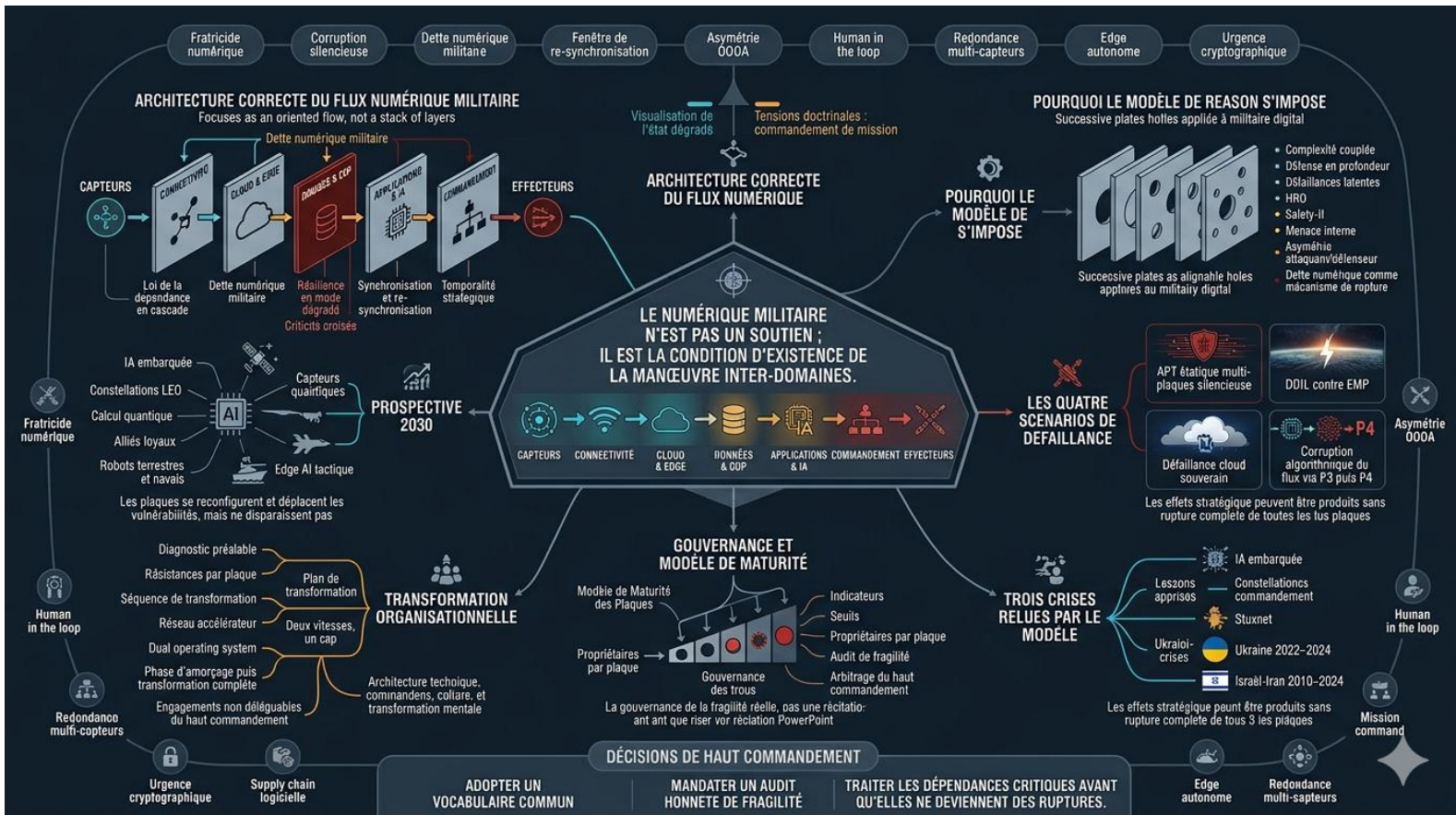


Architecture, Flux et Résilience de l'Écosystème Numérique Militaire : Architecture, flux et résilience décentralisée

Application du Modèle des Plaques de Reason — Flux orienté, dette numérique militaire et prospective 2030



POUR LE LECTEUR PRESSÉ

Ce document en 5 minutes — sans jargon technique

01 LE PROBLÈME EN UNE PHRASE

Nos armées savent très bien décrire ce qu'elles veulent faire avec le numérique. Elles décrivent mal comment ce numérique est réellement construit — et donc mal où il peut casser. Ce document propose un modèle pour corriger cette erreur.

02 IMAGINEZ UNE CHAÎNE DE 5 MAILLONS

Tout ce que le numérique militaire accomplit passe par une seule chaîne, dans l'ordre, de gauche à droite :

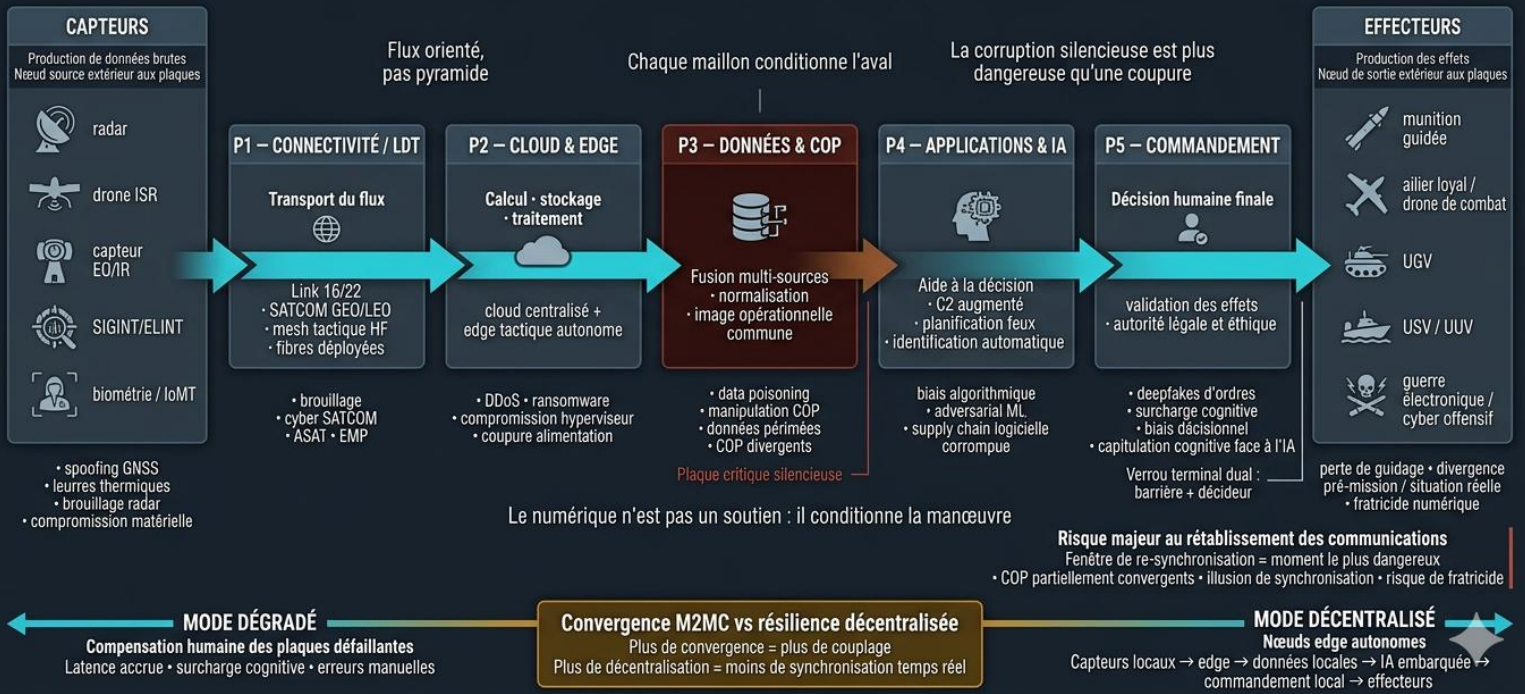


Cette chaîne a une propriété implacable : si n'importe quel maillon casse, tout ce qui est à droite devient aveugle ou inutile. Un adversaire intelligent ne cherche pas à tout détruire — il cherche à casser le bon maillon au bon moment. Et souvent, il n'a besoin d'en fragiliser que deux ou trois pour produire un effet de niveau stratégique.

Section I — Architecture du Flux Numérique Militaire

ARCHITECTURE DU FLUX NUMÉRIQUE MILITAIRE

Flux orienté • cinq plaques internes • résilience décentralisée



03 LA LEÇON DE L'AVIATION

Le Pr James Reason a étudié pendant des décennies pourquoi les avions s'écrasent. Sa conclusion : les catastrophes ne surviennent pas d'un coup, par une seule erreur. Elles surviennent quand plusieurs petites faiblesses — qui coexistaient silencieusement depuis des mois — s'alignent au même moment, comme des trous dans des plaques de fromage qu'on empile. L'aviation a utilisé ce modèle pour diviser par vingt son taux d'accidents mortels en trente ans. Dans ce document, nous appelons « plaques » ces cinq maillons — directement inspiré de l'image du fromage de Reason — parce qu'ils fonctionnent de la même façon : chacun a ses propres trous cachés, et c'est leur alignement simultané qui produit la catastrophe.

Ce document applique exactement le même raisonnement à nos systèmes numériques militaires. Nos cinq maillons sont cinq plaques. Chacune a des faiblesses cachées que personne ne mesure réellement. Un adversaire patient attend que les trous s'alignent — ou les aligne lui-même.

04 CINQ VÉRITÉS QUI DÉRANGENT

La corruption silencieuse est plus dangereuse qu'une coupure. Si notre image opérationnelle commune — la carte numérique partagée par tous les états-majors — est empoisonnée par de fausses données, tous nos systèmes continuent de fonctionner parfaitement. Sur de fausses informations. Aucune alarme ne sonne. Nos soldats peuvent tirer sur les mauvaises cibles — c'est ce qu'on appelle le fratricide numérique.

Notre fragilité s'accumule sans que personne ne la voit. Chaque équipement non mis à jour, chaque procédure non exercée, chaque redondance non construite s'accumule silencieusement. Comme aucun incident n'est survenu, on croit le système solide. Mais l'absence d'incident ne prouve pas la solidité — elle prouve seulement que l'adversaire n'a pas encore trouvé le bon alignement. Un jour, il le trouvera.

Une coupure et une destruction physique ne se traitent pas pareil. Une coupure des communications (brouillage, cyberattaque) est fonctionnelle et réversible en quelques heures. Une destruction physique par impulsion électromagnétique est irréversible — il faut remplacer le matériel. Les confondre dans un seul plan de défense est une erreur grave.

Quand les communications tombent, le danger ne disparaît pas — il change de forme. Les unités qui opèrent en autonomie sur des données locales peuvent prendre des décisions incompatibles avec leurs voisins. Au moment où les communications reviennent, le moment le plus dangereux commence : une partie des unités est resynchronisée, d'autres pas encore. Sans protocole précis, c'est là que les accidents se produisent.

L'IA ne remplace pas le jugement — elle l'amplifie, dans le bon sens comme dans le mauvais. Une intelligence artificielle nourrie de données fiables accélère la décision. La même IA nourrie de données falsifiées accélère les mauvaises décisions — avec une confiance algorithmique qui inhibe le questionnement humain. C'est pourquoi un humain doit toujours rester dans la boucle, et pourquoi les officiers doivent régulièrement commander sans aucun appui numérique pour ne pas perdre ce réflexe.

05 QUATRE INCIDENTS QUI ILLUSTRONT CES VÉRITÉS

Ukraine, 24 février 2022, 4 heures du matin. La Russie coupe en une heure les communications satellitaires ukrainiennes, isolant les unités dès les premières heures de l'invasion. Leçon : une seule voie de communication est une vulnérabilité stratégique. L'Ukraine s'en est remise parce qu'elle avait entraîné ses unités à opérer en autonomie.

Stuxnet, Iran, 2010. Des centrifugeuses nucléaires iraniennes ont été détruites par un virus informatique — sans qu'une seule bombe soit lâchée. Le virus a attaqué simultanément deux maillons de la chaîne. Il a suffi de deux maillons sur cinq pour produire un effet militaire de niveau stratégique.

SolarWinds, États-Unis, 2020. Un logiciel livré par un fournisseur de confiance contenait déjà un accès caché. Le danger n'a pas été introduit par une attaque extérieure — il a été livré avec le produit. Neuf mois d'exploitation silencieuse sans aucune alarme. Leçon : la sécurité de notre numérique dépend aussi de nos fournisseurs.

Ukraine 2022–2024, dans la durée. Le premier grand théâtre où le numérique militaire a été testé à grande échelle et sous haute intensité. La résilience ukrainienne n'était pas seulement technologique — elle était doctrinale et humaine : entraînement au commandement sans numérique, redondance des communications, habitude de décider vite avec des données incomplètes.

06 CE QU'ON VOUS DEMANDE — TROIS DÉCISIONS

D1

Adopter un vocabulaire commun. Les cinq maillons de la chaîne deviennent le référentiel partagé de tous les briefings et plans de résilience. Sans vocabulaire commun, chaque bureau ne voit que son bout de chaîne — et personne ne voit l'alignement des faiblesses.

D2

Mandater un audit de fragilité honnête. Chaque maillon évalué objectivement : où en sommes-nous réellement ? Horizon 6 mois. Sans cet inventaire, tout plan de résilience est bâti sur des hypothèses — pas sur des faits.

D3

Traiter le problème de chiffrement avant 2027. Nos adversaires enregistrent aujourd'hui nos communications chiffrées pour les déchiffrer demain, quand ils auront les ordinateurs quantiques nécessaires. Ce danger est invisible maintenant — mais chaque mois de retard aggrave définitivement notre exposition. C'est la définition d'une urgence sans alarme visible.

⚠ La question finale de ce document s'adresse directement au haut commandement — elle mérite une réponse avant la prochaine revue de capacités numériques.

→ **Le document complet suit.** Les sections I à VII développent chaque point avec les fondements doctrinaux, les crises historiques analysées, les outils de gouvernance et la stratégie de transformation — avec toutes les sources.

SOMMAIRE

Sommaire.....	5
Résumé Exécutif.....	7
Section I — Architecture du Flux Numérique Militaire.....	8
1.1 Le flux orienté : correction d'une erreur d'architecture répandue.....	8
1.2 La dette numérique militaire : le risque invisible du haut commandement....	12
1.3 Les capteurs : vulnérabilités d'entrée et stratégie de robustesse.....	13
1.4 Les effecteurs : autonomie croissante et responsabilité déplacée dans le temps	14
1.5 Résilience opérationnelle : mode dégradé, mode décentralisé et tension M2MC	16
1.6 Le chemin critique et la cartographie des cinq plaques	17
1.7 Le problème de la synchronisation : coordonner l'action décentralisée	19
1.8 La temporalité comme variable stratégique indépendante	21
1.9 Matrice de criticité croisée : l'adversaire n'a pas besoin des cinq plaques.....	22
Section II — Pourquoi le Modèle de Reason s'impose	25
2.1 Trois propriétés de l'écosystème qui rendent Reason incontournable	25
2.2 La menace interne : le trou que l'adversaire n'a pas besoin de créer.....	25
2.3 Précédents sectoriels et limites du modèle.....	26
2.4 Du modèle de Reason aux HRO : vers une résilience active	28
2.5 La dette numérique : du fil rouge au mécanisme de rupture.....	30
2.5.1 Taxonomie des sources : comment la dette se crée	30
2.5.2 Comment se résorbe-t-elle : séquence priorisée par plaque	31
2.5.3 Le mécanisme de basculement : de la dette latente à la rupture critique	32
Section III — Les Quatre Scénarios de Défaillance	34
3.1 APT étatique : la pénétration multi-plaques silencieuse.....	34
3.2 DDIL et EMP : deux ruptures de P1 aux mitigations fondamentalement distinctes.....	35
3.3 Défaillance cloud souverain : P2 effondrée, P1 intacte.....	36
3.4 Corruption algorithmique : le poison silencieux dans P3 qui traverse P4	37
Section IV — Trois Crises Relues par le Modèle de Reason	38

4.1 Stuxnet (2010) : anatomie d'un alignement parfait	38
4.2 Ukraine (2022–2024) : le premier théâtre de résilience numérique en haute intensité	40
4.3 Israël-Iran (2010–2024) : la guerre permanente des plaques.....	41
Section V — Gouvernance et Modèle de Maturité des Plaques.....	43
5.1 Le Modèle de Maturité des Plaques (MMP)	43
5.2 Indicateurs, seuils et propriétaires — la gouvernance des trous	44
Section VI — Transformer l'organisation : une stratégie en trois lentilles	46
6.1 Le diagnostic préalable : nommer ce qui bloque vraiment.....	46
6.2 Les trois lentilles : voir l'organisation telle qu'elle est	46
6.3 Profil de résistance de chaque plaque.....	48
6.4 Les trois lentilles en action : la séquence de Kotter comme illustration opérationnelle.....	48
6.5 Le Dual Operating System : deux vitesses, un cap	50
6.6 Calibrage réaliste : phase d'amorçage vs transformation complète	51
6.7 Les trois engagements non déléguables du haut commandement	51
Section VII — Prospective 2030 : Reconfiguration de la Carte des Plaques.....	53
7.1 IA embarquée : P4 épaissie, nouveau trou P3 de péremption	53
7.2 Constellations LEO : P1 épaissie, surface d'attaque déplacée vers l'espace	53
7.3 Calcul quantique : bombe à retardement dans P1	54
7.4 Capteurs quantiques : fermeture architecturale du trou GNSS.....	54
7.5 Ailiers loyaux et robots : autonomie locale et nouvelles questions doctrinales	54
Conclusion — La Supériorité Numérique comme Obligation Stratégique Non Déléguable.....	56
Annexe — Glossaire des acronymes	57

RESUME EXECUTIF

Thèse centrale : le numérique n'est pas le soutien de la manœuvre M2MC — il en est la condition d'existence. La rupture d'un maillon du flux numérique ne dégrade pas la manœuvre inter-domaines : elle l'annule. Ce document cartographie ce flux, nomme ses vulnérabilités avec précision, et propose un cadre de gouvernance actionnable pour le haut commandement — sans illusion sur les difficultés, sans indulgence sur les angles morts.

