plus vital à une époque où le moindre retard de livraison peut avoir de lourdes conséquences.

Dans un monde où les flux logistiques sont aussi stratégiques que les feux, la cyberdéfense doit s'intégrer dans la réflexion logistique (démarche pro-active avec l'évolution des flux d'information et de marchandises). La *Supply Chain* doit être considérée non seulement comme une ligne d'approvisionnement mais comme une ligne d'affrontement. En adoptant cette approche novatrice, les parties prenantes du secteur de la Défense pourront se positionner en acteurs de pointe face aux défis du futur. Organiser la résilience de la logistique, c'est gagner en autonomie, en crédibilité et en capacité à durer dans un conflit où l'attaque commencera peut-être par un « simple » retard de livraison de munitions.

---

1- Cf. campus cyber : fiche pratique « Prévenir les risques cyber d'une supply chain", 5 décembre 2023.

2- Rapport de l'Organisation du Traité de l'Atlantique Nord (OTAN) sur la cyberdéfense et les nouvelles menaces.

3- KNDS, (Association entre Krauss-Maffei Wegmann et Nexter), témoigne sur GATEWATCHER.

4- Dans le sens de faire se comprendre dans leurs champs de domaine respectifs les « logisticiens » et « administrateurs cyber ».

5- Blogs de cyberdéfense et de gestion de la chaîne d'approvisionnement qui abordent les tendances et défis actuels. CSO Online, SupplyChain247.

**« L'internet du futur sera peut-être quantique »**

*Par le Commandant Léna MERCADER, Stagiaire EMSST 2024-2025- DT SI technologies quantiques, Master informatique quantique, Sorbonne Université*

Les technologies quantiques fascinent autant qu'elles intriguent, tant sur leurs fondements qui semblent s'opposer au monde classique que, sur la réalité de leurs applications. Pourtant, l'étude du quantique, c'est-à-dire l'étude des propriétés de la matière aux niveaux atomique et subatomique, pourrait révolutionner les réseaux de communication.

Depuis quelques années, plusieurs laboratoires de recherche[1] s'intéressent à la manière dont la physique quantique peut améliorer la transmission d'information, en s'appuyant sur des satellites avec des technologies quantiques embarquées. Si ces études sont encore essentiellement théoriques, elles permettent d'anticiper les futurs modes de communication, notamment pour échanger des données sécurisées.

La communication quantique consiste à transmettre des données entre deux points éloignés, conventionnellement appelés Alice et Bob, en utilisant des technologies quantiques. Contrairement aux bits classiques, les particules ou bits quantiques (qubits) se transmettent mieux à travers l'air libre que par fibre optique[2]. Les protocoles de communication quantique sont donc étudiés en exploitant un satellite afin de couvrir des distances utiles.

Et l'un des scénarios les plus simples représente une transmission de données entre Alice et Bob, avec uniquement un satellite entre eux.

Parmi les principales propriétés quantiques[3], l'intrication représente une source importante de preuve de l'avantage quantique par rapport au classique et est donc le point de départ des travaux sur la communication. L'intrication correspond à l'établissement d'un lien entre deux qubits, quelle que soit la distance qui les sépare : on parle alors d'état (global) intriqué. Puisque cette intrication est quantifiable, dans le sens où il existe des états fortement ou faiblement intriqués, il est donc possible de mesurer l'efficacité d'un système de communication qui utilise les technologies quantiques. En particulier, ce système de mesure de l'intrication peut être intégré au sein du satellite avec le protocole suivant :

➔Alice et Bob envoient chacun un qubit vers le satellite ;

➔le système quantique intégré au satellite mesure le degré d'intrication entre les deux qubits reçus :

- si l'intrication est maximale, alors le satellite informe Alice et Bob du succès de la communication, par un signal classique ;
- dans le cas contraire, Alice et Bob envoient un nouveau qubit[4].

Ce type de protocole peut déjà être simulé sur des ordinateurs classiques, permettant d'en analyser les propriétés fondamentales. Cependant, en raison d'hypothèses simplificatrices comme l'absence de perturbations atmosphériques, ces simulations ne représentent pas encore toute la complexité des conditions réelles.

