Mémoire

EGE Ecole de Guerre Economique

1 École de Guerre Économique

Mémoire de MBA

Management de la Cybersécurité et Gouvernance des Systèmes d'Information

Présenté et soutenu par

F. DELIGNETTE, C. KAYA, M. ROUSSEAU et G. TURLAN

L'Intelligence économique comme facteur de performance de la cybersécurité : une voie vers l'accroissement de puissance de la France et de ses entreprises

Mémoire dirigé par Fabien RENAUDIN et Christian HARBULOT

JURY :

- M. Fabien Renaudin, Chef du bureau Management des Risques Cyber à l'ANSSI
- M. Laurent Barrat, Adjoint au RSSI et Responsable du Système de Management de la Sécurité de l'Information de la Direction interministérielle du numérique
- M. Guy-Philippe Goldstein, auteur, chercheur, conseiller stratégique chez Expon Capital
- M. Thiebault Meyer, directeur cybersécurité chez Google Cloud

L'art de la guerre, c'est l'art de garder sa liberté d'action.
Xénophon

Remerciements

Nos remerciements vont à **Fabien RENAUDIN**, Chef du bureau Management des Risques Cyber à l'ANSSI, qui a dirigé ce travail, nous orientant dans nos réflexions.

Nous remercions également vivement tous les intervenants qui ont nourri la réflexion de notre groupe de travail (ordre alphabétique) :

- Nicolas ARPAGIAN, Directeur de la Stratégie et des Affaires publiques, Orange Cyberdefense
- Antoine CHAUVOT, étudiant à l'École Normale Supérieure de la rue d'Ulm « département sciences sociales, méthodes quantitatives », et doctorant (Sorbonne - sciences politiques)
- Thomas FAURE, fondateur et président de la plateforme collaborative Whaller
- Benoît FUZEAU, Responsable de la Sécurité des systèmes d'information à la CASDEN, Président du CLUSIF (ARUP)
- Xavier LEPAGE, Professeur associé « stratégie & intelligence économique » à l'EGE, Conférencier + *serious game designer* à IHEDN
- Guy-Philippe GOLDSTEIN, Professeur « Cyberdéfense & Cyberpuissance » à l'EGE, auteur, chercheur, conseiller stratégique chez Expon Capital
- Alfred HUOT de SAINT-ALBIN, responsable pôle fraude, Orange Cyberdéfense
- Michel SEJEAN, Professeur de droit privé à l'Université de Paris XIII, Directeur scientifique du Code de la Cybersécurité Dalloz
- Martin UNTERSINGER, journaliste au journal *Le Monde*
- Mohamed SAYED GAFFAR, Senior BID Manager Défense CLOUD chez THALES SIX FRANCE
- Jeremy COUTURE, Head of Lottery Cybersecurity, CISO chez FDJ
- Yannick PECH, enseignant-chercheur en intelligence économique et cybersécurité

Droits d’auteurs

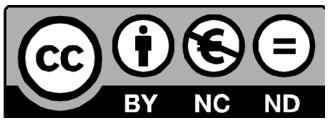


Table des matières

Table des illustrations

Table des tableaux

Introduction

Au mois de mai 2025, suite à l'émission d'un mandat d'arrêt international par la Cour pénale internationale de La Haye à l'encontre du premier ministre Benjamin Netanyahu et d'autres responsables, et sur demande de l'administration du nouveau président américain Donald Trump, Microsoft a suspendu l'accès du président de la CPI - Karim Khan - à sa boîte mail[1]. De plus, ses comptes bancaires au Royaume-Uni ont été gelés, et le personnel de la CPI a été averti des risques d'arrestation s'il entrait aux États-Unis[2].

Une décision qui conduit à s'interroger sur l'(in)dépendance de la justice internationale, et surtout qui a constitué un choc pour l'Europe dans la mesure où le président de Microsoft venait de défendre la souveraineté numérique face aux aléas géopolitiques, lors d'une récente visite à Bruxelles. Peut-être trop vite rassurés, les Européens négligeaient ainsi un axiome de base de la realpolitik : peu importe les liens d'amitié et les relations commerciales entre partenaires, un fournisseur stratégique étranger est également régi par le cadre légal d'un gouvernement étranger… et généralement le sien (surtout lorsqu'il est américain) !