Ces réflexions partent d'un constat dérangeant : la plupart des doctrines numériques militaires décrivent correctement leurs ambitions et incorrectement leurs architectures. Elles traitent capteurs et effecteurs comme des couches du système numérique — alors qu'ils en sont les nœuds périphériques d'entrée et de sortie. Elles évoquent la résilience comme un objectif sans en cartographier les mécanismes de défaillance. Et elles sous-estiment systématiquement ce que nous appellerons ici la dette numérique militaire : l'accumulation silencieuse de vulnérabilités latentes dans les plaques numériques qui soutiennent l'ensemble des capacités opérationnelles.

Le document s'articule en sept sections. La Section I établit l'architecture correcte du flux numérique militaire — flux orienté, non pyramide de plaques — avec ses nœuds périphériques (capteurs, effecteurs) et ses cinq plaques internes (connectivité, cloud/edge, données, applications/IA, commandement). La Section II démontre la pertinence du modèle de Reason, le complète par les HRO et Safety-II (§2.4), et formalise le mécanisme de basculement de la dette numérique (§2.5). La Section III analyse quatre scénarios de défaillance, distinguant notamment les ruptures fonctionnelles (DDIL) des destructions physiques (EMP). La Section IV relit trois cas historiques sous l'angle des plaques : Stuxnet, Ukraine, Israël-Iran. La Section V propose un Modèle de Maturité des Plaques actionnable. La Section VI traite la conduite du changement avec une franchise inhabituelle sur les résistances institutionnelles. La Section VII anticipe la reconfiguration des plaques à l'horizon 2030.

SECTION I — ARCHITECTURE DU FLUX NUMÉRIQUE MILITAIRE

1.1 Le flux orienté : correction d'une erreur d'architecture répandue

L'écosystème numérique militaire — formalisé en France par la doctrine M2MC¹ et par le concept américain de Multi-Domain Operations² — est un système de traitement de l'information dont la topologie correcte est celle d'un *flux orienté*, non d'une pile de couches homogènes. Cette distinction n'est pas sémantique : elle conditionne toute l'analyse des vulnérabilités et toute la stratégie de résilience.

À une extrémité du flux, des nœuds source produisent des données brutes sur l'environnement opérationnel : ce sont les capteurs. À l'autre extrémité, des nœuds de sortie reçoivent des ordres d'engagement et produisent des effets cinétiques ou non-cinétiques : ce sont les effecteurs. Entre les deux, quatre plaques numériques successives transforment, transportent, stockent et interprètent le flux — avant que le commandement humain ne prenne la décision finale.

⚠ CLEF DE LECTURE — LA LOI DE LA DÉPENDANCE EN CASCADE

Chaque maillon du flux conditionne tous les maillons en aval. Cette dépendance est orientée et non réversible à court terme. Un capteur de première qualité ne sert à rien si la LDT ne transporte pas ses données. Une IA parfaite produit des recommandations erronées si les données qu'elle reçoit sont corrompues. Un effecteur guidé de précision devient une arme aveugle si la chaîne qui le désigne est rompue. Nuance essentielle : cette dépendance en cascade s'applique à pleine intensité sur le flux nominal centralisé. Les architectures edge-first correctement conçues peuvent atténuer la pente de cette cascade à moyen terme — c'est l'objet de la section 1.5.

¹Ministère des Armées / EMA, Concept de Manœuvre Multi-Milieus et Champs (M2MC), Paris, 2021 — document doctrinal de référence qui formalise les opérations inter-domaines (Terre, Mer, Air, Espace, Cyber, Champ informationnel). CICDE, Concept interarmées d'opérations CIA-01(A)_CICDE(2021). Voir aussi : Strachan H. (dir.), *The Changing Character of War*, Oxford UP, 2011 ; IFRI, « La doctrine M2MC et la transformation des armées françaises », Focus stratégique n° 109, 2022.

²US Army TRADOC, *The US Army in Multi-Domain Operations 2028*, TRADOC Pamphlet 525-3-1, décembre 2018 — concept fondateur des MDO posant la convergence des effets à travers tous les domaines pour créer des fenêtres d'opportunités. Perkins D. & Holmes J., « Multi-Domain Battle: Converging Combined Arms for the 21st Century », *Military Review*, nov.-déc. 2018. NATO ACT, *Concept for Multi-Domain Operations (MDO)*, Norfolk, 2023. Homologie structurelle avec le M2MC français : les deux doctrines requièrent un écosystème numérique robuste comme condition d'existence.

POSITION	NOM	RÔLE	STATUT DANS LE FLUX	VULNÉRABILITÉ PROPRE
ENTRÉE	Capteurs	Production de données brutes : radar (SAR, MTI), ISR, SIGINT/ELINT, imagerie EO/IR, drones, capteurs biométriques, IoMT	Nœud source – extérieur aux plaques de Reason	Spoofing GNSS silencieux, leurres thermiques, brouillage radar, compromission supply chain matérielle
PLAQUE 1	Connectivité – LDT	Transport du flux capteurs vers le cloud/edge. Supports : Link 16/22, SATCOM (GEO/LEO), mesh tactique HF, fibres déployées	1re plaque de Reason – fondation systémique	Brouillage LDT, EMP (fonctionnel vs physique – cf. § 3.2), cyber SATCOM, frappe ASAT
PLAQUE 2	Cloud & Edge	Calcul, stockage, traitement. Deux segments distincts : cloud global centralisé + edge autonome tactique déployé jusqu'au nœud bataillon	2e plaque de Reason	DDoS, ransomware, compromission hyperviseur, coupure alimentation, saturation bande passante

<p>PLAQUE 3</p>	<p>Données & COP</p>	<p>Fusion multi-sources, normalisation, production du Common Operating Picture partagé. Plaque la plus silencieusement vulnérable</p>	<p>3e plaque de Reason</p>	<p>Empoisonnement (data poisoning), manipulation COP, données périmées non signalées, COP divergents entre nœuds edge</p>
<p>PLAQUE 4</p>	<p>Applications & IA</p>	<p>Aide à la décision, C2 augmenté, planification feux, identification automatique, GE cognitive</p>	<p>4e plaque de Reason</p>	<p>Biais algorithmique, adversarial ML, supply chain logicielle corrompue (type SolarWinds), dépendances non auditées</p>
<p>DÉCISION</p>	<p>Commandement</p>	<p>Décision humaine finale – validation des effets, contrôle des effecteurs autonomes, autorité légale et éthique. Cumule deux rôles : barrière passive (doctrine, procédures) et décideur actif</p>	<p>5e plaque de Reason – verrou terminal délibérément dual</p>	<p>Deepfakes ordres, surcharge cognitive, biais décisionnel, insider threat haut rang, atrophie compétences analogiques, capitulation cognitive face à l'IA</p>

<p>SORTIE</p>	<p>Effecteurs</p>	<p>Production des effets : PGM, ailiers loyaux (CCA), UGV, USV/UUV, GE, cyber offensif. Autonomie locale croissante mais conditionnée par la programmation pré-mission</p>	<p>Nœud de sortie — extérieur aux plaques de Reason</p>	<p>Perte de guidage si flux rompu, divergence entre programmation pré-mission et situation réelle, fratricide si COP locaux divergents</p>
----------------------	-------------------	--	---	--

Le chemin critique opérationnel nominal : Capteur → LDT → Cloud/Edge → Données/COP → Apps/IA → Commandement → Effecteur. Ce flux est présenté sous forme linéaire pour en clarifier les dépendances séquentielles. Les systèmes C2 réels comportent des boucles de rétroaction (les effecteurs remontent des données d'évaluation vers P3, les capteurs embarqués sur ailiers loyaux alimentent P3 pendant l'engagement, le commandement peut court-circuiter P4 pour un guidage terminal direct) — chaque boucle est un vecteur d'injection de données corrompues supplémentaire dans P3 et doit être surveillée avec la même rigueur que le flux primaire.

⚠ NUANCE ESSENTIELLE : LA DÉPENDANCE EN CASCADE ET LES MÉCANISMES CORRECTEURS

La loi de la dépendance en cascade ne signifie pas que des capteurs leurrés corrompent nécessairement l'information en aval. Un écosystème bien conçu intègre dans P3 des mécanismes de correction : fusion multi-sources, scoring de cohérence entre capteurs, détection d'anomalies comportementales. Si plusieurs types de capteurs physiquement indépendants convergent sur la même information, la probabilité d'une corruption simultanée homogène est structurellement faible.

Le piège est précisément là : ces mécanismes correcteurs sont eux-mêmes dans la plaque P3. Si P3 est compromise — par data poisoning, manipulation COP, ou corruption du système de fusion — le correcteur tombe avec la plaque. L'adversaire avancé ne cherche donc pas à corrompre les capteurs : il cherche à compromettre P3, qui rendra alors toute correction impossible. C'est la raison pour laquelle P3 est décrite en §1.6 comme la plaque la plus silencieusement vulnérable — et pourquoi son niveau MMP minimum est fixé à 3 avec propriétaire J3 et arbitrage J6.

1.2 La dette numérique militaire : le risque invisible du haut commandement

La notion de dette technique est bien établie en ingénierie logicielle : il s'agit de l'accumulation de choix d'architecture sous-optimaux, de composants non mis à jour, de procédures non exercées, dont le coût différé augmente exponentiellement avec le temps. Appliquée au domaine militaire numérique, la dette numérique militaire désigne l'accumulation silencieuse de trous dans les plaques — équipements non patchés, procédures non documentées, architectures sans redondance, compétences analogiques atrophiées — dont personne ne mesure l'épaisseur réelle et dont l'effet ne se manifeste que le jour où une trajectoire de menace trouve le bon alignement. Le mécanisme précis de ce basculement — et la notion de marge de résilience résiduelle qui le formalise — est développé en §2.5.

Cette dette est structurellement invisibilisée par trois mécanismes. Le biais de normalité : l'absence d'incident est interprétée comme preuve de solidité des plaques, alors qu'elle ne prouve que l'absence de trajectoire de menace alignée jusqu'ici. Le cloisonnement fonctionnel J1–J9 : chaque bureau voit ses propres trous mais personne ne voit l'alignement transverse. La culture de la perfection technique : dans une organisation militaire à forte culture de responsabilité individuelle, admettre un trou dans sa plaque est culturellement proche d'admettre une faute — ce qui crée un puissant biais de sous-déclaration. Ces trois mécanismes sont documentés comme principaux freins à la transformation numérique des armées françaises dans les rapports parlementaires de référence.³

SI CE MAILLON CÈDE...	IMPACT SUR LE FLUX	CE QUI RESTE OPÉRATIONNEL	HORIZON DE RÉCUPÉRATION
Capteurs corrompus / spoofés	Données erronées en entrée — le COP devient un mensonge structuré	Stack numérique intact mais alimenté par du bruit	INSIDIEUX — récupération lente
Connectivité LDT rompue (DDIL)	Flux d'entrée coupé pour P2, P3, P4 — modes edge autonomes activés	Edge autonome (72h si architecturé) ; capteurs locaux	SYSTÉMIQUE — récupération par vecteur redondant

³Assemblée nationale, Rapport d'information sur les enjeux de la numérisation des armées, Commission de la défense nationale, n° 1836, 2023. Sénat, Rapport d'information sur la souveraineté numérique dans le domaine de la défense, n° 622, 2023. Cour des comptes, « La transformation numérique du Ministère des Armées », Rapport thématique, 2022. Sources institutionnelles françaises de référence identifiant les freins structurels à la transformation numérique des armées.

Connectivité LDT détruite (EMP)	Destruction physique irréversible des équipements non durcis	Équipements durcis EMP pré-positionnés uniquement	CRITIQUE — récupération par remplacement matériel
Cloud/Edge hors service	Aucun traitement — les données s'accumulent sans être traitées	IA embarquée légère au nœud edge si déployée	CRITIQUE — récupération par basculement edge
Données/COP empoisonnés	L'IA produit des recommandations viciées — aucune alarme générée	Vérification humaine croisée (lente et coûteuse cognitivement)	INSIDIEUX — récupération par audit et purge
Apps/IA hors service	L'aide à la décision disparaît — C2 humain seul face à la complexité	Procédures manuelles analogiques si exercées	MAJEUR — récupération par procédures dégradées
Commandement compromis	Ordres falsifiés ou décisions viciées à la source même du verrou	Contrôle hiérarchique secondaire si prévu ; règles d'engagement autonomes	CRITIQUE/DIH — récupération par contrôle externe
Effecteurs sans guidage	PGM redeviennent non précises — ailiers loyaux perdent leur désignation	Séquences préprogrammées pré-mission dans les limites de la programmation	MAJEUR — récupération par re-désignation si P1 rétablie

1.3 Les capteurs : vulnérabilités d'entrée et stratégie de robustesse

Les capteurs ne sont pas une plaque de Reason — ils sont le point d'injection du flux. Leurs vulnérabilités sont des vulnérabilités d'entrée : elles contaminent le flux à son origine, avant même d'atteindre P1, et peuvent traverser l'ensemble de la chaîne sans déclencher d'alarme si le stack numérique est conçu pour faire confiance à ses capteurs par défaut.

La vulnérabilité d'entrée structurellement la plus dangereuse est le spoofing silencieux : un signal GNSS falsifié, un leurre thermique ou un payload radar corrompu injectent des données fausses dans le flux sans déclencher d'alarme dans

les plaques de traitement aval. Le stack numérique fonctionne parfaitement — sur des données fausses. C'est l'équivalent systémique d'un laboratoire d'analyse parfaitement équipé qui travaille sur un échantillon contaminé à l'insu de tous ses opérateurs.

La défense architecturale fondamentale est la redondance multi-capteurs avec fusion cross-domaines et scoring de cohérence : si trois types de capteurs physiquement indépendants convergent sur la même information, la probabilité d'une corruption simultanée homogène est structurellement faible. Les capteurs quantiques à horizon 2030 — magnétomètres, gravimètres, horloges atomiques — offriront une navigation décimétrique sans GNSS, fermant structurellement le trou de spoofing GNSS non par compensation mais par élimination de la dépendance.

1.4 Les effecteurs : autonomie croissante et responsabilité déplacée dans le temps

Les effecteurs consomment les sorties du stack numérique. La transformation la plus structurante de cette plaque de sortie est l'émergence de l'autonomie locale : un effecteur préprogrammé peut exécuter une séquence sans connexion permanente au stack central. Les ailiers loyaux⁴ et les systèmes autonomes terrestres et navals⁵ illustrent cette capacité. Elle produit un déplacement temporel fondamental : l'autorité de commandement n'est pas supprimée — elle est exercée en amont lors de la programmation pré-mission. La plaque P5 n'a pas sauté ; elle a été activée avant le décollage.

⁴DARPA, Collaborative Combat Aircraft (CCA) Program, 2023–2024. Boeing MQ-28A Ghost Bat (Australie) ; Kratos XQ-58A Valkyrie (USAF) ; Dassault Aviation / MBDA nEUROn (démonstrateur franco-européen). RAND, « Loyal Wingman Concepts and Implications », RR-A1214, 2022. IRSEM, « Autonomie et LAWS dans les opérations aériennes françaises », Étude 116, 2023. DGA, Feuille de route Aéronefs de Combat Collaboratifs (ACC), 2023.

⁵RAND Corporation, Autonomous and Remotely Piloted Military Systems, RR-A2196-1, 2023. NATO STANAG 4670 (UAV Operations). CSIS, « The Future of Ground Combat », 2023. FRS, « Robotisation du champ de bataille : enjeux doctrinaux », Note 32/2023. DGA, Feuille de route Systèmes Terrestres Autonomes (STA), 2022.

