D'UN SYSTEME D'INFORMATION RESILIENT A UN SYSTEME D'INFORMATION ANTI-FRAGILE? ILLUSTRATIONS A PARTIR DES ORGANISATIONS MILITAIRES

Cécile Godé, Jean-Fabrice Lebraty, Pierre Barbaroux

Godé, C., Lebraty J-F. et Barbaroux, P. (2023), "D'un système d'information résilient à un système d'information antifragile : illustrations à partir des organisations militaires », *Les Cahiers Risques et Résilience*, accepté pour publication.

D'UN SYSTEME D'INFORMATION RESILIENT A UN SYSTEME D'INFORMATION ANTI-FRAGILE ?

ILLUSTRATIONS A PARTIR DES ORGANISATIONS MILITAIRES

Cécile Godé
Professeure agrégée des Universités
Aix-Marseille Univ, CERGAM, Aix en Provence, France

Jean-Fabrice Lebraty
Professeur agrégé des Universités
IAE de Lyon, MAGELLAN, Lyon, France

Pierre Barbaroux
Enseignant-chercheur (HDR)
Centre de Recherche de l'Ecole de l'Air et de l'Espace (CReA), Salon de Provence, France

Introduction

Ces derniers mois, la littérature en sciences de gestion et management, qu'elle soit académique ou professionnelle, ne cesse d'adresser des injonctions à la résilience à des entreprises encore traumatisées par la crise sanitaire (Frimousse et Peretti, 2020). Devenir ou rester résiliente, c'est pour une organisation savoir rebondir après un choc, externe ou interne, à la fois en maintenant ses processus, fonctions et structures initiaux (par exemple, Roberts et al., 1994 ; Sutcliffe et Vogus, 2003) mais également en développant des capacités d'évitement des crises et turbulences (Weick, 1993 ; Roux-Dufort, 2003). L'organisation résiliente est donc celle qui sait « *entretenir ou rétablir un état dynamiquement stable qui lui permette de poursuivre ses opérations après un incident majeur et/ou en présence d'un stress continu* » (Hollnagel et al., 2006, p. 16). La résilience organisationnelle, et la notion de rebond qui lui est fréquemment associée, s'entendent différemment selon les auteurs spécialisés. Lorsque, pour la grande majorité d'entre eux, il s'agit de revenir à la position initiale, d'autres adoptent une compréhension plus ouverte en considérant la possibilité pour l'organisation de trouver un nouvel état d'équilibre après le choc (Bout-Vallot, 2008 ; Koninckx et Teneau, 2010) et de s'adapter aux nouvelles exigences de son environnement.

Parallèlement à cet intérêt post-covid croissant pour la résilience organisationnelle, d'autres contributions en management (voir par exemple Frimousse et Gaillard, 2021 ; Frimousse, 2022) s'emparent de la notion d'anti-fragilité (Taleb, 2013) pour voir au-delà. Une organisation anti-fragile se renforce dans l'adversité ; elle prospère et se développe au sein d'environnements variables. L'organisation anti-fragile tire profit du caractère dynamique non linéaire des « cygnes noirs », entendus comme des évènements extrêmes et souvent imprévisibles, de grande ampleur dans leurs effets et qu'il est possible d'expliquer rétrospectivement[1] (Taleb, 2012). Par ailleurs, plus l'organisation est confrontée aux imprévus, plus son exposition aux pertes est limitée et sa potentialité de gain s'accroît (Taleb et Douady, 2013 ; Taleb et West, 2022). Ainsi, être ou devenir une organisation anti-fragile implique d'aborder les chocs comme autant d'opportunités de progresser et de contribuer à la performance, tout en restant sensible aux menaces potentielles qu'ils représentent.

Dans cet article, nous portons le regard au niveau du Système d'Information (SI). Comme l'avance Taleb (2013), « *l'information est anti-fragile ; elle se nourrit davantage des tentatives de lui porter*

[1] Un cygne noir possède trois attributs : *« premièrement, il s'agit d'une aberration ; de fait il se situe en dehors du cadre de nos attentes ordinaires, car rien dans le passé n'indique de façon convaincante qu'il ait des chances de se produire. Deuxièmement, son impact est extrêmement fort. Troisièmement, en dépit de son statut d'aberration, notre nature humaine nous pousse à élaborer après coup des explications concernant sa survenue, le rendant aussi explicable et prévisible »* (Taleb, 2012, p. 10).

préjudice que des efforts que l'on fait pour la promouvoir » (p. 66). Dans l'organisation, ce sont les SI qui prennent en charge la collecte, le stockage, l'analyse et la diffusion de l'information. Ils ont été largement sollicités ces derniers mois, pour garantir le bon fonctionnement des activités courantes et du pilotage d'organisations confrontées aux cygnes noirs. Nous cherchons ainsi à comprendre comment diagnostiquer un SI résilient et anti-fragile ?