Cet évènement constitue bien un incident de cybersécurité puisqu'il porte atteinte à la disponibilité d'un service et des données liées. On en déduit que la vulnérabilité repose dans la dépendance envers une entreprise étrangère pour la fourniture d'un service essentiel à la communication, et que la menace correspond à une législation américaine particulièrement offensive et contraignante. Il ne s'agit pas d'une faille technique ou humaine, mais d'une faille de confiance puisant sa source dans une faille juridique. Or ces failles remettent en cause la liberté d'action de la Cour pénale. Ce risque avait-il été suffisamment pris au sérieux, pensé et envisagé au moment de la contractualisation avec Microsoft ? L'arrivée de Donald Trump à la présidence des Etats-Unis d'Amérique constitue un moment de dévoilement et de basculement car, jusqu'à récemment, ce risque était souvent alors considéré comme théorique, car jamais mis en œuvre de manière aussi frontale et brutale. On pouvait feindre d'ignorer le réel, la menace… A la lumière de cet évènement, la liste des administrations et entreprises françaises sous *cloud* et environnement numérique étranger donne le tournis et fait craindre le pire… tandis que de nombreuses institutions, en Allemagne ou aux Pays-Bas, cherchent déjà des alternatives.

En toile de fond de cet incident révélateur, la transformation numérique des acteurs publics et privés s'est accompagnée de la production d'une grande quantité de données. Or blanc du vingt-et-unième siècle, cet incroyable stockage et production de données au niveau mondial constitue un levier de croissance fort dont le traitement et l'analyse permettent la constitution d'informations stratégiques et vitales. Accompagnant cette transformation, la cybersécurité est logiquement devenue ces dernières années une préoccupation majeure des organisations de toute taille et de toute nature, les États et les acteurs privés prenant progressivement conscience des enjeux stratégiques liées au stockage, traitement et

[1] Owen Sayers. « Microsoft coupe les mails de la Cour Pénale Internationale, un avertissement pour tous les Européens », LeMagIT, 27-. https://www.lemagit.fr/actualites/366624982/Microsoft-coupe-les-mails-de-la-Cour-Penale-Internationale-un-avertissement-pour-tous-les-Europeens.

[2] « Telex : Le compte Microsoft du procureur de la CPI suspendu, Vincent Villette nommé secrétaire général de la Cnil », *Le Monde Informatique*, 19 mai 2025. https://www.lemondeinformatique.fr/actualites/lire-telex-le-compte-microsoft-du-procureur-de-la-cpi-suspendu-vincent-villette-nomme-secretaire-general-de-la-cnil-un-datacenter-pour-chauffer-l-eau-de-brassage-d-une-biere-96874.html.

transmission de ces informations. En effet, de nombreux acteurs de natures différentes cherchent à voler ces données, et à utiliser le cyberespace tant comme nouveau territoire de la compétition économique féroce des agents économiques, que comme l'expression de la volonté de puissance des États.

Pour que ce travail soit pleinement compréhensible, il suppose plusieurs postulats. Tout d'abord celui de la bonne compréhension de la place qu'est en train de prendre ce continent numérique et immatériel que constitue le cyberespace. Territoire innervant, il deviendra de plus en plus stratégique et incontournable au fur et à mesure qu'il deviendra le substrat de tous les autres milieux (terre, air, mer, espace). Deuxièmement, il suppose d'accepter la conflictualité du monde, c'est-à-dire de "voir ce que l'on voit". Non pas la conflictualité rassurante entre l'alliance des États "gentils" d'un côté et les États "méchants" de l'autre, mais celle entre tous les États, qui mobilisent leurs ressources au service de l'accroissement de leur puissance. Cette conflictualité à 360° s'illustre au travers d'une loi d'airain de l'Histoire : quand un État (et donc un peuple) refuse ce jeu de la quête de l'accroissement de puissance, il disparaît ou décline.

Ce qui évolue à travers l'histoire, ce n'est pas cette lutte, cette compétition pour persévérer dans son être (souvent au détriment de l'être des autres), ce sont les visages de cette lutte. L'absence de conflits armés, ce n'est pas l'absence de compétition et de lutte(s). Enfin, ce travail suppose que, collectivement, c'est-à-dire en tant que Nation, nous prenions conscience de notre faiblesse la plus importante : nous avons, a minima, sous-estimé cette conflictualité dans notre rapport au monde. Et les conséquences en sont importantes : nous n'avons plus de réponse à deux questions fondamentales : "quelle puissance voulons-nous être ? Quel est le chemin pour y parvenir ?". Ce n'est pas la Puissance qui a changé de mains, c'est nous qui avons déserté la Puissance.