Ainsi, ces travaux préliminaires pourraient structurer les bases d'un internet quantique, à l'instar de l'informatique ou de l'intelligence artificielle, dont les développements actuels ont nécessité des décennies de recherche. Dans un premier temps, ces technologies pourraient servir à des communications ultra-sécurisées. Cependant, l'histoire des sciences montre que les innovations, une fois largement diffusées, suivent souvent des trajectoires imprévues. Il est probable que les technologies quantiques ne fassent pas exception à cette règle.

---

1- Dont les laboratoires de KeioUniversity (Japon) et de Sorbonne Université.

2- Une autre différence intéressante réside dans le fait que la perte des qubits lors de la communication ne peut pas être compensée par une saturation du nombre de données transmises.

3- Les principales propriétés quantiques sont la superposition des états, la dualité onde-corpuscule de la lumière, l'intrication et l'effet tunnel.

4- Ce protocole se distingue de celui des distributions quantiques de clés de chiffrement. Dans ce dernier cas, le satellite joue souvent le rôle d'une source qui envoie des qubits individuellement vers Alice et vers Bob ; la transmission est donc descendante.

**« Éloge des CORSIC »**

*Par le Lieutenant-colonel Rémy SOUVESTRE, stagiaire EMSST 2024-2025, Institut national du service Public*

La numérisation a fait de la cyber sécurité un sujet majeur de souveraineté et de sécurité, dans le domaine de la défense, mais aussi dans la mise en œuvre des politiques publiques comme dans le quotidien de nos concitoyens. A la fois enjeux et défenseurs, les administrateurs réseau – le CORSIC de nos régiments – constituent le maillon tactique essentiel de la sécurité des systèmes d'information.

L'attaque d'envergure déclenchée contre le Groupe Hospitalier Grand Ouest en octobre 2024[1], résultat d'une compromission interne ayant pour origine un ancien responsable de la sécurité des systèmes d'information (RSSI) du groupe, illustre à la fois la nécessité, la vulnérabilité et la criticité de cette ressource placée au cœur des systèmes.

La théorie d'O-ring issue du destin tragique de la navette Challenger illustre parfaitement l'adage faisant de la cybersécurité « l'affaire de tous[2] ». Pour autant, les missions de l'administrateur réseau vont bien au-delà des tâches essentielles de formation et de sensibilisation des utilisateurs aux plus bas échelons. La connaissance fine des réseaux et logiciels permet la surveillance des systèmes et de fait une détection précoce des anomalies ou activités suspectes.

La numérisation continue accroît naturellement la charge de travail et les responsabilités pesant sur les épaules de ces experts dont le nombre est compté et les compétences très recherchées. La question des ressources humaines (RH) se pose ainsi avec acuité, en termes de rétention et de compétitivité par rapport au secteur civil privé, mais également en termes de densité dans les écosystèmes concernés, au quartier comme en opérations.

La gouvernance de la cyber sécurité est mature et clairement établie au niveau national[3]. Pour les niveaux stratégique et opératif, la création du COMCYBER (commandement de la cyberdéfense) par décret en 2017 et l'offre de recrutement/formation mise en place par les armées – telle que le BTS CIEL (cybersécurité, informatique et réseaux, électronique) proposé au sein du lycée militaire de Saint-Cyr - traduisent la prise en compte de la problématique dans ses dimensions doctrinales, opérationnelles et RH, sans pour autant consacrer l'importance de l'administrateur réseau aux plus bas échelons.

A l'échelle tactique, régiment et brigade notamment, le positionnement des administrateurs réseau pourrait être rehaussé afin de constituer un bureau dédié, à l'instar du bureau maintenance et logistique, et placé au plus près du commandement. Souvent constitué d'une seule personne, généralement un jeune sous-officier, cette capacité manque de résilience et d'épaisseur humaine, malgré une importance croissante de par le nombre de logiciels gérés comme de par la transversalité des domaines concernés : communication/information, budget, tactique, transmissions, réseau « du quotidien » notamment.