Pour se faire, nous identifions dans la littérature en Management des Systèmes d'Information (MSI) et en sciences informatiques des caractéristiques constitutives de la résilience et de l'anti-fragilité d'un SI. Nous les articulons ensuite aux trois dimensions d'un SI (technologique, organisationnelle et managériale). L'objectif poursuivi est l'élaboration, dans sa version première, d'une matrice de diagnostique permettant de situer un SI en termes de résilience et d'anti-fragilité. Nous illustrons ensuite l'application de cette matrice à des SI exploités au sein d'organisations militaires.

De la résilience à l'anti-fragilité : vers l'élaboration d'une matrice de diagnostique d'un SI anti-fragile

Dans cet article, un SI est considéré comme « *un ensemble de processus formels de saisie, de traitement, de stockage et de communication de l'information, basés sur des outils technologiques, qui fournissent un support aux processus transactionnels et décisionnels ainsi qu'aux processus de communication actionnés par des acteurs organisationnels, individus ou groupes d'individus, dans une ou dans plusieurs organisations* » (Kéfi et Kalika, 2004, p. 23). Pour appréhender le SI dans toute sa complexité et contourner le piège du déterminisme (technologique ou social), nous l'abordons selon une perspective socio-matérielle (voir par exemple, Orlikowski, 2010 ; Leonardi, 2013), qui articule agence humaine – les structures sociales, organisationnelles, collectives et les utilisateurs dans leurs perceptions et interactions avec le système – et agence matérielle – la technologie, sa matérialité, ses règles, ses fonctionnalités, etc.

En MSI, des travaux se penchent sur la résilience des SI (par exemple, Zhang et Lin, 2010 ; Tseitlin, 2013 ; Heeks et Ospina, 2018 ; Sakurai et Chughtai, 2020 ; pour une revue systématique de littérature sur la notion de résilience digitale, Dupin et al., 2023 ; Kohn, 2023). Pour certains, ils s'attachent à identifier les grands principes de conception (ou caractéristiques) d'un SI résilient. Ces derniers sont pensés en lien avec les quatre leviers de la résilience organisationnelle proposés par Weick (1993), à savoir l'improvisation (ou le bricolage), l'ajustement des rôles (ou les systèmes de rôles virtuels), la réflexivité (ou la sagesse comme attitude) et la fiabilité des interactions (ou les interactions respectueuses dans la confiance, l'honnêteté et le respect de soi).

Basé sur la littérature spécialisée en MSI, le tableau N°1 propose une liste des principes de conception (ou caractéristiques) d'un SI résilient :

Principe/caractéristique	Description
La fiabilité	La transmission, l'intégrité, la conformité, la sécurité et la consolidation des données saisies dans le SI (automatisation)
La surveillance continue	Des capteurs dédiés à la surveillance temporelle et spatiale du bon fonctionnement du SI
La prédiction	Des capacités prédictives pour anticiper les vulnérabilités (internes) et les menaces (externes) du SI
L'adaptabilité	L'architecture flexible, capable d'absorber les évolutions des sources d'information et des besoins clients par interfonctionnement de composants logiciels « historiques » (par exemple, ERP, CRM) et nouveaux (par exemple, APIs)
La redondance des données	La duplication des données
L'apprentissage du changement	Des ressources humaines en charge de l'urbanisation du SI (évolution de son infrastructure, de ses composants), de la conception et/ou mise en œuvre de dispositifs d'apprentissage à destination des utilisateurs du SI (formations) et, plus globalement, de la gestion de la transformation digitale

Tableau 1. Principes de conception d'un SI résilient

A l'exception notable de l'article de Gorgeon (2015), qui identifie des « directives anti-fragiles » et des processus de création de valeur à destination de l'informatique d'entreprise, le MSI reste concentré sur le SI résilient et ne s'empare que très peu de la notion de l'anti-fragilité pour penser au-delà. Les sciences informatiques viennent combler ce vide en développant des travaux dédiés à la question de la conception et du développement de logiciels et d'architectures informatiques anti-fragiles[2] (voir par exemple, De Florio, 2014 ; Hole, 2016 ; O'Reilly, 2019 ; Simonette et al., 2019).

Pour la plupart, les auteurs partent du constat que, puisqu'il est impossible d'éviter la survenance de cygnes noirs, il convient de développer des systèmes adaptatifs complexes capables à la fois de réduire leurs impacts et d'en tirer avantage pour se transformer. Comme le rappellent Frimousse et Gaillard (2021), « *l'anti-fragilité se façonne en s'exposant intelligemment à certains préjudices qui, in fine, renforcent plutôt qu'ils n'affaiblissent* » (p. 274). Il s'agirait donc de développer un SI en mesure d'absorber et d'apprendre les/de petits chocs inévitables, tout en se protégeant des grands risques, porteurs de trop fortes menaces pour le système.

Là encore, la littérature s'attache à identifier les caractéristiques de telles architectures informatiques et logicielles. Le tableau N°1 en liste les plus saillantes :

[2] Un manifeste du logiciel anti-fragile a été publié (Russo et Ciancarinia, 2016), à la base d'une série annuelle de séminaires (*International Workshop on Computational Antifragility and Antifragile Engineering*) autour du thème.