Fort de cette clarification, comment appréhender aujourd'hui la cybersécurité à l'aune de ce réel plus volatile, incertain, complexe et ambigüe ? L'approche prédominante, que nous avons choisi de nommer « technico-financière », permet-elle encore de produire une cybersécurité efficace, au service des intérêts stratégiques de l'entreprise ? D'autres cadres de réflexion, d'autres manières d'étudier une situation donnée, d'autres méthodologies n'auraient-ils pas permis de prévenir cet évènement, en limitant à la fois la probabilité d'occurrence et la gravité d'impact ? Plus spécifiquement, l'apport de l'intelligence économique, parce qu'elle contribue à dévoiler la conflictualité des rapports économiques et politiques entre nations prétendument « amies », parce qu'elle améliore la perception d'une situation donnée, n'aurait-elle pas amélioré la gouvernance de la cybersécurité de cette organisation internationale ? **L'intelligence économique peut-elle constituer un facteur de performance de la cybersécurité dans les entreprises ?**

En réponse à cette question particulièrement sensible, dans la mesure où celle-ci aura un impact important sur la meilleure manière d'assurer la sécurité de ses actifs informationnels, **nous pensons en effet que l'intelligence économique doit constituer une ressource essentielle pour améliorer la gouvernance de la cybersécurité dans les entreprises, notamment parce qu'elle permet d'aligner profondément celle-ci avec la stratégie totale de l'entreprise, parce qu'elle renforce la liberté d'action de cette dernière.** Préserver l'indépendance des organisations, c'est-à-dire leur capacité à déterminer souverainement les orientations qu'elles souhaitent se donner et les moyens qu'elles souhaitent mobiliser, tel est l'enjeu d'une cybersécurité rénovée par l'apport de l'intelligence économique. Parce que l'intelligence économique permet de rendre plus intelligible l'état de guerre économique, elle

permet également d'en conclure que tout ce qui contribue à la liberté d'action des agents économiques ne peut et ne doit pas être négligé. Or c'est exactement ce qu'apporte cette gouvernance rénovée de la cybersécurité : une politique de protection du capital informationnel au service de la liberté d'action de l'entreprise, afin que celle-ci puisse mettre en œuvre sa stratégie de développement et de puissance.

Pour démontrer cette position, cette option préférentielle pour faire entrer la cybersécurité dans une démarche d'intelligence économique, la première partie présentera les hypothèses de base, servant de socle à la démonstration, et dressera un état des lieux de la gouvernance de la cybersécurité dans les entreprises françaises. Dans un deuxième temps seront explicités la relation entre cette gouvernance de la cybersécurité et la grande stratégie des entreprises, ainsi que l'apport de l'intelligence économique à la cybersécurité. Puis la troisième partie de ce document se consacrera au rôle de l'État comme soutien et facilitateur d'une plus grande vision et autonomie des acteurs privés et publics dans le cyberespace en favorisant un positionnement pertinent. La quatrième partie présentera une gouvernance de la cybersécurité largement rénovée par l'intelligence économique qui impactera l'organisation et l'affectation des moyens de l'entreprise. Elle posera également les bases théoriques et conceptuelles d'un modèle de maturité de la stratégie de cybersécurité. Ce modèle de maturité sera présenté de manière détaillée dans la cinquième partie qui ne manquera pas de s'appuyer sur les quatre piliers énoncés précédemment : cybersécurité, intelligence économique, vision et positionnement, organisation et moyens. Nous conclurons ce mémoire par une présentation succincte d'un cadre de gouvernance de la cybersécurité et des transformations de l'entreprise.

Ce travail de réflexion s'adresse en premier lieu aux personnes portant la responsabilité de la stratégie au sein de leur organisation, qu'elle que soit sa taille et son secteur d'activité, afin qu'elles y trouvent matière à réflexion pour préparer toujours mieux leur organisation à affronter les défis futurs. En second lieu, les personnes portant la charge de la sécurité et de la sûreté du patrimoine informationnel pourront mieux comprendre, si tant est que ce besoin existe, le contexte géo-économique dans lequel leur organisation évolue, et ce qu'elles peuvent donc proposer pour améliorer cette gouvernance de la cybersécurité.

I. Etat des lieux de la cybersécurité

Entreprendre une telle réflexion sur l'apport de l'intelligence économique à la gouvernance de la cybersécurité sans prendre soin de définir le cadre et le socle de cette réflexion ne pourrait qu'amener à la confusion. Dans la mesure où l'introduction générale ne pouvait absorber à elle seule ce besoin de clarification, ce sera l'objet de cette première partie. Y seront successivement traités la description du paradigme stratégique contemporain, la présentation du concept de « stratégie totale » et son intérêt pour mieux comprendre la finalité de la cybersécurité, l'intérêt et le rôle d'un système de management de la sécurité de l'information, la définition de l'approche « technico-financière » de la cybersécurité.