CATÉGORIE	SYSTÈMES ACTUELS	DÉPENDANCE AU FLUX (RÉGIME NOMINAL)	AUTONOMIE LOCALE (RUPTURE P1)	RISQUE RÉSIDUEL
Munitions guidées (PGM)	JDAM, SCALP-EG, Storm Shadow, Excalibur	Désignation d'objectif via LDT + GNSS	Guidage inertiel terminal si GNSS coupé — précision dégradée	Impuissance si désignation impossible et inertielle non calibrée
Ailiers loyaux / CCA	XQ-58A Valkyrie, MQ-28A Ghost Bat, nEUROn	Datalink tactique pour missions collaboratives	Exécution séquences préprogrammées — haute autonomie	Règles d'engagement pré-mission obsolètes si situation réelle diverge
Robots terrestres (UGV)	THeMIS, MUTT, Titan	LDT courte portée pour téléopération	Navigation autonome locale — engagement sous autorisation humaine	Fratricide si IFF numérique rompu en mode autonome
Drones navals (USV/UUV)	Sea Hunter, MUSV, Remus, Orca	SATCOM surface / acoustique sous-marin	Mission préprogrammée — remontée données différée	Déconnexion prolongée = décisions sur données périmées
GE & cyber offensif	EA-18G, NGJ-MB, AESA, capacités SIGINT	Entièrement dépendant de C4 (Apps/IA)	Faible — requiert coordination temps réel	Panne P4 = cécité GE totale

Doctrine fondamentale sur l'autonomie des effecteurs : l'autonomie locale ne supprime pas la dépendance au commandement humain — elle la déplace dans le temps. Un ailier loyal exécute une séquence autorisée lors de sa programmation pré-mission. La plaque P5 n'a pas été contournée ; elle a été activée en amont. Cette distinction est capitale pour la conformité au Droit International Humanitaire : l'autorisation humaine doit être explicite, documentée et traçable, qu'elle soit exercée en temps réel ou en amont sous forme de règles d'engagement préautorisées.

1.5 Résilience opérationnelle : mode dégradé, mode décentralisé et tension M2MC

La résilience numérique opérationnelle repose sur deux modes complémentaires que la doctrine doit distinguer rigoureusement, car leurs conditions d'activation et leurs risques propres sont différents.

MODE	DÉFINITION	CE QUI RESTE OPÉRATIONNEL	CONDITIONS REQUISES	RISQUE PROPRE
MODE DÉGRADÉ	Maintien d'une capacité réduite malgré la perte partielle d'un maillon – des maillons humains compensent manuellement les plaques défailtantes	Flux partiel avec compensation humaine	Procédures dégradées documentées et exercées au minimum trimestriellement	Latence décisionnelle accrue, surcharge cognitive des opérateurs, erreurs manuelles
MODE DÉCENTRALISÉ	Délégation de l'autorité décisionnelle aux nœuds edge – chaque nœud opère avec ses propres données locales et ses règles d'engagement prédéfinies	Flux complet miniature au niveau bataillon : capteurs locaux → edge → données locales → IA embarquée → commandement local → effecteurs	Architecture edge-first, IA embarquée, commandement par mission, règles d'engagement préautorisées	COP locaux divergents → risque de fratricide numérique et de décisions tactiques incompatibles

🛡️ TENSION ARCHITECTURALE : CONVERGENCE M2MC VS RÉSILIENCE DÉCENTRALISÉE

La doctrine M2MC exige une convergence maximale des données inter-domaines pour produire les effets combinés qu'elle promet — ce qui requiert un flux numérique riche, central et synchronisé. L'architecture de résilience décentralisée fragmente intentionnellement ce flux pour maintenir l'autonomie edge en cas de rupture — ce qui réduit la convergence. Ces deux impératifs sont en tension structurelle irréductible : plus le flux est convergent, plus la surface d'attaque et le couplage sont élevés ; plus il est décentralisé, moins la M2MC est garantie en temps réel. Cette tension n'a pas de résolution architecturale absolue — elle a une résolution doctrinale : prioriser la convergence en régime nominal et déclencher automatiquement le mode décentralisé dès que P1 ou P2 est dégradée au-delà d'un seuil prédéfini. Ce basculement doit être une procédure automatisée, non une décision ad hoc sous stress.

Le *commandement par mission* — formalisé dans la doctrine française par l'EMA et le CICDE comme mode d'exercice de l'autorité fondé sur la délégation de l'initiative — est le socle doctrinal du mode décentralisé. Son principe : le supérieur fixe l'intention et l'objectif final ; le subordonné détermine librement les moyens et l'exécution selon son appréciation de la situation locale. L'initiative du subordonné n'est pas une tolérance exceptionnelle face à la panne — elle est la norme d'emploi présumée. La connectivité centrale est souhaitée ; elle n'est jamais requise.

Ce principe comporte un risque opérationnel propre que la doctrine numérique doit anticiper explicitement : le fratricide numérique. Deux unités adjacentes opérant sur des COP locaux divergents peuvent prendre des décisions tactiques incompatibles — zones de frappe qui se chevauchent, axes de progression conflictuels, identification ami-ennemi incohérente entre secteurs. Ce risque est réel et documenté dans les exercices OTAN de commandement décentralisé. La mitigation repose sur trois piliers : (1) règles de déconfliction sectorielles intégrées aux règles d'engagement préautorisées ; (2) fenêtres de re-synchronisation COP dès que P1 est partiellement rétablie, même brièvement ; (3) culture d'état-major entraînée à signaler activement les divergences de situation.

1.6 Le chemin critique et la cartographie des cinq plaques

Les cinq plaques de Reason dans l'écosystème numérique militaire sont les quatre plaques internes du stack (P1 à P4) plus le commandement (P5). Elles constituent les barrières structurantes dont l'alignement de trous produit les défaillances

systemiques. Capteurs et effecteurs ne sont pas des plaques — ils sont les nœuds périphériques du flux, avec leurs propres profils de vulnérabilité traités séparément.

PLAQUE	PLAQUE	TROUS CARACTÉRISTIQUES	BARRIÈRES ACTIVES	SOLIDITÉ CIBLE
P1	Connectivité — LDT	Brouillage Link 16/22, EMP (destruction physique), cyber SATCOM, frappe ASAT, harvest now/decrypt later (PQC)	Redondance multi-vecteurs (SATCOM+mesh+HF), fréquences anti-brouillage, durcissement EMP, migration PQC avant 2027	Niveau 4 minimum — niveau 5 pour les états-majors opératifs
P2	Cloud & Edge	DDoS, ransomware, compromission hyperviseur, coupure alimentation, modèles IA non synchronisés	Edge-first design (72h autonomie validée en exercice), isolation réseaux critiques, indicateur fraîcheur modèle IA	Niveau 4 — edge autonome validé trimestriellement
P3	Données & COP	Data poisoning (silencieux), manipulation COP, données périmées non signalées, divergence COP inter-nœuds edge, flux de rétroaction effecteurs corrompus	Anomaly detection comportementale IA, audit de source horodaté, scoring de cohérence multi-sources, seuil fraîcheur AJP-2.1	Niveau 3 minimum — propriétaire J3 avec arbitrage J6
P4	Applications & IA	Biais algorithmique, adversarial ML, supply chain logicielle corrompue (type SolarWinds), dépendances non auditées, composants d'origine étrangère	HITL obligatoire, red-team adversarial semestriel, SBOM (Software Bill of Materials), sandbox déploiement mises à jour critiques	Niveau 3 minimum — audit supply chain annuel

P5	Commandement	Deepfakes ordres, biais décisionnel non reconnu, insider threat haut rang, atrophie compétences analogiques, capitulation cognitive face aux recommandations IA	Procédures analogiques maintenues et exercées, compartimentage des droits, surveillance accès privilégiés (J2+J6), culture de questionnement de l'IA	Niveau 4 — exercice C2 analogique trimestriel
----	--------------	---	--	---

Note théorique sur le statut de P5 : dans le modèle de Reason original, les plaques sont des défenses passives. P5 cumule ici deux rôles — barrière passive (doctrine, procédures) et décideur actif (le commandant). Cette dualité est assumée : dans l'écosystème numérique militaire, le commandant EST la procédure terminale. Ses propres défaillances — biais cognitif, erreur de jugement, décision incorrecte sous stress, capitulation cognitive face à l'IA — constituent des trous dans P5 au même titre qu'une procédure non documentée. Cette posture est cohérente avec la doctrine HRO : la barrière humaine terminale est à la fois la plus flexible et la plus exposée à la variabilité.

1.7 Le problème de la synchronisation : coordonner l'action décentralisée

La section 1.5 a décrit la tension architecturale entre convergence M2MC et résilience décentralisée. Elle a traité les deux modes séparément. Ce qui n'a pas été formalisé est le problème central qui les relie : comment des noeuds edge opérant de façon autonome — chacun avec son propre COP local, ses propres règles d'engagement, ses propres données — se resynchronisent-ils lorsque P1 se rétablit partiellement ou totalement ? Ce problème de synchronisation inter-plaques est la clé de voûte du mode décentralisé. Sans réponse doctrinale précise, le commandement par mission numérique reste une intention non opérationnalisable.

Le problème se pose en trois temps. En premier lieu, pendant la phase d'autonomie (P1 rompue), chaque noeud edge accumule un historique d'actions, de décisions et de modifications COP locales qui n'ont pas été partagées. La divergence entre COP locaux croît de façon monotone avec la durée de la déconnexion — c'est la raison pour laquelle AJP-2.1 fixe un seuil de fraîcheur à 24 heures de stabilisation. En second lieu, lors du rétablissement partiel de P1, la fenêtre de re-synchronisation est le moment de risque maximal : certains noeuds ont reçu la mise à jour COP, d'autres pas encore. Les

décisions prises dans cette fenêtre peuvent reposer sur des COP partiellement convergents — une configuration plus dangereuse qu'un COP uniformément dégradé car elle crée une illusion de convergence.

En troisième lieu, après re-synchronisation complète, les actions prises en mode autonome doivent être intégrées dans le COP commun en les distinguant clairement des données temps réel — avec leur timestamp d'origine, leur niveau de fraîcheur, et une indication de leur statut (confirmé, non vérifié, potentiellement périmé). Ce n'est pas un problème technique — c'est un problème doctrinal : les systèmes C2 actuels ne sont pas tous conçus pour gérer cette sémantique de fraîcheur distribuée.

PHASE	RISQUE PRINCIPAL	MÉCANISME DE MITIGATION	INDICATEUR DE CONTRÔLE
Autonomie (P1 rompue)	Divergence COP inter-nœuds — fratricide numérique si actions simultanées sur zones adjacentes	Règles de déconfliction sectorielles intégrées aux règles d'engagement préautorisées	Délai d'autonomie validé en exercice — seuil MMP P2 : 72h
Rétablissement partiel P1	COP partiellement convergent — illusion de synchronisation plus dangereuse qu'une déconnexion totale	Protocole de neutralité décisionnelle pendant la fenêtre de re-sync — proposition doctrinale de ce document (durée estimée : 15 à 30 min selon le niveau de l'échelon)	Indicateur de convergence COP — % nœuds re-synchronisés avant reprise décisions coordonnées
Re-synchronisation complète	Intégration d'actions autonomes dans le COP commun sans distinction de fraîcheur	Timestamping obligatoire des données edge avec statut de fraîcheur (confirmé / non vérifié / périmé)	Audit de cohérence post-synchronisation — propriétaire J3
Régime nominal rétabli	Retour prématuré au flux centralisé avant validation de la convergence	Validation explicite de convergence COP par l'échelon J3 avant reprise du flux M2MC complet	Temps de validation convergence — objectif : moins de 30 min après rétablissement P1

SYNCHRONISATION ET DUAL OPERATING SYSTEM (KOTTER)

Le problème de synchronisation inter-plaques est également un problème organisationnel. La section 6.5 décrit le Dual Operating System de Kotter — système hiérarchique + réseau accélérateur. En termes de synchronisation numérique, le réseau accélérateur joue le rôle de mécanisme de re-synchronisation culturelle (voir §1.7 pour la dimension technique de cette synchronisation inter-plaques) : il assure que les équipes numériques des différents noeuds partagent non seulement les mêmes données mais les mêmes schémas mentaux pour les interpréter.

Un noeud edge parfaitement synchronisé techniquement mais culturellement déconnecté du référentiel commun prendra des décisions incompatibles avec les autres noeuds. La synchronisation est donc à la fois un problème d'architecture (P1, P3) et un problème de gouvernance organisationnelle (P5, Section VI).

1.8 La temporalité comme variable stratégique indépendante

La temporalité n'est pas simplement un paramètre du flux numérique — elle est une variable stratégique indépendante que l'adversaire maîtrise et que le défenseur sous-estime structurellement. Deux dimensions temporelles coexistent dans l'écosystème numérique militaire et leur interaction détermine l'issue de la confrontation : la latence de détection et le cycle OODA de l'adversaire.

La latence de détection est le délai entre le moment où une plaque est compromise et le moment où cette compromission est détectée par le défenseur. Pour une rupture franche (EMP sur P1, DDoS sur P2), cette latence est quasi nulle — l'effet est immédiat et visible. Pour une corruption silencieuse (data poisoning sur P3, implant sur P4), cette latence peut atteindre plusieurs semaines ou mois. SolarWinds a été déployé en mars 2020 et détecté en décembre 2020 — neuf mois de fenêtre d'exploitation silencieuse.

Le cycle OODA (Observe-Orient-Decide-Act) de l'adversaire cyber fonctionne à une vitesse structurellement asymétrique par rapport au cycle de détection défensive. L'adversaire observe en continu (reconnaissance passive), oriente en temps différé (analyse hors ligne), décide de façon centralisée (planification), et agit de façon ciblée (frappe unique ou campagne longue durée). Le défenseur doit détecter, analyser, décider et répondre dans une fenêtre beaucoup plus contrainte, souvent sous pression opérationnelle simultanée.

SCÉNARIO

LATENCE DE
DÉTECTIONFENÊTRE
D'EXPLOITATION

LEÇON DOCTRINALE

Rupture P1 franche (EMP / jamming)	Moins d'1 minute	Nulle — effet immédiat, mode dégradé activé instantanément	Procédures dégradées et edge autonome doivent être pré-activés, pas réactifs
Compromise P2 (ransomware)	Moins de 24 heures	Quelques heures — propagation latérale rapide avant détection	Micro-segmentation et isolation réseau critiques pour limiter la propagation
Corruption P3 silencieuse (data poisoning)	Plusieurs jours à semaines	Longue — toutes les décisions prises pendant la fenêtre sont viciées	Anomaly detection comportementale avec seuil d'alerte AJP-2.1 : priorité absolue
Implant P4 (supply chain)	Semaines à mois	Très longue — exfiltration, cartographie, positionnement possible	SBOM vivante + sandbox déploiement + red-team adversarial semestriel
Compromission P5 (deepfake / insider)	Potentiellement indétectable sans protocole spécifique	Illimitée — les ordres falsifiés entrent dans le flux sans signal d'alerte	Culture de vérification croisée + surveillance accès privilégiés J2+J6

L'implication opérationnelle est directe : la temporalité doit être intégrée dans la posture défensive non pas comme contrainte mais comme levier. Pour les ruptures franches, la réponse est réactive et préparée. Pour les compromissions silencieuses — data poisoning, supply chain, insider — la réponse doit être proactive et continue : détection comportementale permanente, exercices de red-team réguliers, et culture de signalement des anomalies même mineures, conformément aux principes HRO de préoccupation pour l'échec (§2.4).

La temporalité éclaire également la notion de dette numérique (§2.5) : une plaque dont la marge de résilience résiduelle a été réduite par l'accumulation de dette est précisément une plaque dont la fenêtre d'exploitation adversariale s'est allongée. L'adversaire patienteur — profil APT étatique — optimise ses opérations en attendant que la dette du défenseur atteigne le point d'inflexion avant d'agir.

1.9 Matrice de criticité croisée : l'adversaire n'a pas besoin des cinq plaques

Une lecture linéaire du modèle des cinq plaques pourrait laisser croire que l'adversaire doit traverser l'intégralité du flux pour produire un effet opérationnel significatif. C'est une erreur analytique que les crises réelles corrigent brutalement. Stuxnet a ciblé P2 et P4. Shamoon a frappé P2 directement, sans toucher P1. Viasat H-1 a rompu P1 en une heure sans que P2 à P5 soient directement compromises. Dans chaque cas, une combinaison partielle de plaques fragilisées ou rompues a suffi à produire un effet opérationnel de niveau stratégique.

La matrice suivante cartographie les combinaisons critiques — les configurations de ruptures partielles qui produisent un niveau de dégradation opérationnelle suffisant pour interdire ou dégrader significativement la manœuvre M2MC. Elle ne prétend pas à l'exhaustivité mais identifie les combinaisons les plus probables selon le profil de l'adversaire.

COMBINAISON	EFFET OPÉRATIONNEL PRODUIT	CAS HISTORIQUE	DÉGRADATION M2MC
P1 seule rompue	Isolement des noeuds — edge autonome activé, synchronisation COP dégradée	Viasat (02/2022)	MAJEURE — convergence inter-domaines impossible en temps réel
P3 seule corrompue	COP empoisonné — décisions vicieuses à la source, aucune alarme générée	Campagnes APT P3 (Ukraine 2022)	CRITIQUE — la rupture est invisible jusqu'à l'engagement
P1 + P3	Isolement + COP local corrompu — le noeud edge opère sur des données fausses sans possibilité de vérification externe	Scénario haute intensité modélisé OTAN	CATASTROPHIQUE — fratricide numérique probable
P2 + P4	Traitement détruit + IA compromise — aucun traitement fiable disponible, aide à la décision corrompue ou absente	Stuxnet (profil P2+P4)	CRITIQUE — C2 humain seul, surcharge cognitive maximale
P4 seule corrompue (supply chain)	IA produit des recommandations viciées sans signal d'alerte — P1, P2, P3 intactes	SolarWinds (2020)	INSIDIEUSE — dégradation invisible, potentiellement durable
P5 seule dégradée	Décisions vicieuses au niveau commandement — le flux est intact mais son utilisation est compromise	Deepfakes / insider threat	STRATÉGIQUE — légitimité des ordres en question
P1 + P2 + P3	Effondrement complet du flux nominal — mode décentralisé activé sur données potentiellement corrompues	Scénario DDIL + empoisonnement simultané	RUPTURE TOTALE du flux centralisé

Trois enseignements structurants ressortent de cette matrice. Premièrement, P3 est la plaque dont la rupture isolée produit l'effet le plus insidieux : le flux continue, les systèmes semblent fonctionner, mais les décisions sont viciées à la source. C'est la raison pour laquelle le niveau MMP minimum sur P3 est fixé à 3 — propriétaire J3 avec arbitrage J6 — dans le cadre de gouvernance du §5.2.