Principe/caractéristique	Description
La modularité	La conception d'un système constitué de modules logiciels et matériels faiblement interconnectés (en cas de panne, défaut ou problème local détecté sur un module, la connexion aux autres est interrompue pour éviter la propagation à l'ensemble du système) (par exemple, Flow First Design, IDesign Method)
La redondance des modules	La duplication des modules logiciels et matériels composant le SI
La diversité	Les modules dupliqués sont conçus ou implémentés différemment, tout en délivrant les (quasi) mêmes fonctionnalités (il s'agit d'éviter que le module dupliqué connaisse la même panne ou défaut que le module d'origine)
L'apprentissage par l'erreur	Les petits chocs (pannes, défauts) doivent être sciemment introduits dans le système pour favoriser l'apprentissage par l'erreur et faire évoluer le SI afin de limiter l'impact des incidents à venir (par exemple, Failure Mode Effects Analysis)

Tableau 2. Principes de conception d'un SI anti-fragile

Dans cet article, nous proposons d'élaborer une matrice de diagnostique d'un SI anti-fragile en croisant les trois dimensions d'un SI (technologique, organisationnelle et humaine – ou managériale) aux grands principes de conception d'un SI résilient et d'un SI anti-fragile, tels qu'identifiés par la littérature spécialisée (MSI et informatique). Comme la Figure N°1 le met en lumière, certaines de ces caractéristiques sont semblables, ou du moins suffisamment homogènes, pour être considérées comme communes aux SI résilient et anti-fragile.

Godé, C., Lebraty J-F. et Barbaroux, P. (2023), “D’un système d’information résilient à un système d’information antifragile : illustrations à partir des organisations militaires », *Les Cahiers Risques et Résilience*, accepté pour publication.

	SI RESILIENT				**SI RESILIENT/ANTIFRAGILE**				**SI ANTIFRAGILE**	
SI	Fiabilité	Surveillance continue	Prédiction	Adaptabilité	Redondance des données	Apprentissage du changement	Apprentissage par l'erreur	Redondance des modules	Modularité	Diversité
Dimension technologique										
Dimension organisationnelle										
Dimension managériale										

Figure 1. Vers une matrice de diagnostique d’un SI anti-fragile

Les sections suivantes s'attachent à appliquer la matrice de diagnostique d'un SI anti-fragile aux SI militaires ou exploités en environnement militaire. Ils servent en effet des activités opérationnelles et stratégiques conduites en contextes extrêmes (Bouty et al., 2012 ; Potosky et al., 2022), venant en soutien des processus de coordination et de décision face aux cygnes noirs (Godé, 2008 ; Godé et al., 2020). Les SI militaires sont-ils résilients ou anti-fragiles ?

SI résilients et SI anti-fragiles dans les organisations militaires

La référence au concept d'anti-fragilité est peu présente dans les publications stratégiques et doctrinales, comme dans les travaux académiques appliqués aux affaires militaires ou traitant des questions de défense et de sécurité. A l'exception de quelques travaux portant sur l'exercice du commandement (leadership anti-fragile, Luft, 2021), la posture du combattant (combattant anti--fragile, Chambers 2021), ou les relations internationales (la notion d'Etat anti-fragile, Law, 2021), rares sont les publications institutionnelles ou académiques qui explorent le caractère anti-fragile des systèmes d'information opérationnels (SIO) ou des systèmes d'information et de communication (SIC) utilisés par les armées.

Les experts militaires portent en revanche une attention considérable à la notion de résilience appliquée à des « objets » aussi divers que les infrastructures critiques, la société civile, les organisations militaires, les systèmes d'armes, les combattants, les structures de commandement et de conduite des opérations et, fort logiquement, les SI militaires (Hamilton, 2016 ; Shea 2016 ; Cao et al., 2021).

Pour les pays membres de L'OTAN, dont la France, la résilience désigne une propriété comportementale attachée aux capacités militaires, observable à différentes échelles – individuelle et collective, technologique, organisationnelle, voire sociétale (El Fertasi et De Vivo, 2016 ; RNS, 2022). Dans les Armées françaises par exemple, la résilience qualifie les capacités déployées et les aptitudes associées (connaitre et anticiper, prévenir, dissuader, protéger et intervenir), et repose notamment sur un ensemble de « prédispositions intrinsèques » qui forment le « socle de la résilience » : les forces morales du personnel militaire, les équipements rustiques et de hautes technologies utilisés en combinaison, la redondance et l'autonomie (DIA 3-4-1, 2022, p. 13). La résilience des Armées françaises concerne donc l'ensemble des ressources et fonctions (doctrine, organisation, ressources humaines et formations, entraînement, soutien et équipement ; DORESE) qui concourent au déploiement des capacités ; elle relève in fine de la « cohérence de l'ensemble des fonctions leur permettant de faire face à une crise majeure sans rupture d'aucune sorte » (DIA 3-4-1, 2022, p. 14).