I.1 La primauté contemporaine du mode stratégique indirect

Pour comprendre les enjeux géo-économico-stratégiques contemporains, c'est-à-dire le rôle de l'économie dans la compétition entre puissances, il est indispensable de comprendre les règles du jeu régissant les rapports entre les Etats.

Les rivalités entre puissances s'expriment aujourd'hui majoritairement selon le mode stratégique indirect, après un très long règne du mode stratégique direct. Le général André Beaufre définit la stratégie directe comme « *le mode stratégique où la force représente un facteur essentiel*[3] ». Tandis que le mode stratégique indirect se définit par *« la recherche de la décision par des actions plus ou moins insidieuses de caractère politique, diplomatique ou économique. (…) C'est une stratégie qui correspond aux cas où la plage de liberté d'action de la force est étroite.*[4] »

On peut citer plusieurs causes à ce changement de mode stratégique : l'avènement de l'ère atomique et donc la crainte d'une montée aux extrêmes qui ne puisse être maîtrisée, l'écœurement du recours à la force en Occident suite aux conséquences des deux guerres mondiales, la délégitimation de la guerre comme mode de règlement des différends entre nations, la mondialisation économique ayant abouti à une situation de forte interdépendance entre les pays...

La primauté de ce mode stratégique indirect sur celui direct s'illustre de plusieurs manières. La guerre froide a parfaitement illustré cette prévalence puisque les deux Etats qui s'opposaient ont finalement toujours cherché à éviter un affrontement militaire direct, préférant l'espionnage, la compétition technologique, les manipulations d'opinion, mais aussi l'utilisation de conflits périphériques pour tenter d'accroître leur influence. Ce dernier exemple permet de préciser qu'au sein du mode stratégique indirect, le conflit, et donc la stratégie militaire, peut être employé. C'est alors toujours de manière annexe, périphérique, marginale. Aujourd'hui, le remplacement du triptyque paix-crise-guerre par le triptyque compétition-contestation-affrontement illustre également la prévalence du mode stratégique indirect. C'est dans le cadre de ce triptyque qu'il faut penser l'émergence des menaces dites « hybrides » (ce triptyque sera présenté de manière détaillée dans la partie II.4.3).

[3] A. Beaufre, Introduction à la stratégie, op. cit., p.183.

[4] André Beaufre., p.40.

I.2 Stratégie totale et stratégie de cybersécurité

Dans cette sous-partie, seront définies les notions de cybersécurité, de stratégie totale et de gouvernance appliquée à la cybersécurité.

I.2.1 Cybersécurité

L'Agence Nationale de la Sécurité des Systèmes d'Information donne la définition suivante de la cybersécurité : « état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptible de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.[5] »

Cette définition particulièrement claire et complète appelle un certain nombre de commentaires.

La cybersécurité correspond à un niveau de maturité organisationnelle, humaine, physique et technologique recherché pour permettre à un système d'information de résister à des événements malveillants ou accidentels issus du cyberespace, susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises, ainsi que des services associés. On en comprend que la cybersécurité aide l'entreprise à assurer tant la **sécurité** (protection contre un évènement malveillant) que la **sûreté** (protection contre un évènement accidentel) des informations détenues dans le cyberespace.

La cybersécurité mobilise des techniques issues de la sécurité des systèmes d'information, contribue à la lutte contre la cybercriminalité, et s'exerce dans le cyberespace — c'est-à-dire l'espace numérique constitué de réseaux interconnectés, dans lequel circulent les données et s'exécutent les services numériques. Elle n'est pas fondée sur la cyberdéfense, mais la précède dans l'échelle d'intensité des réponses : la cyberdéfense intervient en complément dans des contextes critiques, stratégiques ou souverains, notamment face à des menaces étatiques ou de haute intensité.

Enfin, la cybersécurité s'étend également à la protection de certains actifs immatériels dans l'environnement numérique, tels que les idées, la propriété intellectuelle, ou les modèles sensibles des organisations.

[5] « Le CyberDico | ANSSI », s. d. https://cyber.gouv.fr/le-cyberdico.

Une façon de gérer le développement et la maturité de cette cybersécurité est présentée dans la figure suivante.