Deuxièmement, la combinaison P1+P3 est la plus dangereuse en haute intensité car elle active simultanément le mode décentralisé (P1 rompue) et corrompt les données sur lesquelles ce mode décentralisé opère (P3 corrompue). Le noeud edge autonome prend ses décisions sur un COP local faux sans possibilité de vérification externe. Le risque de fratricide numérique dans cette configuration est maximal.

Troisièmement, P4 corrompue par supply chain (profil SolarWinds) est structurellement imperceptible par les défenses classiques : P1, P2 et P3 sont intactes, les flux passent normalement, mais l'IA en P4 traite des données réelles avec un modèle corrompu. La seule défense efficace est en amont du flux : SBOM vivante, sandbox de déploiement, red-team adversarial semestriel.

IMPLICATION POUR LA POSTURE DÉFENSIVE

La matrice de criticité croisée modifie la logique de priorisation défensive. Il ne suffit pas de consolider chaque plaque individuellement — il faut identifier les combinaisons de ruptures partielles que l'adversaire peut produire avec le moindre effort et les durcir en priorité.

Pour un adversaire étatique disposant de capacités cyber et EMP : la combinaison P1+P3 est sa cible optimale. Pour un adversaire spécialisé en APT : P4 par supply chain est sa porte d'entrée favorite. La planification défensive doit intégrer ces profils adversariaux dès la conception des architectures — pas uniquement lors des exercices de red-team.

SECTION II — POURQUOI LE MODELE DE REASON S'IMPOSE

2.1 Trois propriétés de l'écosystème qui rendent Reason incontournable

L'écosystème numérique militaire présente trois propriétés structurelles qui le rendent directement isomorphe au modèle de Reason. La complexité couplée (Perrow⁶) : chaque plaque transmet ses sorties sans délai à la suivante pour comprimer le cycle OODA⁷ — ce couplage temporel rend la défaillance en cascade quasi-instantanée et non réversible à court terme. La défense en profondeur organisée : la doctrine militaire a toujours structuré sa posture défensive en strates indépendantes — c'est exactement ce que Reason formalise. L'hétérogénéité des défaillances latentes : les trous dans les plaques existent en permanence (équipements non patchés, procédures non exercées, architectures sans redondance) — ils attendent que d'autres trous s'alignent.

Ces trois propriétés sont explicitement documentées par l'IRSEM et la RAND Corporation comme conditions de fragilité systémique des systèmes C2 numériques — ce qui rend l'application du modèle de Reason à l'écosystème militaire non seulement légitime mais académiquement nécessaire.

2.2 La menace interne : le trou que l'adversaire n'a pas besoin de créer

Le modèle de menace implicite dans la plupart des analyses de cybersécurité militaire est exclusivement exogène : l'adversaire entre par effraction. Cette hypothèse est structurellement incomplète. Un trou dans P4 ou P5 n'est pas seulement le résultat d'une attaque externe — il peut être créé, maintenu ou exploité délibérément par un acteur interne disposant d'accès légitimes. Les compromissions majeures de la dernière décennie (Snowden 2013, Manning 2010, affaires nationales documentées

⁶Perrow C., *Normal Accidents: Living with High-Risk Technologies*, Basic Books, 1984. Pour l'application aux systèmes de commandement : RAND, « High Reliability Organizations and Military Cyber Resilience », RR-4408, 2021. La complexité couplée de Perrow est la propriété systémique qui rend le modèle de Reason particulièrement adapté aux écosystèmes C2 numériques.

⁷Boyd J., « A Discourse on Winning and Losing », USAF briefing, 1987. Osinga F., *Science, Strategy and War: The Strategic Theory of John Boyd*, Routledge, 2007. Bousquet A., *The Scientific Way of Warfare*, Columbia UP, 2009. Le cycle OODA est le référentiel de la compétition décisionnelle en conflit à haute intensité — IRSEM, « Décision et vitesse : le cycle OODA dans les opérations numériques », Étude 98, 2022.

par les services de contre-ingérence⁸) montrent que l'insider est structurellement le vecteur le plus difficile à détecter : il opère en-deçà du périmètre que P1 à P3 sont conçus à défendre.

La plaque P5 est particulièrement exposée : un officier supérieur compromis ou un opérateur IA disposant de droits d'administration sur P4 peut aligner silencieusement des trous sur l'ensemble de la chaîne sans déclencher aucune alarme périmétrique. Les barrières spécifiques — moindre privilège, compartimentage des droits, surveillance comportementale des accès privilégiés, rotation des habilitations — relèvent de la responsabilité conjointe J2 et J6 et constituent une couche de protection distincte des barrières techniques classiques. Une plaque sans surveillance des accès internes est une plaque dont les trous peuvent être créés de l'intérieur.

2.3 Précédents sectoriels et limites du modèle

L'aviation civile⁹ a réduit son taux d'accidents mortels par passager-kilomètre de l'ordre de 80 à 95% entre 1970 et 2000 — réduction dont l'adoption systémique du modèle de Reason est l'un des facteurs structurants, aux côtés des progrès de conception et de la régulation internationale. Le nucléaire civil¹⁰ en a fait le fondement de sa défense en profondeur à trois barrières physiques. Les organisations à haute fiabilité¹¹ partagent cinq propriétés directement transposables aux états-majors

⁸Rapport de la Commission nationale de contrôle des techniques de renseignement (CNCTR), 2022–2023 — sur la menace interne dans les institutions françaises. DPSD (Direction de la Protection et de la Sécurité de la Défense), Rapport annuel de la menace, 2023 (diffusion restreinte, résumé public). Verizon DBIR 2023 : 19% des violations de données impliquent une menace interne (insider threat), taux en augmentation de 4 points depuis 2021.

⁹ICAO, Human Factors Training Manual (Doc 9683), 1998. La réduction du taux d'accidents mortels par passager-kilomètre de l'aviation commerciale est de l'ordre de 80 à 95% entre 1970 et 2000 (IATA, Safety Report 2022) — réduction dont le modèle de Reason est l'un des facteurs structurants, aux côtés des progrès de conception des aéronefs, de la gestion du trafic aérien et de la régulation internationale. Boeing / Airbus accident statistics, 1970–2000.

¹⁰IRSN, Défense en profondeur et barrières de sécurité nucléaires, INF-2019-00083, 2019. ASN, La sûreté nucléaire en France, Rapport annuel 2022. La défense en profondeur à trois barrières physiques (gaine de combustible, circuit primaire, enceinte de confinement) est le modèle précurseur du Swiss Cheese appliqué à un système industriel critique.

¹¹Weick K.E. & Sutcliffe K.M., *Managing the Unexpected: Assuring High Performance in an Age of Complexity*, Jossey-Bass, 2001, pp. 10–17 — cinq propriétés HRO : préoccupation pour l'échec, résistance à la simplification, sensibilité aux opérations, engagement pour la résilience, déférence à l'expertise terrain. RAND, « HRO and Military Cyber Resilience », RR-4408, 2021. IRSEM, « Résilience organisationnelle des forces armées », Études et Observations 12/2022.

numériques : préoccupation pour l'échec, résistance à la simplification, sensibilité aux opérations, engagement pour la résilience, déférence à l'expertise terrain.

Le modèle STAMP de Leveson¹² est théoriquement plus rigoureux : il modélise les contraintes de contrôle qui empêchent les accidents dans un système défini globalement, là où Reason identifie des trous dans des barrières prédéfinies. STAMP est potentiellement supérieur en phase de conception de systèmes — son implémentation requiert cependant une expertise en ingénierie des systèmes incompatible avec la réactivité des états-majors en opérations. Le choix de Reason ici n'est pas un jugement de supériorité théorique — c'est un jugement d'applicabilité opérationnelle. Les deux modèles sont complémentaires : STAMP en conception, Reason en analyse continue.

✘ L'ASYMÉTRIE FONDAMENTALE ATTAQUANT / DÉFENSEUR

Le modèle de Reason révèle une asymétrie stratégique structurelle : l'attaquant n'a besoin de trouver qu'un seul alignement de trous traversant les cinq plaques — au moment de son choix, avec l'élément de surprise. Le défenseur doit maintenir toutes les plaques, simultanément, en permanence, avec des ressources contraintes. Cette asymétrie coût-bénéfice est favorable à l'offensive par construction. La réponse doctrinale n'est pas de prétendre à des plaques parfaites — c'est d'augmenter le coût de l'alignement pour l'adversaire en multipliant l'indépendance des plaques, en réduisant leur corrélation, et en rendant les trous imprévisibles et dynamiques plutôt que fixes et cartographiables.

La résonance avec la tradition stratégique militaire confirme le choix : Sun Tzu¹³ — « attaque là où il est vide » — est la formulation doctrinale la plus ancienne de la stratégie d'exploitation des trous alignés. Le modèle de Reason n'apporte pas un concept nouveau à la pensée militaire ; il en fournit la formalisation analytique rigoureuse.

¹²Leveson N., *Engineering a Safer World: Systems Thinking Applied to Safety*, MIT Press, 2012. Le modèle STAMP (Systems-Theoretic Accident Model and Processes) est théoriquement supérieur à Reason pour la conception ex nihilo de systèmes complexes — sa modélisation est causale et systémique là où Reason est post-hoc et séquentielle. Mais son implémentation requiert une expertise en ingénierie des systèmes de sécurité incompatible avec l'adaptation doctrinale continue. STAMP en conception de systèmes, Reason en analyse opérationnelle continue : les deux modèles sont complémentaires, non rivaux. IRIS, « Sécurité des systèmes complexes de défense », Lettre de l'IRIS n° 47, 2023.

¹³Sun Tzu, *L'Art de la Guerre*, ~500 av. J.-C., ch. VI : « Attaque là où il est vide. » Cette formulation est la plus ancienne expression documentée de la stratégie d'exploitation des lacunes défensives adverses — directement isomorphe à la recherche d'alignement de trous dans les plaques. IRSEM, « Sun Tzu et la cyberstratégie contemporaine », Note de lecture 14, 2021.

L'ancrage dans la doctrine M2MC est direct : la convergence des effets inter-domaines (Terre, Mer, Air, Espace, Cyber) que la M2MC requiert ne peut se réaliser que si les cinq plaques du flux numérique sont suffisamment solides pour soutenir la cadence décisionnelle exigée. Une doctrine de convergence inter-domaines sur un écosystème numérique criblé de trous n'est pas une doctrine d'emploi — c'est une promesse opérationnelle dont les conditions de réalisation ne sont pas garanties.

2.4 Du modèle de Reason aux HRO : vers une résilience active

Le modèle de Reason constitue le socle analytique de ce document. Il répond à une question précise : comment les accidents systémiques se produisent-ils dans les organisations complexes ? Sa réponse — l'alignement de trous dans des plaques de défense successives — fournit un cadre rigoureux pour cartographier les vulnérabilités de l'écosystème numérique militaire et raisonner sur leur exploitation adversariale.

Mais Reason appartient à ce que Hollnagel (2014) nomme le paradigme Safety-I (littéralement : « sécurité par élimination des causes de défaillance ») : une conception de la sécurité centrée sur la prévention des défaillances, sur l'élimination des trous. Cette posture est nécessaire — mais insuffisante dans un environnement à haute intensité où la sollicitation adversariale est continue, où les trous ne peuvent pas tous être comblés, et où la question opérationnelle n'est pas seulement 'comment éviter la rupture' mais 'comment continuer à fonctionner malgré elle'.

C'est précisément ce que les paradigmes complémentaires apportent : les High Reliability Organizations — HRO (Weick et Sutcliffe, 2001 ; La Porte et Consolini, 1991) et la Resilience Engineering (Hollnagel, Woods et Leveson, 2006) déplacent la question fondamentale de la prévention vers l'adaptation dynamique.

PARADIGME	QUESTION CENTRALE	POSTURE	APPLICATION À L'ÉCOSYSTÈME MILITAIRE
Safety-I (Reason)	Pourquoi les systèmes tombent-ils en panne ?	Rétrospective — cartographier et combler les trous	Cartographie des vulnérabilités P1-P5, analyse des scénarios de défaillance (§III)
HRO (Weick, Sutcliffe)	Comment les systèmes tiennent-ils malgré la pression ?	Prospective — développer la conscience situationnelle collective	Culture de signalement des signaux faibles, mindfulness organisationnelle en état-major numérique
Safety-II (Hollnagel)	Comment les systèmes s'adaptent-ils en temps réel ?	Dynamique — amplifier les adaptations qui fonctionnent	Résilience active en mode DDIL, commandement par mission numérique

**Resilience
Engineering
(Woods,
Leveson)**

Quelles sont les marges de manœuvre du système ?

Systémique — gérer les marges de résilience résiduelle

MMP (§5.1), indicateurs de marge par plaque, seuils de basculement (§2.5.3)

Les HRO présentent cinq caractéristiques fondamentales identifiées par Weick et Sutcliffe : la préoccupation pour l'échec (traiter chaque anomalie comme signal potentiel de défaillance systémique), la réticence à simplifier (refuser les explications rassurantes), la sensibilité aux opérations (conscience situationnelle distribuée à tous les niveaux), l'engagement envers la résilience (capacité à improviser sous pression), et le respect de l'expertise (déférence à celui qui sait, pas à celui qui grade). Ces cinq caractéristiques s'appliquent directement à la gouvernance numérique militaire : la préoccupation pour l'échec concerne P3 (signalement de toute anomalie COP même mineure) ; la réticence à simplifier concerne P4 (ne pas accepter l'IA comme boîte noire) ; la sensibilité aux opérations concerne P1 (écoute active de l'opérateur terrain sur la qualité des liaisons) ; l'engagement envers la résilience concerne P2 (improvisation en mode DDIL) ; le respect de l'expertise concerne P5 (déférer au J6 sur les questions architecturales, non au grade). Leur absence constitue elle-même une forme de dette numérique — principalement localisée en P5.

Le concept de Safety-II mérite une attention particulière car il résout élégamment la tension architecturale décrite en §1.5 entre convergence M2MC et résilience décentralisée. Hollnagel observe que dans les systèmes complexes, la performance normale repose non pas sur l'absence d'erreurs mais sur les ajustements permanents des opérateurs qui compensent les imperfections du système. La résilience ne s'obtient pas en éliminant la variabilité — elle s'obtient en développant la capacité à gérer cette variabilité de façon adaptative. Appliqué à l'écosystème numérique militaire : le mode décentralisé n'est pas une dégradation du flux nominal — c'est une forme d'adaptation Safety-II qui doit être entraînée, documentée et valorisée doctrinalement au même titre que le flux centralisé.

REASON, HRO ET SAFETY-II : TROIS OUTILS COMPLÉMENTAIRES, PAS CONCURRENTS

Ce document utilise principalement le modèle de Reason comme outil de cartographie des vulnérabilités — ce pour quoi il est le plus rigoureux. Les HRO et Safety-II complètent ce cadre pour la partie résilience dynamique et transformation organisationnelle. Reason dit où sont les trous. Les HRO disent comment une organisation tient malgré eux. Safety-II dit comment elle s'adapte quand ils s'alignent.

Cette complémentarité n'est pas un compromis théorique — c'est la posture intellectuelle exacte qu'adopte la doctrine OTAN en matière de résilience des systèmes C2 : cartographier les défaillances possibles (Reason), développer une culture organisationnelle de haute fiabilité (HRO), et entraîner la capacité d'adaptation en temps réel (Safety-II / commandement par mission numérique).

2.5 La dette numérique : du fil rouge au mécanisme de rupture

La dette numérique militaire a été introduite en section 1.2 comme un fil rouge analytique. Elle désigne l'accumulation silencieuse de trous dans les plaques — équipements non patchés, procédures non exercées, architectures sans redondance, compétences analogiques atrophiées. Trois questions fondamentales sont restées ouvertes : comment se crée-t-elle précisément, comment se résorbe-t-elle, et — surtout — quel est le mécanisme qui la transforme en rupture opérationnelle réelle ? C'est l'objet de cette section.

2.5.1 Taxonomie des sources : comment la dette se crée

La dette numérique militaire ne se crée pas d'un seul tenant. Elle s'accumule selon quatre vecteurs distincts qui s'alimentent mutuellement.

Le premier vecteur est architectural : des choix de conception initiaux sous-optimaux — architectures plates sans micro-segmentation, absence de redondance multi-vecteurs sur P1, cloud centralisé sans capacité edge autonome — dont le coût de correction croît exponentiellement avec le temps et l'intégration des systèmes aval. Une décision d'architecture prise en 2015 sur P2 contraint la solidité de P3 en 2025.