Lorsqu'elle est utilisée pour caractériser les attributs des SI militaires, la résilience est systématiquement associée à la sécurité des systèmes d'information (SSI) et à la robustesse des activités informationnelles et décisionnelles des armées. Dans ce cadre, la résilience est systématiquement associée à la cyber sécurité des SIO et des SIC (on parle de cyber-résilience et, par extension, de cyberdéfense : Angelotti et Naegels, 2020 ; Barbaroux, 2020 ; Chevrier, 2020). Cette approche de la résilience des SI militaires, que nous pourrions qualifier de techno-centrée, laisse peu de place aux processus dynamiques tels que l'apprentissage et l'agilité, privilégiant davantage la fiabilité, la rusticité, la plasticité et la liberté d'action, autant d'aptitudes essentielles à la conduite des affaires militaires à l'ère numérique et informationnelle (Barbaroux, 2017 ; Duchemin et al., 2018).

L'une des raisons pour lesquelles les militaires focalisent leur attention sur la notion de résilience tient justement à l'adoption d'une grille de lecture essentiellement capacitaire des aptitudes recherchées en matière de performance opérationnelle. Une capacité correspond en effet à un ensemble de ressources matérielles et immatérielles contribuant à la réalisation de certaines missions et/ou actions. Dans ce cadre, les sources et composantes de la résilience sont aussi diverses que les ressources qui composent les capacités : pour les militaires la résilience est tout à la fois informationnelle, cognitive, technologique, organisationnelle, managériale, humaine, institutionnelle voire sociétale (Shea, 2016 ; Cao et al., 2021). La résilience est donc utilisée autant pour qualifier les propriétés des SI militaires que les capacités que ces systèmes supportent (DIA SIC OPS, 2014 pour la France).

En pratique, quatre caractéristiques sont plus particulièrement mises en avant dans le corpus doctrinal lorsqu'il s'agit de caractériser un SI militaire résilient : la décentralisation, la modularité, la redondance et l'interopérabilité. Il s'agit d'attributs attachés aux capacités militaires dans leurs dimensions opérationnelles (par ex., Network-Centric Warfare et Guerre Multi-Domaines Multi-Champs) et technologiques (par ex., SIC OPS). Dans ce contexte, la cybersécurité (détection, protection) est considérée comme essentielle dans la mesure où elle conditionne la résilience des SI militaires et, par extension, des capacités dont ils permettent le déploiement (on parle de cyber-résilience des SIC et de capacités offensives et défensives en matière de cyberdéfense ; Lété et Dege, 2017).

On observe donc que si l'anti-fragilité n'est jamais mentionnée en tant qu'attribut des SI ou des capacités militaires, certaines caractéristiques des SI anti-fragiles sont clairement identifiées par les armées. Ces caractéristiques (modularité, redondance, apprentissage, etc.) sont considérées comme essentielles au développement de la résilience sous toutes ses formes. A titre d'illustration, l'entraînement, l'expérimentation et l'apprentissage dans et par l'action sont des piliers de la culture et de l'identité professionnelles militaires (Barbaroux et Godé, 2016 ; Barbaroux, 2022 ; Potosky et al., 2022). Pour les militaires, ces processus ne contribuent pas uniquement à la résilience des SIC et des SIO, mais également au maintien et au développement de la performance opérationnelle via l'adaptabilité et l'agilité des dispositifs capacitaires déployés sur les théâtres d'opérations (Gros et al., 2022).

Une lecture attentive des publications doctrinales et académiques définissant les attributs des capacités militaires ainsi que les attributs des SI sur lesquels elles reposent, confirme la référence à plusieurs caractéristiques associées au concept de SI anti-fragile. Outre l'apprentissage, l'expérimentation et l'entraînement du personnel, il apparaît que la décentralisation et l'adaptation des modes d'action et de décisions (Barbaroux, 2011), ainsi que la modularité, l'interopérabilité, la redondance et l'adaptabilité des systèmes (Alberts et Hayes 2003 ; Barbaroux, 2010 ; Godé et Barbaroux, 2016 ; Gros, 2020) sont autant d'aptitudes identifiées par les armées comme constitutives – voire génératives – de la résilience cyber-physique des organisations militaires (Barbaroux, 2017).

En articulant les approches de la résilience des SI militaires avec les mécanismes supportant la performance opérationnelle, il apparaît que les caractéristiques attachées aux capacités militaires résilientes sont proches voire équivalentes à celles caractérisant un SI anti-fragile dans les trois dimensions (technologiques, organisationnelles et managériales) identifiées dans la matrice (Figure 1). Les SI militaires, tels que définis dans les documents de doctrine, seraient-ils anti-fragiles … sans le savoir ?

La section suivante présente l'exemple du système Starlink, un SI civil développé par et appartenant à une entreprise privée, visant à fournir une liaison Internet haut débit. Starlink constitue un réseau visiblement fiable puisqu'actuellement utilisé par les unités militaires ukrainiennes (à noter que la partie adverse élabore un système analogue appelé Sphère).