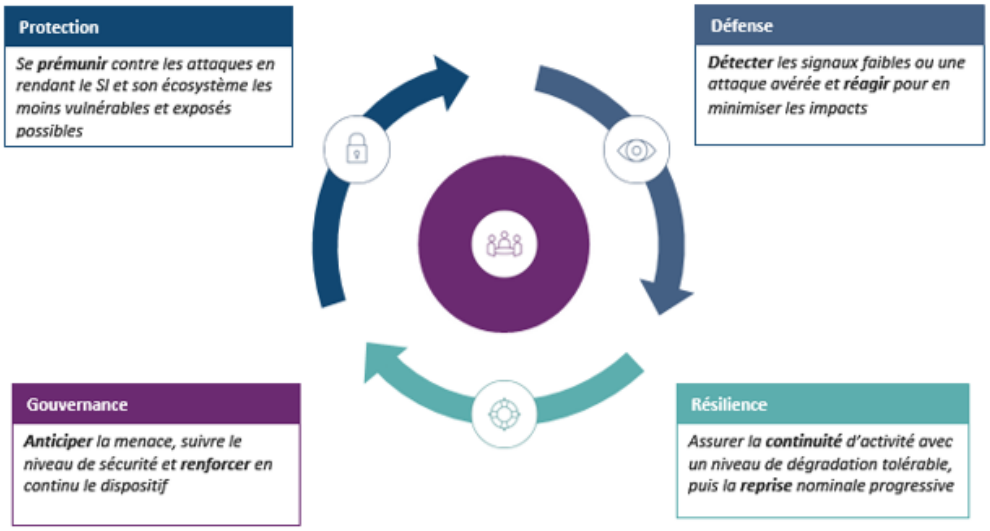


Figure 1 - Structurer ses mesures de sécurité

Source : https://cyber.gouv.fr/structurer-ses-mesures-de-securite

Selon l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), le risque numérique représente aujourd'hui une menace stratégique majeure pour les organisations. Contrairement à d'autres formes de risques, il est qualifié de systémique, potentiellement « mortel », inévitable, et non délégable. En ce sens, la cybersécurité ne peut être perçue comme une simple fonction technique externalisée, mais doit être intégrée de manière intrinsèque à la culture organisationnelle. Les dirigeants et les responsables métiers sont donc appelés à s'approprier pleinement ces enjeux, en assumant leur part de responsabilité dans la gouvernance de la sécurité numérique.

I.2.2 Stratégie totale :

Au sujet des acteurs économiques, l'expression de « stratégie de développement » est souvent rencontrée, alors que le terme de stratégie n'est souvent pas défini précisément.

Figure 2 - *Introduction à la stratégie*, édition de 1998

Nous avons choisi de nous inspirer d'une définition provenant de la pensée militaire, car c'est dans ce contexte qu'est né ce terme. En France, le général André Beaufre a beaucoup apporté, au vingtième siècle, à la compréhension de la notion de stratégie et de tous ses corolaires. Il en donne la définition suivante : « *art de la dialectique des volontés employant la force pour résoudre leur conflit*[6] ». Dans l'optique de notre réflexion, nous nous sommes concentrés sur les conséquences de cette définition, sur l'étude approfondie de la notion de « stratégie ». Ainsi, le général Beaufre écrit dans le même ouvrage : « *la stratégie se subdivise nécessairement en stratégies spécialisées valables uniquement pour un domaine particulier.*[7] », puis un peu plus loin : « *on se trouve ainsi en présence d'une véritable pyramide de stratégies distinctes et interdépendantes qu'il est indispensable de bien définir pour pouvoir les combiner au mieux dans un faisceau d'actions visant le même but d'ensemble.*[8] ». L'auteur donne plusieurs exemples de ces « stratégies distinctes et interdépendantes » : militaire évidemment, mais aussi économique, diplomatique, politique (la plus importante), psychologique / morale… Au sommet de cette pyramide, il place le concept de « stratégie totale », ou de « grande stratégie » (synonyme employé par Liddel Hart, grand stratège anglais). Or ce concept est central, agissant tel une clé de voûte, à tel point que le général Beaufre a écrit : « *Il n'est de bonne stratégie que totale*[9] ».

Figure 3 - La grande stratégie d'un pays

Il est tout à fait possible de raisonner par analogie avec le monde de l'entreprise où les acteurs définissent également des stratégies. Si la « dialectique des volontés » s'applique très bien au monde économique en faisant référence à la concurrence que se livre les entreprises, la « résolution des conflits » nécessite d'être adaptée. Non pas qu'il n'y ait pas de situation conflictuelle dans l'économie de marché mondialisée contemporaine comme cela sera démontré par la suite, mais ce n'est pas avant tout la « force » qui est employée pour les résoudre. D'où d'ailleurs l'intérêt de la démarche d'intelligence économique pour aider à