Le deuxième vecteur est procédural : les procédures dégradées existent sur le papier mais ne sont pas exercées. AJP-2.1 fixe le seuil de fraîcheur du COP ; aucune alarme ne se déclenche si ce seuil est silencieusement dépassé. La procédure non exercée n'est pas un trou visible — c'est une barrière dont on ignore si elle tient jusqu'au moment où elle doit tenir.

Le troisième vecteur est budgétaire : les reports de maintenance, de mise à jour logicielle et de remplacement matériel constituent la forme la plus courante de dette délibérée. Elle est délibérée parce qu'elle est connue et acceptée, mais non documentée comme risque opérationnel dans les systèmes de gouvernance habituels. Le J6 sait que le patch n'est pas déployé ; le COMEX ne le sait pas.

Le quatrième vecteur est humain : l'attrition des compétences analogiques et la dépendance croissante aux systèmes numériques créent une dette de résilience humaine qu'aucune mesure technique ne peut compenser. Quand P4 tombe, ce sont les procédures manuelles exercées qui prennent le relais — ou qui ne le prennent pas.

VECTEUR	MÉCANISME D'ACCUMULATION	PLAQUE CIBLE PRINCIPALE	SIGNAL DE DÉTECTION
Architectural	Choix de conception sous-optimaux non révisés	P1, P2	Audit d'architecture — tous les 3 ans minimum
Procédural	Procédures dégradées non exercées	P2, P3, P5	Taux d'exercice DDIL — indicateur MMP §5.2
Budgétaire	Reports maintenance / patch / remplacement	P1, P2, P4	Âge moyen des composants non patchés par plaque
Humain	Atrophie compétences analogiques	P5	Délai de bascule C2 analogique mesuré en exercice

2.5.2 Comment se résorbe-t-elle : séquence priorisée par plaque

La résorption de la dette numérique n'est pas une opération homogène. Elle doit être séquencée selon la logique du flux orienté : une plaque amont non consolidée rend fragile toute consolidation en aval. Rembourser P4 avant d'avoir consolidé P1 et P2 revient à imperméabiliser le toit d'une maison dont les fondations sont fissurées.

La règle de priorisation découle directement du modèle des cinq plaques. P1 (Connectivité — LDT) est la plaque fondatrice : toutes les autres en dépendent en régime nominal. Sa dette se rembourse en priorité absolue, par redondance multi-vecteurs et durcissement EMP. P2 (Cloud et Edge) est la plaque de traitement : sans edge autonome validé en exercice réel sur 72 heures, le mode décentralisé reste une intention doctrinale. P3 (Données et COP) est la plaque la plus silencieusement vulnérable : sa dette se rembourse par anomaly detection comportementale et horodatage cryptographique des flux. P4 (Applications et IA) nécessite un audit supply chain et un SBOM vivant — toute mise à jour déployée sans sandbox constitue une accumulation de dette de sécurité. P5 (Commandement) se consolide par l'exercice C2 analogique trimestriel et le compartimentage des droits d'accès.

⚠ SÉQUENCE NON NÉGOCIABLE DE RÉSORPTION

P1 → P2 → P3 → P4 → P5. Jamais dans l'autre sens. La logique est celle du flux : si P1 est fragile, toute la chaîne en aval reste exposée quelle que soit la solidité des plaques suivantes. Un état-major qui consolide P4 (Apps/IA) sans avoir atteint le niveau 3 sur P1 construit une forteresse sur du sable numérique.

Exception opérationnelle : P5 peut être consolidée en parallèle de P1 car elle agit comme verrou terminal indépendant du flux nominal. L'exercice C2 analogique ne dépend pas de la solidité de P1 — il est précisément conçu pour fonctionner sans elle.

2.5.3 Le mécanisme de basculement : de la dette latente à la rupture critique

C'est la question centrale que les retours de lecture ont posée avec précision : quel est le mécanisme qui transforme, dans une action donnée, la dette accumulée en tension critique conduisant à la rupture ? La réponse mobilise le concept de marge de résilience résiduelle par plaque — notion heuristique développée dans ce document pour formaliser l'espace entre la solidité effective d'une plaque et son seuil de rupture sous pression adversariale.

Chaque plaque dispose à un instant t d'une marge de résilience résiduelle — la distance entre son état réel de solidité et le seuil de rupture sous sollicitation adversariale. Cette marge se calcule conceptuellement comme la différence entre le niveau MMP effectif de la plaque et le niveau d'intensité de la menace ciblée. Une plaque à niveau 3 peut absorber une menace de niveau 2 sans rupture. Elle ne peut pas absorber une menace de niveau 4.

La dette numérique agit précisément en réduisant silencieusement cette marge. Chaque report de patch, chaque procédure non exercée, chaque architecture non consolidée réduit le niveau MMP effectif d'un ou plusieurs dixièmes. Le piège est que cette érosion est invisible jusqu'au point d'inflexion : la plaque paraît intacte parce qu'aucun incident n'est survenu. L'absence d'incident ne prouve pas la solidité — elle prouve seulement que la trajectoire de menace n'a pas encore trouvé l'alignement optimal.

Le basculement se produit lorsque trois conditions sont réunies simultanément : (1) la marge de résilience résiduelle d'une plaque est tombée en dessous du seuil critique — la plaque est fragilisée mais non rompue ; (2) une perturbation nominale — pas nécessairement une attaque ciblée — crée une sollicitation localisée ; (3) cette sollicitation excède la marge résiduelle. À ce moment, une perturbation qui aurait été absorbée sans incident dix-huit mois plus tôt produit une rupture opérationnelle

réelle. C'est le mécanisme exact que SolarWinds a exploité sur P4 : la supply chain compromise n'a pas créé la vulnérabilité — elle a trouvé une plaque dont la marge résiduelle avait été réduite à zéro par des années de dépendances non auditées.

LA LOI DU POINT D'INFLEXION

La dette numérique ne produit pas de rupture linéaire. Elle produit une rupture à seuil. Le système résiste — résiste — résiste — puis bascule brutalement lorsque la marge résiduelle d'une plaque est franchie. Cette non-linéarité est la raison pour laquelle les organisations sous-estiment structurellement leur exposition : elles extrapolent de l'absence d'incident passé une solidité future qui n'existe plus.

Implication opérationnelle directe : le bon indicateur n'est pas 'avons-nous subi un incident ?' mais 'quelle est la marge résiduelle de chaque plaque aujourd'hui ?' C'est précisément ce que le MMP (§5.1) mesure — et pourquoi il doit être renseigné trimestriellement, pas annuellement.

La question complémentaire posée par le lecteur — comment éviter de créer de la dette dès la conception — appelle une réponse doctrinale : l'intégration du MMP comme critère d'acceptation des systèmes en acquisition. Tout système entrant dans l'écosystème numérique militaire devrait être livré avec un niveau MMP certifié par plaque, une SBOM complète, et un plan de maintenance documenté sur dix ans. C'est la condition pour que la dette ne soit pas créée structurellement au moment de la mise en service.

SECTION III — LES QUATRE SCENARIOS DE DEFAILLANCE

Les scénarios de défaillance s'analysent comme des trajectoires de menace traversant les cinq plaques. Leur classification selon le point d'entrée, la vitesse de propagation et le profil de détection détermine la stratégie de mitigation.

3.1 APT étatique : la pénétration multi-plaques silencieuse

Les APT étatiques¹⁴ exploitent l'alignement de trous par persistance longue durée — implantation silencieuse de plusieurs mois avant activation. Le vecteur le plus redoutable est l'attaque par supply chain logicielle : une mise à jour légitime corrompt d'un composant de confiance. L'opération SolarWinds (2020)¹⁵ a compromis 18 000 organisations dont le Pentagone via une mise à jour de l'outil Orion, contournant l'intégralité des défenses P1 à P3 par définition — le vecteur d'entrée est transporté légitimement sur P1, traité normalement par P2 et P3, avant d'installer son implant dans P4. La seule barrière efficace contre ce vecteur est en amont du flux : Software Bill of Materials (SBOM), vérification comportementale post-déploiement, sandbox d'isolation des mises à jour critiques.

PLAQUE FRANCHIE	MÉCANISME DANS UN APT TYPE	TROU EXPLOITÉ	BARRIÈRE QUI AURAIT BLOQUÉ
P1 — Connectivité	Compromission d'un équipement réseau via zero-day ou identifiant VPN légitime	Absence de surveillance comportementale des connexions, pas d'authentification forte	Zero Trust Network Access + MFA + détection d'anomalies de flux

¹⁴Mandiant Intelligence, APT41: A Dual Espionage and Cyber Attack Operation, 2019. CISA Alert AA22-277A, octobre 2022. SGDSN / ANSSI, Panorama de la cybermenace 2023, Paris, 2024. IRSEM, « Les APT étatiques ciblant les systèmes de défense occidentaux », Étude 95, 2022. Verizon, DBIR 2023.

¹⁵Microsoft MSTIC, Solorigate / SolarWinds Compromise — Technical Analysis, décembre 2020. L'opération a compromis 18 000 organisations via une mise à jour légitime corrompue de l'outil Orion, contournant l'intégralité des défenses périmétriques. CISA, SolarWinds Guidance AA21-008A, 2021. Ce vecteur illustre la limite fondamentale des défenses orientées périmètre : une supply chain logicielle corrompue entre dans le système par définition comme une entité de confiance.

P2 — Cloud/Edge	Mouvement latéral exploitant la segmentation insuffisante	Architecture plate, absence d'isolation entre segments	Micro-segmentation + principe du moindre privilège
P3 — Données/COP	Manipulation silencieuse des données de ciblage ou du COP	Absence d'intégrité cryptographique des données, pas d'audit de cohérence	Signature cryptographique des flux de données + anomaly detection
P4 — Apps/IA	Installation d'un implant via supply chain ou mouvement latéral	Absence de SBOM, dépendances non auditées, droits d'admin non contrôlés	SBOM obligatoire + audit comportemental post-déploiement + moindre privilège
P5 — Commandement	Exfiltration d'ordres ou manipulation de recommandations IA pour induire des décisions erronées	Confiance excessive dans les recommandations IA, absence de vérification croisée	Culture de questionnement systématique + double vérification sur décisions critiques

👤 PROFIL APT : INSIDIEUX / DÉTECTION TARDIVE / IMPACT TERMINAL SUR P5
Point d'entrée : P1 ou P4 (supply chain). Vitesse : lente (semaines à mois). Profil de détection : quasi-nul sans surveillance comportementale dédiée. Impact terminal : compromission P5 — la force ne sait pas qu'elle est aveugle ou manipulée.

3.2 DDIL et EMP : deux ruptures de P1 aux mitigations fondamentalement distinctes

Il est doctrinalement incorrect de traiter DDIL et EMP comme un scénario unique. Ce sont deux familles de menaces distinctes dont les mécanismes et les mitigations ne sont pas les mêmes.

Les environnements DDIL (Degraded, Disconnected, Intermittent, Limited) et le brouillage des LDT constituent des disruptions fonctionnelles de P1 : les équipements physiques restent intacts, mais P1 cesse de transporter des données utilisables. La rupture est potentiellement réversible — changer de fréquence, basculer sur un vecteur redondant, attendre la fin du brouillage. La mitigation est

architecturale : redondance multi-vecteurs, autonomie edge temporaire, procédures de dégradation.

L'impulsion électromagnétique — HEMP (High-altitude EMP, d'origine nucléaire) ou NNEMP (Non-Nuclear EMP, d'origine conventionnelle) — est une destruction physique irréversible des composants électroniques non durcis sur une zone géographique définie. P1 n'est pas dégradée fonctionnellement ; elle est détruite physiquement. Une architecture edge-first brillamment conçue mais non durcie électromagnétiquement ne constitue pas une barrière contre cette menace. La mitigation est physique : blindage Faraday, composants milspec EMP-résistants, équipements de remplacement pré-positionnés hors zone de frappe.

DDIL vs EMP — DEUX PRESCRIPTIONS DE RÉSILIENCE DISTINCTES

DDIL / brouillage : rupture fonctionnelle réversible → mitigation = redondance vecteurs + autonomie edge + procédures dégradées. EMP : destruction physique irréversible → mitigation = durcissement électromagnétique + pré-positionnement matériel hors zone. Traiter ces deux menaces dans une même prescription de résilience produit une doctrine partiellement fautive — et laisse la force sans barrière réelle contre l'EMP.

3.3 Défaillance cloud souverain : P2 effondrée, P1 intacte

La panne ou l'attaque sur l'infrastructure cloud centrale (P2) coupe le traitement et le stockage pour toutes les applications dépendantes — sans toucher P1. Le COP se fige, les applications C2 perdent leurs données, la synchronisation inter-unités s'arrête. Contrairement au scénario DDIL, la connectivité est disponible mais le service qu'elle transporte est vide. La barrière est le même edge computing autonome — nourri cette fois par la LDT disponible. P5 avec ses procédures analogiques devient la barrière terminale.

PROFIL P2 : DESTRUCTEUR / DÉTECTION IMMÉDIATE / REMONTÉE LENTE

Point d'entrée : P2 (cloud central ou edge ciblé). Vitesse : rapide (ransomware) à immédiate (sabotage). Profil de détection : visible — la panne est franche. Durée de remontée : variable selon redondance edge (72h si P2 § MMP niveau 4). Impact si edge non validé : effondrement total du flux nominal — chaque application, chaque IA, chaque COP tombe simultanément. P1 intacte mais inutile : les connexions arrivent, rien ne les traite.

3.4 Corruption algorithmique : le poison silencieux dans P3 qui traverse P4

L'empoisonnement de données¹⁶ et les attaques adversariales ciblent P3 en injectant des données falsifiées dans les flux d'entraînement ou d'inférence des modèles IA. La corruption se propage vers P4 qui traite fidèlement des données viciées, produisant des recommandations de ciblage biaisées. Ce scénario est le seul dont le profil de détection est quasi-nul sans surveillance comportementale dédiée — et dont l'impact peut engager la responsabilité juridique du commandement au regard du DIH¹⁷ indépendamment de sa cause technique. La barrière terminale est P5 : un commandant qui accepte aveuglément toute recommandation IA sans vérification croisée a remplacé une plaque par une passoire.



PROFIL : INSIDIEUX / DÉTECTION QUASI-NULLE / RESPONSABILITÉ COMMANDEMENT

Point d'entrée : P3. Traversée sans alarme : P3 → P4. Barrière terminale requise : P5 (commandement humain critique). Impact si P5 atrophiée : décision erronée à conséquences opérationnelles et juridiques sans signal d'alerte. C'est le seul scénario où l'atrophie cognitive de P5 (confiance aveugle en l'IA) transforme une vulnérabilité technique en violation potentielle du Droit International Humanitaire.

¹⁶Biggio B. & Roli F., « Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning », Pattern Recognition, Vol. 84, 2018. CNAS, « Adversarial Machine Learning in Defense Applications », 2023. IRSEM, « IA et sécurité des systèmes de décision militaires », Étude 121, 2023. ANSSI, Recommandations de sécurité pour un système d'IA, Guide ANSSI-PA-086, 2024.

¹⁷Johnson J., AI and the Future of Warfighting, Georgetown University Press, 2023. COMUN, Group of Governmental Experts on LAWS, Documents CCW/GGE.2/2023/1-5, Genève, 2023. IRSEM, « LAWS : enjeux juridiques, éthiques et opérationnels pour la France », Étude 72, 2021. ICRC, Autonomous Weapon Systems: Implications of Increasing Autonomy, Genève, 2022. FRS, « Gouvernance des LAWS : entre efficacité opérationnelle et contrainte juridique internationale », Note 28/2022.

SECTION IV — TROIS CRISES RELUES PAR LE MODELE DE REASON

4.1 Stuxnet (2010) : anatomie d'un alignement parfait

L'opération Olympic Games — dont Stuxnet est l'outil documenté —¹⁸ est la démonstration empirique la plus complète du modèle de Reason. Sa trajectoire a traversé les installations de Natanz en contournant un réseau air-gappé et a produit la destruction d'un millier de centrifugeuses IR-1 (les estimations publiées varient entre 800 et 1 200 sur un parc d'environ 9 000 unités) — un effet cinétique obtenu par voie purement numérique.

La table ci-après illustre l'anatomie de l'alignement. Note méthodologique : les trous P3a et P3b correspondent à deux sous-composantes distinctes de P3 dans ce contexte industriel spécifique — les données capteurs physiques (P3a) et la couche de présentation opérateur / COP (P3b). Cette granularité démontre que P3 peut présenter des surfaces d'attaque internes séparables, ce qui justifie une surveillance comportementale indépendante sur chacune des deux couches dans tout système à haute criticité.