Cette augmentation est de nature à redonner de la liberté d'action aux chefs de corps en matière d'innovation tout en assurant les conditions matérielles et immatérielles du commandement par intention[4].

En effet, l'administrateur réseau met en œuvre la stratégie de sécurité décidée par le commandement, dans une architecture qui se veut agile et décentralisée[5].

Au-delà de la réduction des risques d'exploitation de vulnérabilités connues par la sensibilisation, contre le *phishing* notamment, et la tenue à jour de l'environnement logiciel, les administrateurs réseau doivent être capables de proposer une stratégie de sécurité en phase avec la stratégie et les manœuvres du régiment, au même titre que dans une entreprise privée[6]. Ceci implique de disposer des moyens humains nécessaires à la manœuvre dans la première brique de l'écosystème cybernétique, enjeu de combat au même titre que les plateformes de combat ou les moyens logistiques.

---

1- Radio France, article du 23/12/2024 "Ille-et-Vilaine : un ancien responsable de la sécurité informatique arrêté après une cyberattaque de plusieurs établissements de santé "

2- Agathe CAGE, Manager la cybersécurité : un enjeu stratégique prioritaire, revue Servir n°515, Juin-Juillet 2022.

3- Sophie AGULHON, La gouvernance de la cybersécurité française : un panorama des acteurs, RDN n° 873, octobre 2024.

4- Le commandement par intention (CPI) est un concept forgé par le CEMAT et constitue la pierre angulaire du commandement voulu pour l'Armée de Terre de Combat (2025).

5- Le concept de décentralisation s'entend ici au sens tactique et non administratif (on utiliserait le cas échéant le terme déconcentré).

6- Quentin GAUMER, « Cybersécurité dans un contexte d'intelligence économique », I2D - Information, données & documents, N°3, 2017.

**« Rendre les Honneurs »**

*Par le Colonel (H) André MAZEL*

Rendre les Honneurs à une personnalité de haut rang est un honneur, mais les préparatifs sont parfois une corvée.

J'étais en ce temps-là affecté à un groupe d'artillerie nucléaire *Honest John*, fer de lance des Forces françaises en Allemagne.

La garnison était située dans cette région paradisiaque que les Allemands surnomment « *Unsere Kôte d'Assur* ». Nous avions le ski en Allemagne, Autriche ou Suisse à une heure de voiture ; et les eaux du lac de Constance dont les vaguelettes léchaient nos rangers ! Ah si le temps avait pu suspendre son vol et ces heures propices suspendre enfin leur cours !

En contrepoint de ces délices nous avions 36 heures de manœuvres par semaine en terrain civil afin d'être prêts à foncer vers la Tchécoslovaquie pour vitrifier si nécessaire des Forces du Pacte de Varsovie envahissantes.

Un jour nous avons été prévenus que le Général MASSU, commandant en chef les forces françaises en Allemagne, devait venir nous inspecter. Non pas le lendemain ou deux jours plus tard, mais dans un mois.

Désigné, avec ma batterie, pour rendre les Honneurs, les répétitions ont aussitôt commencé, conformément aux recommandations strictes que comportait l'alerte, qui furent largement complétées par des détails qu'apportaient un ou deux officiers supérieurs[1] débarquant bi-quotidiennement du quartier général situé à Baden-Baden.

Et des détails il y en a eu ! Sur l'ordre serré qui nous faisait arpenter le quartier de long en large ou sur les ceinturons qui devaient être tous de la même couleur. Les stocks régimentaires ne le permettant pas il fallut faire appel à l'esprit de camaraderie du régiment d'infanterie partageant notre quartier.

Et puis il fallait chanter en défilant devant l'Autorité. Mais aussi être capables de s'arrêter tout en continuant à chanter. Chanter, oui mais quoi ? Les chants virils de la Wehrmacht ou de la Légion n'étaient pas bien vus. Oublier aussi le « Maréchal, nous voilà devant toi, le sauveur de la France… » que j'avais appris à l'école primaire pour une exceptionnelle visite en 1942.