[6] André. Beaufre, Introduction à la stratégie, Paris, Hachette, 1998, p.34.
[7] Ibid, p.45.
[8] Ibid, p.45.
[9] André Beaufre et François Géré, La stratégie de l'action, Nouv. éd., La Tour-d'Aigues, Éd. de l'Aube, 1997, p.130.

comprendre la complexité des situations auxquelles doivent faire face les agents économiques, ainsi que leurs méthodes employées pour résoudre leurs conflits, c'est-à-dire la captation de nouvelles parts de marché pour accroître leur richesse et leur puissance. Il est donc possible de concevoir que chaque entreprise devrait définir une « stratégie totale », ou « grande stratégie », qui se subdiviserait en stratégies « distinctes et interdépendantes » : inventions / innovations, ressources humaines, marketing, juridique, commerciale… et cybersécurité évidemment ! **La stratégie de cybersécurité devient donc, avec ce référentiel, un sous-système qui concourt à la réalisation de la stratégie totale de l'entreprise.**

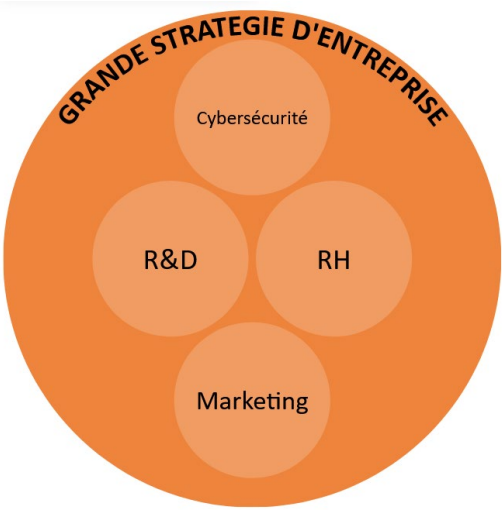
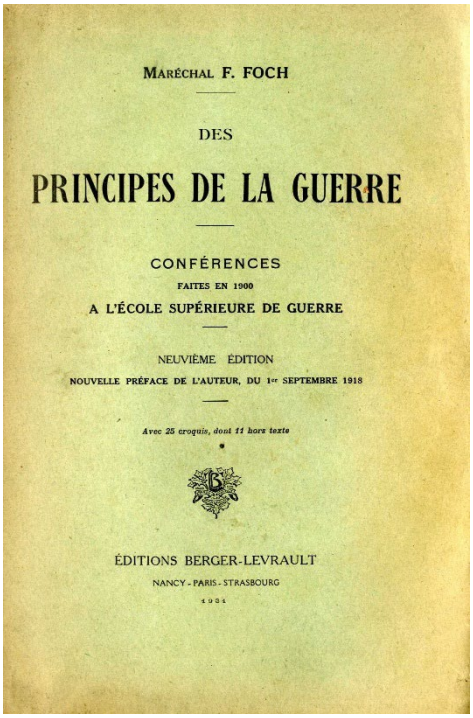


Figure 4 - La grande stratégie d'une entreprise


MARÉCHAL F. FOCH

DES

PRINCIPES DE LA GUERRE

CONFÉRENCES
FAITES EN 1900
A L'ÉCOLE SUPÉRIEURE DE GUERRE

NEUVIÈME ÉDITION
NOUVELLE PRÉFACE DE L'AUTEUR, DU 1er SEPTEMBRE 1918

Avec 25 croquis, dont 11 hors texte

ÉDITIONS BERGER-LEVRAULT
NANCY - PARIS - STRASBOURG
1931

Figure 5 - *Des principes de la guerre*, édition de 1906

Pour mieux comprendre comment se réalise une stratégie, qu'elle soit « totale » ou « distincte et interdépendante », il faut revenir à la pensée militaire qui a trouvé dans la notion de « liberté d'action » l'élément indispensable à la réalisation de toute stratégie. En effet, on peut définir cette notion comme la capacité d'être autonome dans la prise de décisions, et de les mettre en œuvre sans entrave. Le général Vincent Desportes éclaire sur le rôle fondamental de cette liberté d'action au service de la stratégie : *« La stratégie est l'art de l'action, mais aussi l'art « pour » l'action : elle doit produire des résultats. (…) Le stratège doit pouvoir agir : l'art de penser l'action n'a d'intérêt qu'à la condition d'être libre de la mettre en œuvre. Stratégie et liberté d'action sont indissociables à ce point que la seconde est la condition même de la première, mais également son cœur. Acteur-observateur de la guerre du Péloponnèse, élu stratège en son milieu, Thucydide*[10] *conclut de cette expérience : « L'art de la guerre est l'art de garder sa liberté d'action. » C'est pour contenir l'hégémonie d'Athènes, et donc recouvrer sa liberté d'action, que Sparte se lance dans cette aventure dont elle sort vainqueur après avoir réussi à détruire l'instrument essentiel de la liberté d'action athénienne : sa flotte.* [11] » Bien avant le général Desportes, le maréchal Foch, dans son livre *Des principes de la guerre*, avait identifié la liberté d'action comme le principal principe fondamental de la stratégie militaire. Il la définit comme le fait, pour le stratège, de pouvoir