PLAQUE	MÉCANISME	TROU EXPLOITÉ	BARRIÈRE QUI AURAIT BLOQUÉ
P1 — Connectivité	Air gap contourné par infection USB via sous-traitants Siemens	Absence de politique de contrôle des médias amovibles dans la supply chain matérielle	UEBA (User and Entity Behavior Analytics) + contrôle physique des médias
P2 — Cloud (SCADA)	Injection dans WinCC/Step7 — prise de contrôle des automates S7-315	SCADA non segmenté de l'IT — architecture plate sans isolation OT/IT	Micro-segmentation OT/IT + réseau unidirectionnel (diode réseau)

¹⁸Langner R., « Stuxnet: Dissecting a Cyberweapon », IEEE Security & Privacy, Vol. 9/3, 2011. ESET, Win32/Stuxnet Analysis, 2010. Lindsay J.R., « Stuxnet and the Limits of Cyber Warfare », Security Studies, Vol. 22/3, 2013. IRSEM, « Opérations cyber offensives : doctrine et retours d'expérience », Étude 68, 2021. Rid T., Cyber War Will Not Take Place, Hurst & Co., 2013. Les estimations du nombre de centrifugeuses détruites varient entre 800 et 1 200 selon les sources (sur un parc d'environ 9 000 unités) — Albright D. et al., ISIS Report on the Natanz Enrichment Facility, 2011.

P3a — Données capteurs	Manipulation des données de pression transmises aux opérateurs	Absence de validation croisée capteur / état physique réel mesurable indépendamment	Capteurs physiques redondants avec canal de validation indépendant
P3b — COP opérateurs	Rejeu des données nominales pendant les cycles de sabotage — COP industriel falsifié	Absence d'anomaly detection comportementale sur les flux de process	Détection d'anomalies comportementales sur les séquences de processus industriel
P4 — Logique de contrôle	Reprogrammation des vitesses de rotation au-delà du seuil de rupture mécanique	Logique de sécurité non redondante, pas de validation physique indépendante des commandes	Validation physique indépendante des commandes sur les équipements critiques
P5 — Commandement	Opérateurs voyant des données nominales pendant la destruction physique effective	Culture de la confiance absolue dans les capteurs — aucun réflexe de vérification croisée	Formation aux anomalies silencieuses + procédures de vérification physique périodique

Leçon de Reason : Stuxnet n'est pas un exploit technologique exceptionnel — c'est la démonstration qu'un réseau air-gappé réputé inviolable ne l'est que si toutes ses plaques sont solides simultanément. Chaque trou était tolérable isolément. Alignés, ils ont transformé une installation nucléaire sécurisée en système totalement compromis. La destruction physique d'infrastructure a été obtenue sans jamais pénétrer physiquement l'installation.

4.2 Ukraine (2022–2024) : le premier théâtre de résilience numérique en haute intensité

Le conflit ukrainien constitue le premier théâtre de guerre documenté où toutes les plaques de Reason ont été simultanément ciblées et testées à grande échelle.¹⁹²⁰ Il offre le corpus empirique le plus dense sur la validité opérationnelle du modèle.

Le 24 février 2022, à H-1 de l'invasion terrestre, la frappe cyber russe AcidRain cible P1 en neutralisant les modems Viasat KA-SAT — satellite commercial utilisé par des entités gouvernementales ukrainiennes et des partenaires OTAN, non un système SATCOM militaire classifié. L'effet est significatif : plusieurs milliers de terminaux perdent leur liaison. La trajectoire de Reason s'engage. Elle échoue précisément pour la raison que le modèle prédit : la redondance inter-vecteurs — SpaceX activant des terminaux Starlink dans les jours suivants, terminaux qui ne dépendent d'aucune infrastructure sol en zone de conflit — reconstruit P1 par un chemin entièrement indépendant. La solidité architecturale de P2 (edge computing ukrainien décentralisé et géographiquement dispersé) complète la résilience.

Sur P3 (données/COP), les opérations de brouillage GPS et de spoofing ont tenté de corrompre le COP ukrainien systématiquement. La réponse — application COP Delta décentralisée, vérification terrain humaine, fusion multi-sources — illustre le mode décentralisé en temps réel : lorsque P3 est compromise, P5 (commandement humain avec culture de vérification croisée) compense. La force qui a exercé le commandement par mission a maintenu son efficacité malgré la dégradation. Celle qui ne l'avait pas exercé a subi une dégradation capacitaire disproportionnée.

¹⁹RUSI, *Ukraine's Cyber Experience — Lessons for Western Defence*, Occasional Paper, 2023. Watling J. & Reynolds N., « Manoeuvre in Russian Tactical Operations », RUSI Occasional Paper, 2023. IISS, « Russia's Military Modernisation and the Ukraine War », Strategic Survey 2023. IFRI, « La guerre en Ukraine et la transformation du champ de bataille numérique », Note du Centre des Études de Sécurité, 2023. Note sur Viasat : KA-SAT est un satellite commercial utilisé par des entités gouvernementales et des partenaires OTAN, non un système SATCOM militaire classifié — la neutralisation a dégradé une fraction de P1 sans la neutraliser complètement.

²⁰ISW (Institute for the Study of War), *Russian Offensive Campaign Assessment, 2022–2024*. CNAS, « Lessons from Ukraine for Multi-Domain Competition », 2023. Brookings Institution, « The Ukraine War's Implications for Future Conflict », 2023. Charap S. & Darden K. (RAND), « Russia and Ukraine: Theories of Victory », *Survival*, IISS, Vol. 65/3, 2023.

4.3 Israël-Iran (2010–2024) : la guerre permanente des plaques

Le conflit numérique prolongé entre Israël et l'Iran²¹ constitue la démonstration la plus durable de stratégies de Reason offensives et défensives en compétition continue. L'Iran conduit deux types d'opérations distincts : contre Israël directement (APT33/HOLMIUM, ciblage infrastructures critiques, opérations de commandement) et contre les alliés régionaux — l'attaque Shamoon/DistTrack d'août 2012 ciblait Saudi Aramco (35 000 postes détruits en quelques heures), entreprise saoudienne, dans le cadre de la stratégie iranienne de déstabilisation régionale et non d'une opération directe contre Israël. La leçon de Reason est identique dans les deux cas : l'Iran exploite méthodiquement les alignements de trous dans les plaques adverses par persistance et adaptation.

PLAQUE	CAMPAGNE DOCUMENTÉE	TROU EXPLOITÉ	BARRIÈRE QUI AURAIT BLOQUÉ
P1 – Connectivité	Opérations Charming Kitten / APT35 (IRGC, 2019–2023) : spear-phishing ciblant des fournisseurs de systèmes de communication israéliens — compromission de P1 par la chaîne logistique des équipements réseau, sans attaque directe frontale	Absence d'authentification forte sur équipements réseau, firmware non vérifié	Authentification forte + vérification d'intégrité firmware + segmentation entrée/sortie
P2 – Cloud/Edge	Wiper DistTrack/Shamoon (2012, 2018) : destruction MBR sur 35 000 postes Aramco en quelques heures — P2 entièrement détruite sur le périmètre ciblé	Architecture plate, absence d'isolation entre segments bureautique et opérationnel	Micro-segmentation + copies offline + procédures de reprise sans P2 centrale

²¹ClearSky, Fox Kitten Campaign, 2020. Checkpoint Research, Domestic Kitten / APT-C-50, 2018. The Economist, « The Art of Cyberwar: How Iran and Israel Trade Blows in the Shadows », 24 avril 2021. FRS, « Cyberspace et conflits hybrides : le cas du Moyen-Orient », Recherches & Documents 07/2022. IRSEM, « La guerre informationnelle et cyber iranienne », Étude 82, 2022. INSS, « Iran's Cyber Strategy », Insight 1712, 2023. Note contextuelle : l'attaque Shamoon/DistTrack d'août 2012 (35 000 postes détruits) ciblait Saudi Aramco — entreprise saoudienne — dans le cadre de la stratégie iranienne de déstabilisation régionale, non d'une opération directe contre Israël.

P3 — Données/COP	Opérations de manipulation des systèmes SCADA industriels (Predatory Sparrow, 2022) : données de process falsifiées avant l'arrêt forcé de systèmes de sécurité	Absence d'anomaly detection sur les flux de données process — confiance par défaut dans les capteurs	Anomaly detection comportementale + canal de validation physique indépendant
P4 — Apps/IA	Implants APT33/HOLMIUM dans la supply chain logicielle de l'industrie aérospatiale et de défense israélienne (CERT-IL, 2023)	Dépendances non auditées, absence de SBOM, sandbox de déploiement inexistante	SBOM vivante + red-team semestriel + sandbox obligatoire sur toute mise à jour
P5 — Commandement	Campagnes de désinformation et deepfakes visant à induire des décisions erronées au niveau du commandement politique et militaire (INSS, 2023)	Confiance excessive dans les flux d'information numériques, absence de vérification croisée sur décisions critiques	Culture de questionnement systématique + double vérification sur décisions irréversibles

Tableau 4.3 — Anatomie des alignements de trous dans le conflit numérique Israël-Iran. Sources : CERT-IL 2023 ; INSS Insight 1712 ; ClearSky 2020 ; IRSEM Étude 82 ; Mandiant APT33.

La leçon stratégique est triple. Premièrement, dans un conflit cyber permanent, c'est l'adversaire qui maintient la pression offensive sur les trous adverses tout en bouchant méthodiquement les siens qui domine structurellement dans le temps. Deuxièmement, les effets d'un alignement de trous sur une infrastructure non-militaire (Aramco) sont comparables à une frappe cinétique — ce qui démontre que la protection des infrastructures numériques de soutien (opérateurs télécoms, data centers industriels, logistique) relève de la sécurité nationale au même titre que la protection des infrastructures militaires directes. Troisièmement, l'absence de retour à un état de paix cyber remet en cause la notion même de paix dans le domaine numérique : les plaques adverses sont attaquées en permanence, y compris en dehors de tout conflit armé déclaré.

✘ LEÇON STRATÉGIQUE — GUERRE PERMANENTE DES PLAQUES

Dans un conflit cyber permanent, la paix n'existe pas dans le domaine numérique — seulement des phases de haute et basse intensité offensive. La supériorité numérique n'est pas un état à atteindre : c'est une discipline à maintenir. La force qui bouchera ses trous plus vite que son adversaire ne les ouvre dominera structurellement — indépendamment de sa supériorité cinétique. C'est la reformulation numérique de la loi de Lanchester appliquée aux plaques.

SECTION V — GOUVERNANCE ET MODELE DE MATURITE DES PLAQUES

5.1 Le Modèle de Maturité des Plaques (MMP)

En s'inspirant du CMMC 2.0²² et du concept d'anti-fragilité de Taleb²³ — la propriété d'un système qui se renforce sous perturbation —, le Modèle de Maturité des Plaques propose cinq niveaux de solidité pour chacune des cinq plaques. Sa conception est délibérément lisible à deux niveaux : un général d'armée doit pouvoir en saisir les implications en cinq minutes ; le J6 doit pouvoir le renseigner avec des indicateurs mesurables.

NIVEAU	DÉSIGNATION	DESCRIPTION OPÉRATIONNELLE	SIGNAL D'ALERTE
1 – INITIAL	Plaque absente	Aucune mesure identifiée. Vulnérabilité ouverte non documentée. Dette maximale.	Plaque jamais auditée
2 – RÉPÉTÉ	Plaque mince	Mesures ponctuelles, dépendantes de l'initiative individuelle. Non reproductibles.	Procédures non documentées
3 – DÉFINI	Plaque documentée	Politique formalisée, procédures écrites, formation initiale réalisée.	Formation sans exercice réel
4 – GÉRÉ	Plaque mesurée	Indicateurs mesurés trimestriellement, exercices de dégradation réels, propriétaire identifié.	Exercice > 6 mois
5 – OPTIMISÉ / ANTI-FRAGILE	Plaque renforcée	Révision continue post-incident. Redondance validée. La plaque se renforce sous perturbation.	Budget insuffisant / atrophie

²²CMMI Institute, CMMC 2.0 (Cybersecurity Maturity Model Certification), US DoD, 2022. ISO/IEC 27001:2022, Systèmes de management de la sécurité de l'information. Le Modèle de Maturité des Plaques (MMP) proposé ici s'en inspire tout en l'adaptant à la granularité opérationnelle militaire française.

²³Taleb N.N., Antifragile: Things That Gain from Disorder, Random House, 2012. L'anti-fragilité — propriété d'un système qui se renforce sous perturbation — est l'horizon cible du modèle de maturité des plaques : niveau 5 « optimisé » correspond à une plaque anti-fragile, non seulement résiliente. Pour les applications militaires : RAND, « Antifragility in Defense Systems Design », PE-A1975, 2023.

Objectif minimum non négociable : niveau 3 pour toutes les plaques. Cible opérationnel : niveau 4 pour P1 et P5. Niveau 5 pour P1 des états-majors de niveau opératif et stratégique.

5.2 Indicateurs, seuils et propriétaires — la gouvernance des trous

PLAQUE	INDICATEUR PRIMAIRE (SOURCE DOCTRINALE)	SEUIL D'ALERTE	PROPRIÉTAIRE	ARBITRE EN CAS DE CONFLIT
P1 — Connectivité	Nb de chemins LDT physiquement indépendants vers C2 en mode DDIL total (AJP-6.0)	< 2 = CRITIQUE	J6 / CND / CEMA	CEMAT — rapport mensuel
P2 — Cloud/Edge	Durée d'autonomie edge validée en exercice réel sans cloud central (seuil dérivé des plans opérationnels force)	< 72h = MAJEUR	J6 / DGA-MI	J6 — revue trimestrielle
P3 — Données/COP	Âge moyen données COP lors du dernier exercice DDIL complet (dérivé AJP-2.1 — fraîcheur renseignement)	> 4h HI / > 24h stabilisation = SIGNIFICATIF	J3 (contenu)	J3 — arbitre sur J6 pour toute décision P3

P4 — Apps/IA	Mois depuis dernier red-team adversarial, test data poisoning et audit SBOM complet	> 6 mois = MAJEUR	DGA / SIC / Comité IA	DGA — revue biannuelle
P5 — Commandement	Mois depuis dernier exercice C2 complet sans aucun appui numérique + taux d'incidents signalés sans sanction	> 3 mois exercice / taux = 0 = CRITIQUE	État-major opérationnel	CEMAT — revue annuelle

Principe fondamental : une plaque sans propriétaire identifié est une plaque sans maintenance — sa dette augmente silencieusement. Corollaire immédiat : une propriété partagée entre deux fonctions sans arbitre désigné est une non-propriété. Sur P3, J3 est le propriétaire du contenu et J6 le propriétaire du transport — J3 dispose d'une autorité formalisée sur J6 en cas de conflit de priorité. Sans cet arbitrage explicite, P3 sera la plaque dont personne ne se sentira pleinement responsable, reproduisant précisément la faille que le modèle cherche à éradiquer.

SECTION VI — TRANSFORMER L'ORGANISATION : UNE STRATEGIE EN TROIS LENTILLES

6.1 Le diagnostic préalable : nommer ce qui bloque vraiment

Roberto M. Fernandez (MIT Sloan, 2023) formule le problème avec une brutalité salutaire : « *Organizational Insanity : faire la même chose encore et encore en espérant un résultat différent.* » La quasi-totalité des plans de transformation numérique échouent non pas parce que l'architecture est mauvaise — la lentille BLEUE — mais parce que les dimensions politique (ROUGE) et culturelle (BLANCHE) ont été ignorées. **BLEU = 15 % du problème seulement.** Traiter un problème ROUGE avec des outils BLEUS — réorganiser ce qui est en réalité un conflit de territoire — est la faute de diagnostic la plus répandue dans les états-majors de transformation.

Trois résistances structurelles sont documentées comme principaux freins dans les rapports parlementaires de référence sur la transformation numérique des Armées françaises. Le **biais de normalité** : l'absence d'incident est interprétée comme preuve de solidité des plaques, alors que Reason démontre l'inverse. Le **cloisonnement J1-J9** : la structure organique militaire favorise une analyse du risque par domaine, alors que les accidents traversent les silos par définition. La **culture de la perfection technique** : les accidents systémiques ne sont causés par personne en particulier — ils émergent de l'interaction de défaillances latentes distribuées, ce qui heurte la culture de responsabilité individuelle forte des Armées et crée un puissant biais de sous-déclaration. À ces trois résistances documentées s'ajoute une quatrième, moins visible : l'illusion de la convergence numérique. La M2MC crée une pression vers plus d'intégration — opérationnellement désirable mais architecturalement risquée si cette convergence se fait sans renforcement simultané des plaques.

Le corollaire pratique est exigeant : *Unlearning is harder than learning* (Fernandez). Dans les Armées, certaines habitudes ont quarante ans et sont adossées à des identités professionnelles solides. La transformation ne commence pas par une décision technique — elle commence par un diagnostic honnête de ce qui résiste, et pourquoi.

6.2 Les trois lentilles : voir l'organisation telle qu'elle est

Fernandez fonde son protocole sur trois lentilles qui s'appliquent simultanément à chaque obstacle de transformation. La séquence prescrite est néanmoins précise : commencer par BLEU (même 15 minutes pour clarifier le quoi), cartographier ROUGE avant d'agir (qui perd quoi ?), sonder BLANC en parallèle (qu'est-ce qu'on fait depuis toujours sans se demander pourquoi ?), puis croiser les trois sur chaque résistance identifiée. Comme le souligne John Seeley Brown (PARC Xerox) : « *Au lieu de verser de la connaissance dans les têtes, aidez les gens à se forger de nouvelles paires de lunettes pour voir le monde différemment.* » Le diagnostic n'est pas une photographie — c'est un film. Il faut le relancer après chaque victoire rapide.