Le cas Starlink : diagnostique d'un SI anti-fragile civil exploité par les armées ukrainiennes

Starlink est une constellation de satellites appartenant à l'entreprise SpaceX, fondée par Elon Musk en 2002. Les premiers satellites ont été lancés en 2019 et, à ce jour, près de 3.900 ont été mis en orbite. Ce chiffre élevé s'explique par leur taille modeste, qui facilite des lancements en grand nombre : par exemple, le 24 janvier 2021, 143 satellites ont été lancés en une seule fois. SpaceX vise un objectif de plus de 10.000 satellites dans les prochaines années. Cette constellation a pour vocation de fournir un service internet haut débit à l'échelle mondiale. Les satellites ont en effet été conçus pour offrir une connexion Internet stable et fiable, avec des vitesses pouvant aller jusqu'à 1 gigabit. Les services de connexion sont proposés à des prix compétitifs.

Du point de vue militaire, Starlink joue un rôle important pour les flux de communication de l'armée et de la population ukrainiennes. En effet, en avril 2022, la société annonçait que près de 150.000 personnes utilisaient ce service dans le pays. Transmission d'ordres, coordination des effets, utilisation de drones et de capteurs, les besoins en flux Internet sont nombreux. Les réseaux filaires ou sans fil classiques (fibre et station émettrice-réceptrice de base-BTS) étant fortement dégradés, Starlink constitue ainsi un outil déterminant dans l'issue des combats en cours. D'ailleurs, début décembre 2022, l'entreprise a annoncé le lancement de la gamme Starshield, variation militaire de la version civile. D'intérêt au niveau des SI, voyons comment Starlink peut être considéré du point de vue des notions de résilience et d'anti-fragilité.

L'étude de documents publics et de données ouvertes recueillies sur des chaines Telegram de comptes suivant le conflit ukrainien (voir les principales chaînes utilisées en fin de liste bibliographique) montre que Starlink couvre de nombreuses caractéristiques d'un SI résilient et anti-fragile (sous réserve que l'équipe dirigeante de Starlink le laisse à disposition). Reprenons la matrice de diagnostic d'un SI anti-fragile, et croisons-la avec des faits rapportés par les observateurs du théâtre.

Du point de vue de la résilience et de son attribut « fiabilité technologique », le système est considéré comme fiable : il y a en effet très peu de commentaires rapportant des pannes, ou des problèmes liés à l'intégrité des données. A noter cependant que les conditions d'emploi sont restrictives (zone plate, météo favorable notamment), et que des brouillages ont été signalés à différents endroits de la ligne de contact, qui ont pu empêcher la bonne transmission de données. En termes managériaux, les usages de Starlink déployés sur théâtre semblent remplir les conditions de fiabilité : il n'a pas été rapporté de tirs fratricides dus à Starlink par exemple (ce qui ne signifie évidemment pas qu'il n'y en a pas eu), ou de problèmes liés à la mise en œuvre du système.

Concernant la caractéristique « prédiction » de la résilience du SI dans sa dimension organisationnelle : il est difficile d'anticiper les vulnérabilités externes de Starlink. Par exemple, Le 26 janvier 2023, un tir d'artillerie de précision russe a détruit un poste de commandement (PC) près de Vugledar à cause des émissions de l'antenne Starlink. Dans le domaine de la guerre d'influence, le 15 octobre 2022, un véhicule militaire de type BMP et au moins un soldat ukrainien sont photographiés, morts près d'une antenne Starlink ; un véritable trophée de guerre. Un autre type de vulnérabilité externe concerne les

coupures d'accès volontaires au réseau Starlink, comme cela a été le cas durant la journée du 4 novembre 2022 sur décision d'Elon Musk ; ce type d'« épée de Damoclès » permanente conduit à limiter les capacités prédictives associées au système.

Concernant la partie mix SI résilient/anti-fragile, sur les aspects technologiques : les données montrent que le système possède des capacités d'apprentissage du changement (patchs correctifs, notamment), une redondance des modules (satellites, bases au sol, antennes) et une redondance des données. En revanche, ce dernier attribut n'a pas été pris en compte par les informaticiens du SIC et donc, de l'organisation. Enfin, et même si Starlink n'est pas le seul élément explicatif à prendre en compte, les unités militaires ukrainiennes ont su s'adapter au changement induit par l'arrivée d'une connexion Internet ubiquitaire. Elles ont également su apprendre de leurs erreurs : la preuve en est du faible nombre de kits de réception et antennes (sur les 22.000 distribués à l'automne 2022, moins d'une dizaine auraient été récupérés) pris par les forces adverses.

Enfin, en termes d'anti-fragilité, Starlink contribue à la modularité, dans ses trois dimensions. Du point de vue technologique, le système s'intègre à tous les terminaux Internet Protocol (IP). L'organisation peut aussi être plus modulaire, un nœud pouvant être remplacé par, mais également combiné avec un autre. Il ne s'agit pas d'une architecture réseau en boucle (comme c'est le cas des lignes coaxiales) mais en étoile, les cohortes de satellites formant l'étoile elle-même. En revanche, concernant la caractéristique « diversité », il est à noter que les équipements Starlink sont propriété de l'entreprise SpaceX, et qu'il n'existe qu'une gamme très finie de composants.