[10] Suite à des recherches ayant pour objet de trouver la source de cette citation, il est beaucoup plus probable que ce soit en réalité Xénophon qui l'ait prononcée ou écrite, et non Thucydide.
[11] Vincent Desportes. « Stratégie et liberté d'action », Politique étrangère, nº 1 (6 mars 2018) : 133-42. https://doi.org/10.3917/pe.181.0133.

choisir comment il va agir et d'agir comme il le souhaite. De manière très éclairante et opportune pour notre travail, il met en relation ce principe avec celui de la sûreté qui vise à « *se soustraire à la volonté [adverse], de parer aux entreprises par lesquelles il pourrait nous empêcher d'aboutir*[12] ». Autrement rédigé, la sûreté*, « c'est la protection de sa propre la liberté d'action*[13] », en mettant l'accent sur la nécessité d'agir en sécurité et en connaissance de cause, en anticipant les menaces et en se protégeant contre les surprises.

En poursuivant l'analogie avec le monde économique, la liberté d'action conserve toute son intérêt. Toute stratégie totale n'a de valeur que si elle peut être mise en œuvre. Or, au service de la liberté d'action, en amont, il y a le principe de sûreté. Il est également tout à fait possible de paraphraser Xénophon ainsi : l'art de la guerre économique est l'art pour l'entreprise de garder sa liberté d'action. Or qu'est-ce que la cybersécurité si ce n'est une activité au service de la sûreté, donc de la liberté d'action, donc de la stratégie totale d'une entreprise ? **La stratégie de cybersécurité, pour révéler tout son potentiel, doit donc être pensée comme une stratégie au service de la liberté d'action de l'entreprise permettant de mettre en œuvre la stratégie totale de celle-ci, dans la mesure où elle contribue à réaliser le principe de sûreté.**

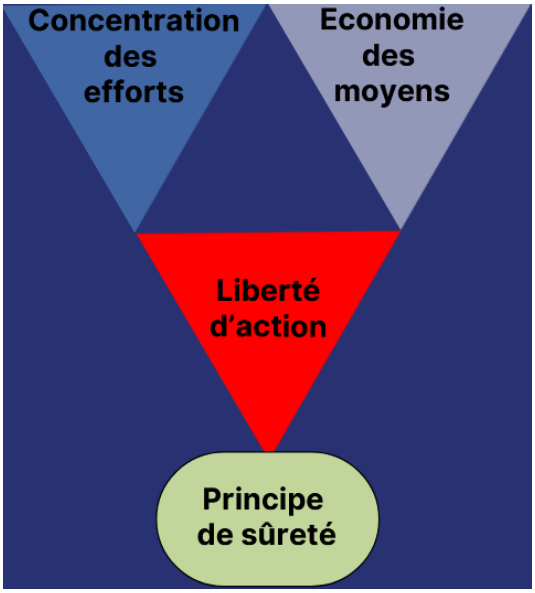


Figure 6 - Les principes de la guerre selon Foch

On pourrait opposer à cette vision que la « stratégie totale » est une option, ou un objet d'étude pour académies militaires, et donc que l'ordonnancement, la subordination d'une stratégie de cybersécurité à une stratégie totale n'en a pas plus de valeur… Il faut alors citer de nouveau le général Beaufre qui a été un praticien de la stratégie militaire dans des fonctions toujours plus élevées, tout au long de la deuxième moitié de ce vingtième siècle d'acier, de feu et de sang : « *Faute d'une stratégie, nous avons été constamment incapables de comprendre les manœuvres par lesquelles on cherchait à nous réduire, et nous avons régulièrement fait porter nos efforts sur des impasses.*[14] ».

[12] Ferdinand Foch, Des principes de la guerre, Deuxième édition Paris, Berger-Levrault & Cie, 1906, 341 p., p.96.
[13] A. Beaufre, Introduction à la stratégie, op. cit., p.184.
[14] André. Beaufre, Introduction à la stratégie, op. cit, p.23.