B BLEUE Strategic Design	R ROUGE Politique	W BLANCHE Culturelle
<p>Question clé Quel problème précis cette transformation résout-elle ? Quels processus J6, J3, J2 doivent être redessinés plaque par plaque ?</p> <p>Action prioritaire Cartographier les processus impactés par plaque. Désigner les propriétaires MMP. Définir les KPI. Produire le plan à 90 jours.</p> <p>Piège <i>Imposer l'architecture sans toucher aux habitudes : adoption formelle, usage réel nul. BLEU sans ROUGE ni BLANC = transformation en paperasse.</i></p>	<p>Question clé Qui perd du territoire ? Quel J6 ou commandant voit son expertise relativisée ? Qui a le plus à perdre — et qu'est-ce qu'on peut lui offrir ?</p> <p>Action prioritaire Identifier alliés, opposants, indifférents. Transformer l'opposant en propriétaire — le nommer co-responsable de la plaque qu'il conteste.</p> <p>Piège <i>Ignorer la résistance identitaire. Un opposant non traité deviendra un poison à diffusion lente dans toute la chaîne de commandement.</i></p>	<p>Question clé Qu'est-ce qu'on fait depuis toujours sans se demander pourquoi ? Quelles croyances non questionnées freineront le changement ?</p> <p>Action prioritaire Nommer les habitudes à briser. Créer les rituels de remplacement. Un récit fondateur visible dès la première victoire rapide.</p> <p>Piège <i>Pencil-whipping : cocher les cases sans rien changer. Les habitudes reviennent dès que la pression de la prochaine urgence opérationnelle s'impose.</i></p>

L'avertissement central de Fernandez mérite d'être intégré à tous les documents de conduite du changement des Armées : « *Les idées, aussi brillantes soient-elles, ne changent rien seules.* » L'architecture des cinq plaques est une idée brillante. Elle ne changera rien seule.

Une précision sur le positionnement théorique s'impose. Kotter appartient à ce que certains auteurs qualifient de tradition post-tayloriste de la transformation : séquence pilotée par le haut, leadership visible, gestion du changement comme projet avec début et fin identifiables. Cette tradition présente des limites reconnues dans les organisations distribuées et à forte culture d'expertise autonome. C'est précisément pour corriger ce déficit que les trois lentilles de Fernandez (MIT Sloan, 2023) constituent le cadre théorique primaire de cette section — Kotter n'y intervient qu'en §6.4 comme illustration opérationnelle de l'ordre dans lequel ces lentilles s'activent. La lentille bleue (design stratégique) correspond au Kotter classique. La lentille rouge (politique) et la lentille blanche (culturelle) introduisent les dimensions que Kotter sous-traite : les jeux de pouvoir, les identités professionnelles, les rituels organisationnels. Ce n'est pas un correctif cosmétique — c'est la reconnaissance que 85 % des obstacles à la transformation numérique militaire ne sont pas dans la lentille bleue.

6.3 Profil de résistance de chaque plaque

Chaque plaque a un profil de résistance distinct selon les trois lentilles. Traiter P1 avec les outils qui fonctionnent sur P5 est une erreur de diagnostic aussi grave que confondre une rupture physique et une défaillance fonctionnelle. Le tableau suivant constitue la matrice de diagnostic préalable à tout plan d'action.

Plaque	Domaine	B — Design	R — Politique	W — Culture
P1	Connectivité	Pas de norme commune de redondance inter-armées. LDT et réseaux HF en silos étanches.	Les opérateurs radio tiennent leur domaine comme un territoire. La LDT est une culture.	On a toujours fonctionné sans redondance formalisée — les opérateurs savent improviser.
	Cloud & Edge	Architecture cloud souverain non définie transversalement. Chaque armée a son edge, aucun interopérable.	Les DSI d'armée protègent leurs budgets respectifs. Une plateforme commune menace leurs périmètres.	Le cloud souverain, c'est pour les civils. Nous, on a des systèmes durcis.
P3	Données	COP fragmentées par armée. Absence de fusion en temps réel. Formats non standardisés.	Le J2 détient la donnée renseignement. Le J3 détient la donnée ops. Partager = perdre l'influence.	If only HP knew what HP knows (Platt, 1999). Le silo est une identité professionnelle.
P4	Apps & IA	Cycle d'acquisition DGA incompatible avec l'itération logicielle. le cycle DGA peut exiger plusieurs années de certification pour valider ce que l'adversaire déploie en 6 semaines.	Les contractants historiques ont des contrats de maintenance qui désincentivent l'innovation architecturale.	Une IA non certifiée est un risque opérationnel. — utilisé pour bloquer toute expérimentation préalable.
P5	Commandement	Pas de processus de bascule formalisé entre mode augmenté et mode dégradé. P5 absorbe la complexité des plaques sous-jacentes.	Renforcer P5 signifie reconnaître ses failles — ce qu'aucun commandant ne fait spontanément dans une culture de responsabilité forte.	Battleship Admirals (Fernandez) : excellence forgée dans les outils d'hier, résistance aux outils de demain par identité, non par mauvaise volonté.

6.4 Les trois lentilles en action : la séquence de Kotter comme illustration opérationnelle

Les travaux de Fernandez posent le cadre — les trois lentilles définissent comment voir les obstacles. Il reste à répondre à la question opérationnelle : dans quelle séquence agir ? C'est ici qu'intervient la contribution de Kotter. Sa séquence de huit étapes (Leading Change, 1996 ; XLR8, 2014), fondée sur l'analyse systématique de plus de cent organisations en transformation, constitue une carte de navigation éprouvée — non pas une théorie concurrente de Fernandez, mais une illustration opérationnelle de l'ordre dans lequel les

lentilles s'activent. La lecture croisée ci-dessous montre que chaque étape de Kotter mobilise une lentille dominante ; son échec s'explique presque toujours par l'ignorance de cette lentille. C'est Fernandez qui explique pourquoi chaque étape résiste ; c'est Kotter qui dit dans quel ordre les affronter.

#	Étape	Lentille	Traduction concrète — Armées	Risque d'échec spécifique
1	Créer l'urgence	B	Montrer en COMEX que l'adversaire planifie 10× plus vite. Présenter l'audit de dette numérique comme un état médical — pas une accusation. Les données OTAN 2024 sur les délais de décision adversariaux sont ici l'outil rhétorique décisif.	<i>Sans urgence visible, aucune énergie pour changer. Le J6 qui présente des vulnérabilités sans données adversariales sera perçu comme alarmiste — et ignoré.</i>
2	Former la coalition	R	Identifier les champions par plaque : J6 sur P1-P2, J2 sur P3, ingénieur DGA sur P4, officier général sur P5. Inclure des sceptiques convertis — une coalition de convaincus seuls n'a aucune crédibilité ROUGE.	<i>Coalition trop homogène = blocage à la première résistance transverse. Le champion unique sans réseau politique n'a aucun levier quand le budget est disputé.</i>
3	Vision claire	B	Chaque plaque a un propriétaire nommé, un niveau MMP mesuré, un plan de résilience validé en COMEX. Une vision chiffrée, non une aspiration. Le modèle des cinq plaques est la vision — pas un outil parmi d'autres.	<i>Vision floue = chaque silo interprète à sa façon. Un J6 qui dit numériser sans définir les cinq plaques laisse ses interlocuteurs définir à sa place.</i>
4	Communiquer ×10	W	Récit fondateur : l'exercice X a révélé que P1 et P3 étaient alignées — la COP était aveugle pendant 4h sans que personne le sache. Répéter en revue de commandement, en formation EMS, dans les évaluations annuelles.	<i>Message technique non traduit en conséquences opérationnelles = message ignoré. Les Armées ne croient pas aux architectures — elles croient aux récits d'incidents.</i>
5	Lever les obstacles	R	Le commandant qui refuse d'allouer du temps de formation numérique : le sponsor ROUGE intervient pour redistribuer les decision rights. L'opposant identifié se voit offrir un rôle — propriétaire d'une plaque, pas ennemi.	<i>Obstacles laissés en place = coalition démoralisée en 90 jours. L'opposition identitaire ne se combat pas avec des arguments techniques.</i>
6	Victoires rapides	B	Premier cas d'usage mesurable sous 30 jours : réduction du temps SITREP de 45 min à 8 min, vérification humaine documentée, KPI visible célébré publiquement. Les POC sans livraison réelle ne comptent pas.	<i>Pas de victoire dans les 90 premiers jours = la résistance culturelle reprend le dessus. Les Armées ne croient pas aux démonstrateurs.</i>

7	Consolider	W	Revue semestrielle MMP intégrée au cycle de planification opérationnelle. Formation Reason dans les cursus EMS. Dette numérique comme indicateur de commandement — au même titre que la disponibilité technique des équipements.	<i>70 % des transformations échouent ici. Sans ancrage dans les évaluations, le retour aux anciennes pratiques est garanti dès la prochaine urgence opérationnelle.</i>
8	Ancrer dans la culture	W	Les cinq plaques entrent dans les critères d'évaluation des J6 et DSI, les récits de la formation initiale, le vocabulaire des revues de commandement. Le modèle de Reason devient référence institutionnelle comme le CHIRP en aviation.	<i>Sans ancrage culturel : le modèle reste un rapport de plus. Il faut que le CEMA cite le MMP pour que l'état-major le considère comme sérieux.</i>

L'étape 8 mérite une attention particulière : l'ancrage culturel prend le plus de temps. Kotter parle de cinq à dix ans pour les grandes organisations. Dans les Armées, où les cultures de commandement sont multigénérationnelles et renforcées par la formation initiale, l'horizon réaliste de l'étape 8 est la révision du règlement de service intérieur — pas la fin d'un plan triennal.

6.5 Le Dual Operating System : deux vitesses, un cap

Kotter a théorisé en 2014 le Dual Operating System : faire tourner en parallèle la structure hiérarchique existante — qui continue de fonctionner et ne peut pas s'arrêter — et un **réseau accélérateur de Task Forces numériques** mandatées, légères, pluridisciplinaires, qui livrent au tempo opérationnel. L'un tient le fort. L'autre change le fort. C'est la seule architecture institutionnelle qui permet à une organisation comme le Ministère des Armées de se transformer sans cesser de fonctionner.

<p>SYSTÈME HIÉRARCHIQUE — maintient la mission</p> <p>CND · DSI-Armées · J6 des GBD</p> <p>Assure la continuité opérationnelle des P1–P5. Ne s'arrête pas. Ne se réorganise pas pendant la transformation. Fournit les ressources et le cadre de légitimité institutionnelle.</p>	<p>RÉSEAU ACCÉLÉRATEUR — change le fort</p> <p>5 Task Forces numériques · sponsor 2* minimum · cycles 90 jours</p> <p>Livre des améliorations MMP mesurables par plaque. Équipe pluridisciplinaire (J6, J2, J3, opérateur terrain, DGA). Droit à l'erreur documenté. Règles d'engagement explicites avant déploiement.</p>
--	---

La condition de survie du réseau accélérateur est constante dans tous les cas documentés par Kotter : un parrain de haut commandement qui reste en poste au-delà des rotations normales et qui protège personnellement les Task Forces de la réabsorption hiérarchique. Sans ce parrain, le réseau disparaît dans les six premiers mois — absorbé par les urgences opérationnelles du quotidien.

6.6 Calibrage réaliste : phase d'amorçage vs transformation complète

La question opérationnelle n'est pas « avons-nous terminé la transformation ? » Elle est : *le retour en arrière est-il devenu plus coûteux que l'avancée ?* Si oui, la transformation est sur rails. Si non, elle n'a pas commencé. Une **phase d'amorçage** — dont la durée doit être fixée selon les capacités réelles de l'organisation et non selon un calendrier idéal — a un objectif précis : verrouiller la trajectoire de manière irréversible. La transformation complète — culturelle, architecturale, doctrinale — prend une décennie. Mais sans cet amorçage, la décennie ne commence jamais.

CE QUE LA PHASE D'AMORÇAGE PEUT PRODUIRE	CE QUI REQUIERT UN HORIZON DE 7 À 10 ANS
<ul style="list-style-type: none"> ✓ Imposer le référentiel des cinq plaques comme vocabulaire commun de tous les briefings J6 ✓ Réaliser l'audit de dette numérique et le présenter en COMEX ✓ Nommer cinq propriétaires de plaques inscrits dans les fiches de poste ✓ Lancer la migration PQC sur les flux P1 les plus critiques ✓ Former une génération d'officiers supérieurs au modèle de Reason ✓ Créer le cadre de gouvernance MMP et le premier rapport annuel ✓ Rendre le retour au modèle ancien institutionnellement coûteux 	<ul style="list-style-type: none"> → Déployer le référentiel sur l'ensemble des systèmes d'information → Résorber la dette numérique accumulée sur dix ans → Terminer la migration PQC sur l'ensemble des flux classifiés → Changer la culture institutionnelle du commandement → Atteindre le niveau 4-5 MMP sur toutes les plaques → Résoudre la tension M2MC / résilience décentralisée → Transformer des Battleship Admirals qui n'ont pas choisi de l'être

Cette distinction n'est pas un aveu d'échec : c'est l'honnêteté intellectuelle que les organisations de haute fiabilité pratiquent. Un plan qui promet plus que ce qu'une phase d'amorçage peut produire génère deux effets toxiques : la désillusion qui tue les initiatives suivantes, et le pencil-whipping qui transforme les cases cochées en simulacre de changement.

6.7 Les trois engagements non déléguables du haut commandement

Les cinq obstacles identifiés par la NCSAI (2021) pour la transformation numérique du Department of Defense s'appliquent avec précision aux Armées françaises : orientation matérielle historique, processus centrés sur des flux manuels, données stovepiped, plateformes déconnectées, processus d'acquisition rigides. Aucun n'est résolu par une décision technique. Tous le sont par du comportement de commandement visible, répété, non déléguable.

1. Parler personnellement le langage des cinq plaques

Pas déléguer cette lecture au J6. En COMEX, en revue de commandement, lors des exercices, le chef nomme les plaques, cite les niveaux MMP, interroge les propriétaires sur leurs trous. C'est le signal BLANC que le modèle est institutionnellement sérieux — sans ce signal, l'état-major le considérera comme une initiative J6 de plus. Kotter étape 4 : le chef est le premier émetteur.

2. Allouer les ressources en priorité aux plaques les plus minces

Même si cela entre en compétition avec des besoins capacitaires cinétiques plus visibles. Le budget alloué à une plaque est le seul signal ROUGE crédible. Sans arbitrage budgétaire visible en faveur du numérique de résilience, toutes les déclarations d'intention restent dans la lentille BLEUE — de la planification sans levier.

3. Protéger personnellement les signaleurs de trous

Le premier officier qui remonte un incident numérique embarrassant sans subir de conséquence hiérarchique crée un précédent culturel qui vaut dix formations Reason. C'est l'équivalent du CHIRP dans l'aviation : décorrélér délibérément découverte de trous et faute individuelle. Sans cet engagement, la lentille BLANCHE ne change pas — les trous continuent d'être sous-déclarés, et la banquise continue de fondre en silence.

« On ne transforme pas une organisation. On transforme les gens qui la composent, un par un, une lentille à la fois. »

— Roberto M. Fernandez, MIT Sloan, 2023

SECTION VII — PROSPECTIVE 2030 : RECONFIGURATION DE LA CARTE DES PLAQUES

Les technologies émergentes à horizon 2030 ne suppriment pas les trous dans les plaques — elles les déplacent. Certaines épaississent une plaque tout en créant une nouvelle vulnérabilité adjacente. Comprendre ces déplacements est une condition de la planification doctrinale et capacitaire.

7.1 IA embarquée : P4 épaissie, nouveau trou P3 de péremption

Les LLM compacts (7–70 milliards de paramètres, GPU embarqués < 20W) rendent P4 autonome sans cloud central. La plaque P4 en mode DDIL passe du niveau 1 au niveau 4 en une génération — c'est une épaisseur massive. Mais un modèle IA non synchronisé opère sur une image du monde figée à la date de sa dernière mise à jour. Nouveau trou P3 : si la date de dernière synchronisation n'est pas monitorée comme indicateur de gouvernance de premier rang, la force opère avec une IA dont la confiance est inversement proportionnelle à l'ancienneté de ses données d'entraînement — sans signal d'alerte. L'atrophie cognitive de P5 est aggravée si les opérateurs font confiance à une IA dont les données sont périmées.²⁴

7.2 Constellations LEO : P1 épaissie, surface d'attaque déplacée vers l'espace

IRIS², SDA, Starshield offrent une redondance de connectivité sans précédent — P1 s'épaissit face aux menaces terrestres traditionnelles. Mais la dépendance accrue à l'espace concentre la vulnérabilité sur les terminaux sol et les segments de commande des constellations — nouvelles cibles ASAT et cyber à effet P1 systémique. La prolifération de constellations commerciales crée également une dépendance de fait à des opérateurs privés étrangers pour des communications militaires opérationnelles, posant des questions de souveraineté numérique documentées dans les rapports SGDSN.²⁵

²⁴IRSEM, « Intelligence artificielle et supériorité informationnelle pour les armées françaises », Étude 100, 2023. Bastien L. & Boulègue M. (IFRI), « La bataille cognitive : dimensions informationnelles du conflit à haute intensité », Focus stratégique n° 112, 2023. Ces deux références françaises fondent le cadre de la compétition décisionnelle comme enjeu de supériorité informationnelle — condition sine qua non de la M2MC.