La figure N°2 suivante applique ces résultats à la matrice de diagnostique d'un SI anti-fragile (les cases sont non renseignées lorsque nous n'avons pas collecté de données nous permettant de les traiter).

Godé, C., Lebraty J-F. et Barbaroux, P. (2023), "D'un système d'information résilient à un système d'information antifragile : illustrations à partir des organisations militaires », *Les Cahiers Risques et Résilience*, accepté pour publication.

	SI RESILIENT				**SI RESILIENT/ANTIFRAGILE**				**SI ANTIFRAGILE**	
SI	Fiabilité	Surveillance continue	Prédiction	Adaptabilité	Redondance des données	Apprentissage du changement	Apprentissage par l'erreur	Redondance des modules	Modularité	Diversité
Dimension technologique	+		+/-		+	+		+	+	
Dimension organisationnelle	+		+/-		-	+	+		+	-
Dimension managériale	+					+	+			

Figure 2. La matrice de diagnostique d'un SI anti-fragile appliquée à Starlink

Conclusion

Pour conclure, cet article s'est attaché à élaborer la première version d'une matrice permettant de diagnostiquer un SI en termes de résilience et d'anti-fragilité. Cette matrice a ensuite été discutée selon le corpus doctrinal s'appliquant notamment aux SI militaires, puis a été appliquée à un SI civil actuellement exploité par les armées ukrainiennes : Starlink. Nous montrons que les notions de résilience et d'anti-fragilité amènent à se poser des questions utiles pour évaluer la performance d'un SI. Nous constatons également que, loin de s'opposer, la résilience et l'anti-fragilité du SI se situent sur un continuum : la conception d'un SI résilient peut être considérée comme une première et nécessaire étape de l'anti-fragilité.

Notre contribution est exploratoire : à notre connaissance, il n'existe pas de travaux qui articulent la littérature en MSI sur les SI résilients, et la littérature, plutôt issue des disciplines informatiques, discutant de SI anti-fragiles. Il serait nécessaire de poursuivre les recherches pour répondre d'une part à la question de l'intérêt conceptuel et managérial d'une telle approche et, si cet intérêt est avéré, d'approfondir d'autre part cette première version d'une matrice somme toute encore très perfectible. En particulier, l'article présente la décentralisation et l'interopérabilité comme deux attributs clés des capacités militaires dans leurs dimensions opérationnelles et technologiques, selon le corpus doctrinal. Or, ces deux attributs n'apparaissent pas dans la matrice de diagnostique d'un SI anti-fragile. Il semblerait pertinent de pousser l'analyse plus avant pour interroger l'intérêt d'intégrer ces deux attributs supplémentaires à la matrice.

Références

Alberts, D.S. et Hayes, R.E. (2003). Power to the Edge: Command Control in the Information Age. CCRP Publications Series, 303 pages. http://www.dodccrp.org/files/Alberts_Power.pdf.

Angelotti, C. et Naegels, C. (2020). Systèmes d'information, intelligence artificielle et cyber sécurité. *Pensée Mili-Terre*, 52, 4 pages.

Barbaroux (2010). Modularité de l'organisation et design des organisations adaptatives : une analyse de la transformation des organisations de défense américaines. *Innovations. Revue d'Economie et de Management de l'Innovation*, 31(1), 31-50.

Barbaroux, P. (2011). A design-oriented approach to organizational change: Insights from a military case study. *Journal of Organizational Change Management*, 24(5), 626-639.

Barbaroux, P. (2017). Cyber résilience : Une capacité des organisations aérospatiales et de défense. *Leçon Inaugurale Chaire Cyber-Résilience Aérospatiale*, Ecole de l'air et de l'espace, Salon de Provence, délivrée publiquement le 5 décembre 2017.

Barbaroux, P. (2020). Cyber-résilience et organisation. Essai de caractérisation de la cyber-résilience comme capacité organisationnelle. *14ème Conférence GeCSO*, Clermont-Ferrand, 18-20 mai 2021.

Barbaroux, P. (2022). Developing leadership skills through simulation-based training: A research framework and interpretive case study. *Management International*, 26(1), 192-208.

Barbaroux, P. et Godé, C. (2016). Le briefing-débriefing : une procédure pour lever les barrières pesant sur l'apprentissage organisationnel ? *Gérer & Comprendre*, 124(2), 41-51.

Bout-Vallot, L. (2008). La résilience au service de la fiabilité organisationnelle : le cas des forces opérationnelles de l'Armée de l'air. Thèse de doctorat en sciences de gestion, Aix-Marseille Université.

Godé, C., Lebraty J-F. et Barbaroux, P. (2023), "D'un système d'information résilient à un système d'information antifragile : illustrations à partir des organisations militaires », *Les Cahiers Risques et Résilience*, accepté pour publication.

Bouty I., Godé C., Drucker-Godard C., Lièvre P., Nizet J. et Pichault F. (2012). Coordination practices in extreme situations. *European Management Journal*, 30(6), 475-489.