Finalement est choisi l'air d'une marche, connu de tous, sur lequel je vais écrire des paroles de circonstance (on ne se refait pas). Je ne les déposerai pas à la SACEM. Elles ne m'auraient d'ailleurs rien rapporté n'ayant jamais été chantées en public.

Tout cela commence à ressembler à du cirque. Devra-t-on aussi défiler en passant sous un arc enflammé ? Le dernier pinailleur n'en a pas ajouté et a déclaré que nous étions fin prêts.

Le grand jour arrive enfin, mais est noyé dans une bruine très fine persistante.

Levés tôt nous sommes briqués de pied en cap comme des sous neufs. Le général en chef, débarqué à la gare de Radolfzell, fait dire qu'il ne voudrait pas que les soldats se mouillassent et qu'il se contentera d'Honneurs rendus, à l'abri du porche d'entrée du quartier, par un maréchal des logis et douze hommes.

Les canonniers allant rendre leur armement sont furieux qu'on les prenne pour des mauviettes.

La visite se terminera par un speech du général aux cadres, dans la salle d'Honneur. Speech dont j'ai retenu qu'il souhaitait que nous apprenions l'allemand pour mieux fraterniser avec la population locale.

En lui rapportant ces propos j'expliquais à mon épouse que pour ce faire la méthode de l'oreiller était bien supérieure à celles des éditions Assimil et de l'Institut Goethe réunis. Sans s'émouvoir elle en convint et me donna son accord à condition de voir la note de service signée MASSU…

Le généralissime oublia de nous la faire parvenir ! Et « *chez bour sa ke che ne barle pas la lank de Keute !* »

Je laisse au génie de Shakespeare le soin de conclure cette histoire : « *Much Ado About Nothing* » ou dans la langue de Molière : « beaucoup de bruit pour rien ».

---

1- Le lecteur assidu doit se souvenir de l'histoire des deux lions, publiée dans la Lettre de Minerve n° 57 (mars 2023). Outre la mise en alexandrins, je n'avais en fait, en la situant à l'École militaire, qu'actualisé cette plaisanterie qui courait déjà les garnisons à cette époque à propos du quartier général de Baden-Baden.

**« Rejoins-nous, lecteur »**

*Par le Colonel (H) André MAZEL*

À moi, lecteur, deux mots ! Connais-tu bien Minerve,
L'Association d'anciens de l'EMSST ?
Que tu sois maintenant d'active ou de réserve,
Toi qui as décroché un titre convoité,

Tu devrais, aujourd'hui, regarder en arrière.
Après avoir trimé au sein de cette École,
École qui t'aida, quand tu étais stagiaire,
À marquer ta carrière du label « Pont d'Arcole »,

Tu devrais adhérer pour revoir des amis
Que tu as dû connaitre dans une académie.
Le site de Minerve fournit un formulaire
Tu l'emplis et l'envoies ; c'est fait en un éclair.

Rejoins l'Association, retrouve ces élites,
Où tu seras, bien sûr, aussitôt reconnu
À la fois par ton rang et aussi tes mérites
Et qui te souhaiteront heureuse bienvenue

**« Déjeuner Minerve du printemps »**

Minerve a organisé son repas de printemps le 13 mars dans un restaurant de spécialités chinoises, à proximité de l'Ecole militaire. Autour de son Président, ce déjeuner a réuni plus d'une vingtaine de membres, dont certains en activité, dans une ambiance sympathique.

Minerve rappelle qu'elle organise deux repas par an – au printemps et à l'automne – dont la date est indiquée par envoi d'un mail à tous les membres franciliens ainsi que par un affichage sur le site de l'association. Tout adhérent qui souhaite y participer est le bienvenu.

**Carnet gris**

Minerve a appris avec tristesse le décès de Marie-Odile, épouse de notre adhérent le Colonel GRUÉ.

**Minerve présente au Colonel ses plus sincères condoléances.**