²⁵NIST, Post-Quantum Cryptography Standardization — FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), FIPS 205 (SLH-DSA), 2024. ANSSI / SGDSN, Guide de migration vers la cryptographie post-quantique, Paris, 2024. SGDSN, Stratégie nationale pour la sécurité du numérique 2023. CSIS, « The Quantum Threat to National

7.3 Calcul quantique : bombe à retardement dans P1

Le « harvest now, decrypt later » signifie que les communications classifiées d'aujourd'hui constituent un corpus d'exploitation future dès que l'adversaire disposera d'un ordinateur quantique suffisant. Migration vers les standards PQC²⁶ (FIPS 203–205) obligatoire avant 2027 pour les systèmes classifiés. Ce trou est structurellement le plus difficile à motiver budgétairement : il est invisible, non-délectable à court terme, et son urgence est inversement proportionnelle à sa visibilité opérationnelle immédiate. Chaque mois de retard est une augmentation mesurable de la dette numérique dans P1.

7.4 Capteurs quantiques : fermeture architecturale du trou GNSS

Les capteurs quantiques²⁷ — magnétomètres, gravimètres atomiques, horloges de précision — permettent une navigation décimétrique sans GNSS. Ce n'est pas une redondance du GNSS — c'est son remplacement architectural. Le trou de spoofing GNSS en entrée du flux est fermé structurellement, non compensé par une procédure. C'est la forme la plus robuste d'une barrière : l'élimination de la dépendance qui crée le trou, non sa couverture.

7.5 Ailiers loyaux et robots : autonomie locale et nouvelles questions doctrinales

Les ailiers loyaux²⁸ réduisent la dépendance des effecteurs aériens à P1 — une rupture de connectivité n'annule plus les séquences préprogrammées. Mais cette autonomie locale crée deux nouveaux trous doctrinaux : les règles d'engagement préautorisées doivent être maintenues à jour par rapport à la situation réelle (risque de fratricide si la situation diverge de la programmation pré-mission), et la traçabilité de l'autorisation humaine pour chaque effet létal doit être architecturalement garantie pour satisfaire les exigences DIH.²⁹

Security », 2023. IRSEM, « Cryptographie quantique et souveraineté numérique de défense », Étude 107, 2023. Horizon de migration obligatoire : avant 2030 pour les systèmes classifiés (Five Eyes, directive NIS2 UE).

²⁷DARPA, Quantum Sensing and Computing Programs Overview, 2024. DGA, Plan d'investissement Quantique Défense 2030, Ministère des Armées, 2023. FRS, « Capteurs quantiques et navigation autonome : enjeux pour la défense française », Note de recherche 09/2023. RAND, « Quantum Technologies and Defense Applications », RR-A1580, 2023. RUSI, « Quantum Technology for Defence and Security », 2022.

PLAQUE / NŒUD	ÉVOLUTION 2030	NOUVEAU TROU CRÉÉ	ACTION DOCTRINALE PRIORITAIRE
P1 – Connectivité	Épaissie – LEO redondant, mesh cognitif IA	Vulnérabilité ASAT segments sol + menace PQC latente	Migration PQC avant 2027 + hardening segments sol LEO
P2 – Cloud/Edge	Épaissie – edge IA autonome au niveau section	Trou P3 de péremption des modèles IA non synchronisés	Indicateur de fraîcheur modèle IA + protocole synchro automatisé
P3 – Données/COP	Stable – fusion multi-sources améliorée	Flux d'empoisonnement plus larges (LEO + IA open-source + rétroaction effecteurs)	Red-team trimestriel sur tous les flux d'entraînement IA
P4 – Apps/IA	Renforcée – LLM embarqués < 20W	Atrophie jugement humain critique si HITL non exercé activement	Formation HITL obligatoire + explainability systématique + red-team adversarial
P5 – Commandement	Inchangée – dépend uniquement de la doctrine et de l'entraînement	Atrophie compétences analogiques + capitulation cognitive croissante face à l'IA	Exercice C2 sans numérique trimestriel – non négociable + formation au questionnement IA
Effecteurs (sortie)	Transformés – ailiers loyaux, robots, autonomie locale étendue	Fratricide numérique si COP divergents + traçabilité DIH des effets autonomes	Cadre LAWS + audit règles engagement + HITL préautorisé documenté
Capteurs (entrée)	Renforcés – capteurs quantiques GNSS-free à horizon 2028–2030	Surface IA d'interprétation plus large + dépendance supply chain capteurs quantiques	Standardiser fusion cross-domaines + triage cohérence IA embarquée

CONCLUSION — LA SUPERIORITE NUMERIQUE COMME OBLIGATION STRATEGIQUE NON DELEGABLE

Ces réflexions ont cherché à démontrer une thèse simple à énoncer mais difficile à accepter institutionnellement : la manœuvre M2MC est une promesse dont les conditions de réalisation sont numériques. Chaque plaque mince dans le flux numérique est une hypothèse non validée dans le plan opérationnel. La dette numérique militaire n'est pas un problème technique — c'est une question de commandement.

Question opérationnelle que chaque général doit se poser avant toute opération : si mon adversaire trouvait l'alignement optimal de trous dans mes cinq plaques aujourd'hui — quelle serait leur épaisseur réelle, non celle que j'aimerais qu'elle soit ? Et si la réponse est honnête, est-ce que j'accepterais de la dire au COMEX ?

CINQ INVARIANTS STRATÉGIQUES

- I.1** P1 (Connectivité/LDT) est la fondation systémique — sa rupture est catastrophique pour toutes les plaques aval. Distinction impérative : DDIL = fonctionnel/réversible ; EMP = physique/irréversible. Mitigations radicalement distinctes.
- I.2** Capteurs corrompus et effecteurs sans guidage sont des vulnérabilités de flux — non des plaques internes. Leur traitement doctrinal ne se confond pas avec la gouvernance P1–P5.
- I.3** La dette numérique s'accumule silencieusement en l'absence d'incident. Sa cartographie honnête n'est pas un acte technique — c'est un acte de commandement.
- I.4** La tension M2MC/résilience décentralisée n'a pas de résolution architecturale absolue — seulement une résolution doctrinale : formalisée, automatisée, exercée.
- I.5** Les technologies 2030 déplacent les trous. Seule une discipline permanente de gouvernance et d'entraînement maintient les plaques au-dessus du seuil de résilience opérationnelle.

ANNEXE — GLOSSAIRE DES ACRONYMES

Le présent glossaire recense les acronymes et abréviations utilisés dans ce document. Les définitions sont données dans le contexte de leur usage militaire ou numérique. Pour les acronymes OTAN, la référence normative est le AAP-06 (NATO Glossary of Terms and Definitions).

A — M	N — U
AAE Armée de l'Air et de l'Espace	J6 Bureau systèmes d'information et de communication
AMIAD Architecture de Maîtrise de l'IA dans la Défense	KPI Key Performance Indicator — indicateur clé de performance
APT Advanced Persistent Threat — menace persistante avancée	LAWS Lethal Autonomous Weapon Systems — systèmes d'armes létaux autonomes
ASAT Anti-Satellite	LDT Liaison de Données Tactiques
C2 Commandement et Contrôle	LEO Low Earth Orbit — orbite basse terrestre
CEMA Chef d'État-Major des Armées	LLM Large Language Model — grand modèle de langage
CEMAT Chef d'État-Major de l'Armée de Terre	LPM Loi de Programmation Militaire
CHIRP Confidential Human Factors Incident Reporting Programme (aviation)	M2MC Multi-Milieus Multi-Champs — concept de manœuvre interarmées étendue
CICDE Centre Interarmées de Concepts, de Doctrines et d'Expérimentations	MDO Multi-Domain Operations — opérations multi-domaines (OTAN)
CNA Computer Network Attack	MMP Modèle de Maturité des Plaques — référentiel de gouvernance numérique développé dans ce document
CNAS Center for a New American Security	NCSAI National Commission on Artificial Intelligence (États-Unis, 2021)
COP Common Operational Picture — image opérationnelle commune	OODA Observe, Orient, Decide, Act — boucle de décision (Boyd, 1987)
COTS Commercial Off-The-Shelf — équipements commerciaux standards	OOTL Human-Out-Of-The-Loop — IA décidant sans supervision humaine

<p>CSET Center for Security and Emerging Technology (Georgetown)</p>	<p>OPORD Operations Order — ordre d'opérations</p>
<p>DDIL Denied, Degraded, Intermittent or Limited — connectivité dégradée ou limitée</p>	<p>OT Operational Technology — systèmes industriels de contrôle et d'automatisation</p>
<p>DGA Direction Générale de l'Armement</p>	<p>OTAN Organisation du Traité de l'Atlantique Nord (NATO en anglais)</p>
<p>DIH Droit International Humanitaire</p>	<p>P1–P5 Plaques 1 à 5 du modèle de l'écosystème numérique militaire : P1 Connectivité, P2 Cloud/Edge, P3 Données, P4 Apps/IA, P5 Commandement</p>
<p>CND Commandement du Numérique de la Défense</p>	<p>PGM Precision-Guided Munition — munition guidée de précision</p>
<p>DoD Department of Defense (États-Unis)</p>	<p>POC Proof of Concept — preuve de concept / démonstrateur</p>
<p>DSI Direction des Systèmes d'Information</p>	<p>PQC Post-Quantum Cryptography — cryptographie post-quantique (FIPS 203–205)</p>
<p>EMA État-Major des Armées</p>	<p>RAG Retrieval-Augmented Generation — génération augmentée par récupération documentaire</p>
<p>EMP Electromagnetic Pulse — impulsion électromagnétique</p>	<p>RAND Research ANd Development Corporation — think tank américain de référence</p>
<p>EMS École Militaire Supérieure / Enseignement Militaire Supérieur</p>	<p>REX Retour d'Expérience</p>
<p>FIPS Federal Information Processing Standards (NIST)</p>	<p>RNS Revue Nationale Stratégique</p>
<p>FRAGORD Fragmentary Order — ordre fragmentaire</p>	<p>RUSI Royal United Services Institute (Royaume-Uni)</p>
<p>GNSS Global Navigation Satellite System — système de navigation par satellite</p>	<p>SATCOM Satellite Communication — communications par satellite</p>
<p>GPU Graphics Processing Unit — processeur graphique</p>	<p>SBOM Software Bill of Materials — inventaire des composants logiciels d'une chaîne de livraison</p>
<p>HF Haute Fréquence</p>	<p>SCADA</p>

	Supervisory Control And Data Acquisition — système de contrôle et d'acquisition de données industriel
HITL Human-In-The-Loop — humain dans la boucle de décision	SDA Space Development Agency (États-Unis)
HOTL Human-On-The-Loop — humain sur la boucle de décision	SGDSN Secrétariat Général de la Défense et de la Sécurité Nationale
IA Intelligence Artificielle	SIGINT Signals Intelligence — renseignement d'origine électromagnétique
IFRI Institut Français des Relations Internationales	SITREP Situation Report — compte-rendu de situation opérationnelle
IISS International Institute for Strategic Studies	STAMP Systems-Theoretic Accident Model and Processes — modèle accidentologique (Leveson, MIT)
IRSEM Institut de Recherche Stratégique de l'École Militaire	STANAG Standardization Agreement — accord de standardisation OTAN
IT Information Technology — technologie de l'information	TF Task Force — groupe de travail ad hoc à mandat et durée définis
J2 Bureau renseignement de l'état-major	UEBA User and Entity Behavior Analytics — analyse comportementale des utilisateurs et entités
J3 Bureau opérations de l'état-major	USB Universal Serial Bus — interface de connexion de périphériques

Sources de référence pour les définitions normatives : AAP-06 (OTAN, édition 2021) ; Dictionnaire de la défense nationale, DGA, 2022 ; NIST Computer Security Resource Center (csrc.nist.gov) ; Lexique numérique interministériel, SGDSN, 2023.

Références bibliographiques

1. Ministère des Armées / EMA, Concept M2MC, Paris, 2021 ; CICDE, CIA-01(A)_CICDE(2021) ; IFRI, Focus stratégique n° 109, 2022.
2. US Army TRADOC, TRADOC Pamphlet 525-3-1 (MDO 2028), déc. 2018 ; NATO ACT, Concept for MDO, 2023.
3. Boyd J., A Discourse on Winning and Losing, USAF, 1987 ; IRSEM, Étude 98, 2022.
4. STANAG 5516/5522 ; DGA, LDT, 2022 ; FRS, Note 14/2022.
5. Reason J., Human Error, Cambridge UP, 1990 ; ENISA, TG-CYB-22-003, 2022.

6. Perrow C., *Normal Accidents*, Basic Books, 1984 ; RAND, RR-4408, 2021.
7. DARPA, CCA Program, 2024 ; RAND, RR-A1214, 2022 ; IRSEM, Étude 116, 2023.
8. RAND, RR-A2196-1, 2023 ; FRS, Note 32/2023 ; DGA, STA, 2022.
9. Langner R., *IEEE Security & Privacy*, 2011 ; Lindsay J.R., *Security Studies*, 2013 ; IRSEM, Étude 68, 2021.
10. RUSI, *Occasional Paper*, 2023 ; IISS, *Strategic Survey 2023* ; IFRI, Note, 2023.
11. ISW, 2022–2024 ; CNAS, 2023 ; Charap S. & Darden K. (RAND), *Survival IISS*, 2023.
12. ClearSky, 2020 ; *The Economist*, 2021 ; FRS, 07/2022 ; IRSEM, Étude 82, 2022 ; INSS, *Insight 1712*, 2023.
13. Mandiant, *APT33 : At the Crossroads of Iran and Cybercrime*, 2017 ; FireEye/Mandiant, *Threat Actor Profile APT33 (HOLMIUM)*, 2020 ; SGDSN/ANSSI, *Panorama cybermenace 2023*.
14. Microsoft MSTIC, *Solorigate*, déc. 2020 ; CISA, AA21-008A, 2021.
15. ICAO, Doc 9683, 1998 ; IATA, *Safety Report*, 2022.
16. IRSN, INF-2019-00083, 2019 ; ASN, *Rapport annuel 2022*.
17. Weick K.E. & Sutcliffe K.M., *Managing the Unexpected*, Jossey-Bass, 2001 ; RAND, RR-4408, 2021.
18. Leveson N., *Engineering a Safer World*, MIT Press, 2012 ; IRIS, *Lettre n° 47*, 2023.
19. CMMI Institute, *CMMC 2.0*, US DoD, 2022 ; ISO/IEC 27001:2022.
20. Kotter J.P., *Leading Change*, HBR Press, 1996.
21. Schein E.H., *Organizational Culture and Leadership*, Jossey-Bass, 4e éd., 2010.
22. NIST, FIPS 203–205, 2024 ; ANSSI/SGDSN, *Guide PQC*, 2024 ; IRSEM, Étude 107, 2023.
23. DARPA, *Quantum Sensing*, 2024 ; DGA, *Programme Quantique 2030* ; FRS, Note 09/2023.
24. Sun Tzu, *L'Art de la Guerre*, ~500 av. J.-C. ; IRSEM, Note 14, 2021.
25. Biggio B. & Roli F., *Pattern Recognition*, 2018 ; IRSEM, Étude 121, 2023 ; ANSSI, PA-086, 2024.
26. Johnson J., Georgetown UP, 2023 ; ICRC, *Autonomous Weapon Systems*, 2022 ; IRSEM, Étude 72, 2021.
27. Ministère des Armées, *Stratégie transformation numérique 2023–2026*, CND ; RNS 2022 ; IFRI, 2022.
28. Chatham House, 2023 ; Schmitt M.N. (dir.), *Tallinn Manual 2.0*, Cambridge UP, 2017.
29. IRSEM, Étude 100, 2023 ; Bastien L. & Boulègue M. (IFRI), *Focus stratégique n° 112*, 2023.
30. Claverie B. (IHEDN), RDN n° 861, 2023 ; Taddeo M. (Oxford), *Philosophy & Technology*, 2012.
31. Posen B.R., *International Security*, Vol. 28/1, 2003 ; Kello L., Yale UP, 2017.
32. Assemblée nationale, *Rapport n° 1836*, 2023 ; Sénat, *Rapport n° 622*, 2023 ; Cour des comptes, 2022.
33. NATO AJP-2.1, *Allied Joint Intelligence Doctrine*.
34. CERI (Sciences Po), *Questions de Recherche n° 68*, 2022 ; Lasconjarias G. & Larsen J.A. (IRSEM), *NDC*, 2015.
35. CNCTR, *Rapport 2022–2023* ; DPSD, *Rapport annuel menace*, 2023 ; Verizon, *DBIR 2023*.
36. NIST SP 800-53 Rev.5, 2020 ; ANSSI, *Guide hygiène informatique*, 2017.

37. IRSEM & FRS, Dissuasion élargie française, Étude conjointe, 2023.
38. Taleb N.N., Antifragile, Random House, 2012 ; RAND, PE-A1975, 2023.
39. Fernandez R.M., Navigating Organizational Change: Lens-Based Frameworks for Strategic Leaders, MIT Sloan Executive Education Program, 2023 ; Brown J.S. & Duguid P., The Social Life of Information, HBR Press, 2000.