Cao, K, Glaister, S., Pena, A., Rhee, D., Rong, W. et Rovalino, A. (2021). Countering cognitive warfare: awareness and resilience. *NATO Review*. https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html

Chambers, J.A. (2021). Thrust and agility from trust and antifragility: A combatant's guide to expeditionary medical leadership. *Joint Forces Quarterly*, 102, 58-66.

Chevrier, N. (2020). La conduite d'opérations de cyberdéfense. *Brennus 4.0. Lettre d'Information du CICDE*, mars 2020, 5 pages. https://www.penseemiliterre.fr/ressources/30147/18/la_conduite_des_operations_cyber.pdf

De Florio, V. (2014). Antifragility = elasticity + resilience + machine learning models and algorithms for open system fidelity. *Procedia Computer Science*, 32, 834-841.

DIA 6 SIC OPS (2014). Les systèmes d'information et de communication (SIC) en opérations. *CICDE*, n°147/DEF/CICDE/NP. 86 pages.

DIA 3-4-1 (2022). Résilience des Armées. *CICDE*, n°23/ARM/CICDE/NP. 39 pages.

Duchemin, F., Cheyppe, J., Caverne, J-F. et Mon, O. (2018). Les enjeux de l'infovalorisation : quels systèmes d'information pour demain ? *Pensée Mili-Terre*, 49, 13 pages.

Dupin, J.J., Pascal, A. et Godé, C. (2023). A systematic literature review on digital resilience in organizations: Towards a conceptualization. *The Hawaii International Conference on System Sciences (HICSS) 2023*, 1-5.

El Fertasi, N. et De Vivo, D. (2016). Cyber resilience: protecting NATO's nervous system. *NATO Review*. https://www.nato.int/docu/review/articles/2016/08/12/cyber-resilience-protecting-natos-nervous-system/index.html

Frimousse, S. et Peretti, J. (2020). Les répercussions durables de la crise sur le management. *Question(s) de management*, 28, 159-243.

Frimousse, S. et Gaillard, H. (2021). Monde chaotique : au-delà de la résilience, vers l'antifragilité. *Recherches en Sciences de Gestion*, 142, 271-307.

Frimousse, S. (2022). *Guide de l'antifragilité – Domptez l'imprévisible et l'incertain*, Editions EMS, collection Académie des Sciences de Management de Paris.

Godé, C. (2008). Les TIC comme leviers du changement organisationnel : une analyse du cas des Armées américaines en Afghanistan, *Systèmes d'Information et Management*, 13(1), 7-30.

Godé, C. et Barbaroux, P. (2016). Combining technologies' properties to cope with uncertainty: lessons from the military. *International Journal of E-Entrepreneurship and Innovation*, 6(1), 1-18.

Godé, C., De Corbière, F. et Pallud, J. (2020). Les technologies émergentes en contexte extrême : de l'adaptation à l'anticipation ? *Systèmes d'Information Management*, 25 (2), 3-6.

Gorgeon, A. (2015). Anti-fragile information systems. Proceedings of *The 36th International Conference on Information Systems (ICIS)*, 1-19.

Godé, C., Lebraty J-F. et Barbaroux, P. (2023), "D'un système d'information résilient à un système d'information antifragile : illustrations à partir des organisations militaires », *Les Cahiers Risques et Résilience*, accepté pour publication.

Gros, P. (2020). Nouveaux enjeux de l'interopérabilité. *Fondation pour la Recherche Stratégique (FRS)*, 52 pages. https://www.frstrategie.org/sites/default/files/documents/programmes/observatoire-des-conflits-futurs/publications/2021/04.pdf

Gros, P., Tourret, V., Mazzucchi, N., Fouillet, T. et Wohrer, P. (2022). Intégration multimilieux/multichamps : enjeux, opportunités et risques à horizon 2035. *Fondation pour la Recherche Stratégique (FRS)*, 139 pages. https://www.defense.gouv.fr/sites/default/files/dgris/l%27EPS%202021-08%20M2MC%20enjeux%2C%20opportunit%C3%A9s%20et%20risques%20%C3%A0%20l%27horizon%202035-2040.pdf

Hamilton, D.S. (2016). *Forward Resilience: Protecting Society in an Interconnected World.* Washington DC: Center for Transatlantic Relations, 190 pages. ISBN: 978-0-9907721-5-6. http://archive.transatlanticrelations.org/wp-content/uploads/2017/02/Forward_Resilience_Full-Book.pdf

Heeks, R. et Ospina, A.V. (2018). Conceptualising the link between information systems and resilience: A developing country field study. *Information Systems Journal*, 29(1), 70-96.

Hole, K.J. (2016*). Anti-fragile ICT systems*. Simula SpringerBriefs on Computing, Springer Cham.

Hollnagel, E., Woods, D.D., et Leveson, N. (2006). *Resilience engineering. Concepts and precepts*. Hampshire, England: Ashgate.

Pernik, P. et Jermalavicius, T. (2016). Resilience as part of NATO's strategy: Deterrence by denial and cyber defence. In Daniel S. Hamilton (Ed.), *Forward Resilience: Protecting Society in an Interconnected World.* Chapter 9, pp. 99-112. Washington DC: Center for Transatlantic Relations. http://archive.transatlanticrelations.org/wp-content/uploads/2017/02/Forward_Resilience_Full-Book.pdf

Kohn, V. (2023). Operationalizing digital resilience – A systematic literature review on opportunities and challenges. Proceedings of *the 56th Hawaii International Conference on System Sciences*, 6431-6441.

Koninckx, G. et Teneau, G. (2010). *Résilience organisationnelle : rebondir face aux turbulences*. De Boeck Supérieur.

Law, R.L. (2021). State antifragility: An agent-based modeling approach to understanding state behavior. *Old Dominion University - PhD Thesis, International Studies*. 386 pages.

Leonardi, P. (2013). Theoretical foundations for the study of sociomateriality. *Information and Organization*, 23(2), 59-76.

Lété, B. et Dege, D. (2017). NATO cyber-security: A roadmap to resilience. *GMF Policy Briefs*, 23, 6 pages.

Luft, A. (2021). An anti-fragile approach to leadership. *The Army Leader Blog*. https://thearmyleader.co.uk/anti-fragile-leadership/

O'Reilly, B. (2019). No more snake oil: Architecting agility through antifragility. *Procedia Computer Science*, 151, 884-890p.

Orlikowski, W. (2010). The sociomateriality of organisational life: Considering technology in management research. *Cambridge Journal of Economics*, 34, 125–141.

Potosky, D., Godé, C. et Lebraty, J.F. (2022). Modeling the feedback process in teams: A field study of teamwork. *Group & Organization Management*, 47(6), 1218–1258.

RNS (2022). Revue Nationale Stratégique 2022. *Secrétariat Général de la Défense et de la Sécurité Nationale*. 60 pages. http://www.sgdsn.gouv.fr/uploads/2022/11/revue-nationale-strategique-07112022.pdf

Roberts, K., Stout, S. et Halpern, J. (1994). Decision dynamics in two high reliability military organizations. *Management Science*, 40(5), 614–624.

Roux-Dufort, C. (2003). La construction d'une théorie de la fiabilité organisationnelle. *Le sens de l'action, Karl Weick : socio-psychologie de l'organisation*, Vidaillet, B. (dir.), Vuibert.

Russo, D. et Ciancarini, P. (2016). A proposal for an antifragile software Manifesto. *Procedia Computer Science*, 83, 982-987.

Sakurai, M. et Chughtai, H. (2020). Resilience against crises: COVID-19 and lessons from natural disasters. *European Journal of Information Systems*, 29(5), 585-594.

Shea, J. (2016). Resilience: a core element of collective defence. *NATO* Review. https://www.nato.int/docu/review/articles/2016/03/30/resilience-a-core-element-of-collective-defence/index.html.

Simonette, M., Magalhães, M., Bertassi, E. et Spina, E. (2019). Beyond resilience in sociotechnical systems. Proceedings of *The International Symposium on Systems Engineering* (ISSE), 1-4.

Sutcliffe K. et Vogus T. (2003). Organizing for resilience. *Positive organizational scholarship: Foundations of a new discipline*. Cameron, K., Dutton, J. et Quinn, R. (Eds.), San Francisco, CA, Berrett-Koehler, 94-110.

Taleb, N.N. (2012). *Le cygne noir : La puissance de l'imprévisible*. Les Belles Lettres. Traduction française de Taleb, N.N. (2008). *The Black Swan: The impact of the highly improbable*, Penguin.

Taleb, N.N. (2013). *Antifragile : Les bienfaits du désordre*. Traduit de *Antifragile: Things that gain from disorder*, Les Belles Lettres. Traduction française de Taleb, N.N. (2012). *Antifragile: Things that gain from disorder*, Random House.

Taleb, N.N. et Douady, R. (2013). Mathematical definition, mapping, and detection of (anti) fragility. *Quantitative Finance*, 13(11), 1677-1689.

Taleb, N.N. et West, J. (2022). Working with convex responses: Antifragility from finance to oncology. arXiv preprint arXiv:2209.14631.

Tseitlin, A. (2013). The antifragile organization: Embracing failure to improve resilience and maximize availability. *Communication of the ACM*, 56(8), 40-44.

Weick K. (1993). The collapse of sense-making in organizations: The Mann Gulch disaster. *Administrative Science Quarterly*, 38, 628-653.

Weick K. (1995). *Sensemaking in organizations*. Thousand Oaks: Sage.

Weick K. Sutcliffe K. (2015). *Managing the unexpected. Sustained performance in a complex world*. John Wiley & Sons, Inc., Hokoben.

Zhang, W.J. et Lin, Y. (2010). On the principle of design of resilient systems – application to enterprise information systems. *Enterprise Information Systems*, 4(2), 99-110.

Chaînes Telegram

https://t.me/anna_news

Godé, C., Lebraty J-F. et Barbaroux, P. (2023), “D’un système d’information résilient à un système d’information antifragile : illustrations à partir des organisations militaires », *Les Cahiers Risques et Résilience*, accepté pour publication.

https://t.me/rybar

https://t.me/conflictzone

https://t.me/pilotblog