I.2.3 L'état de guerre économique :

A ce stade de la réflexion, il est établi que le mode stratégique indirect prévaut, et que toute stratégie nationale, ou totale, se compose nécessairement d'un orchestre de stratégies subordonnées, distinctes mais interdépendantes. Il s'agit désormais de comprendre quel est le rôle de la stratégie économique, et quelles conséquences il faut en tirer.

Puisque la stratégie militaire ne peut plus constituer le fer de lance de l'accroissement de puissance, ce rôle est désormais dévolu à la stratégie économique, c'est-à-dire la création par un Etat d'un environnement favorable au développement et à l'enrichissement des acteurs économiques privés nationaux, qui par des effets bénéfiques directs et indirects renforceront la puissance de la Nation.

Parmi ces effets bénéfiques on peut citer la création d'emplois, l'augmentation des recettes fiscales, l'attractivité matérialisée par l'augmentation des investissements directs à l'étranger, des cycles vertueux d'innovation et la création de propriété intellectuelle... D'autres stratégies sont mises en œuvre dans le cadre de cette stratégie totale, au service de l'accroissement de puissance.

Concernant la France, on peut citer d'autres stratégies qui contribuent, de manière mineure et annexe, à la bonne exécution de la stratégie totale. Tout la stratégie diplomatique grâce à un nombre de consulats et d'ambassades particulièrement important, permettant de nouer des relations avec de nombreux Etats, de comprendre les enjeux locaux et régionaux, de faciliter l'insertion d'entreprises françaises, etc. La stratégie culturelle s'avère particulièrement importante pour la France, puisqu'elle consiste à utiliser la riche histoire, le patrimoine, la gastronomie, la langue (francophonie), les valeurs (patrie des droits de l'homme) comme vecteur de rayonnement et d'attraction. Toutefois, aucune de ces stratégies ne s'avère aussi puissante et dimensionnante que la stratégie économique dans un contexte de libre circulation des biens, des services et des capitaux. (Les alliances françaises, copiés par les Instituts Confucius et les Goethe Institut, etc.).

C'est donc dans cette situation où la stratégie économique « emporte la décision », pèse le plus au sein de la stratégie totale, que l'état de guerre économique devient crédible, que cette expression permet le mieux de comprendre le réel. La guerre économique, dans un contexte de stratégie indirecte, c'est la continuation de la stratégie totale par d'autres moyens que la stratégie militaire, pour paraphraser la formule célèbre de Karl Von Clausewitz. La guerre économique peut se définir par un état de concurrence particulièrement féroce entre les agents économiques, où les Etats mettent leur puissance régalienne au service de la performance de leurs entreprises, afin qu'elles remportent cette compétition. En effet, comme cela sera décrit grâce au recours à l'outil de l'intelligence économique dans la deuxième partie de cet ouvrage, les Etats utilisent leurs acteurs économiques pour s'affronter, utilisent la conquête de marchés et l'innovation comme un moyen d'expression de leurs rivalités. Bref, les Etats utilisent la stratégie économique comme facteur d'accroissement de leur puissance. Pour conclure et l'exprimer autrement, il y a guerre économique lorsque la stratégie économique est devenue le facteur essentiel de la stratégie totale d'une nation, en remplacement de la stratégie militaire, parce que c'est là que la liberté d'action y est la moins « étroite ».

I.2.4 Gouvernance et stratégie d'entreprise

Puisque la stratégie de cybersécurité concourt à la réalisation de la stratégie totale de l'entreprise, alors la gouvernance d'entreprise et la cybersécurité sont désormais étroitement liées dans le contexte des organisations modernes. La gouvernance d'entreprise définit le cadre global de direction, de contrôle et de responsabilité, tandis que la gouvernance de la cybersécurité s'inscrit comme un volet essentiel de ce cadre.

Voici quelques points clés de leur relation :

Gouvernance : La gouvernance de la cybersécurité[15] désigne l'ensemble des processus, politiques, structures et mécanismes mis en place pour garantir la protection des actifs numériques d'une organisation. Elle s'intègre dans la gouvernance totale de l'entreprise et vise à assurer la continuité des activités, la conformité réglementaire et la gestion efficace des risques liés aux technologies de l'information. Une gouvernance totale efficace supervise la définition, l'exécution et la mise à jour régulière d'une stratégie de cybersécurité adaptée à l'évolution des menaces et des besoins internes. Elle implique également la coordination des différents acteurs (équipes techniques, sécurité, juridique, métiers) et l'allocation des ressources nécessaires à la protection des systèmes et données. **La gouvernance de la cybersécurité, c'est donc la traduction en acte de la stratégie de cybersécurité, puisqu'elle concourt à la réalisation du principe de sûreté.**

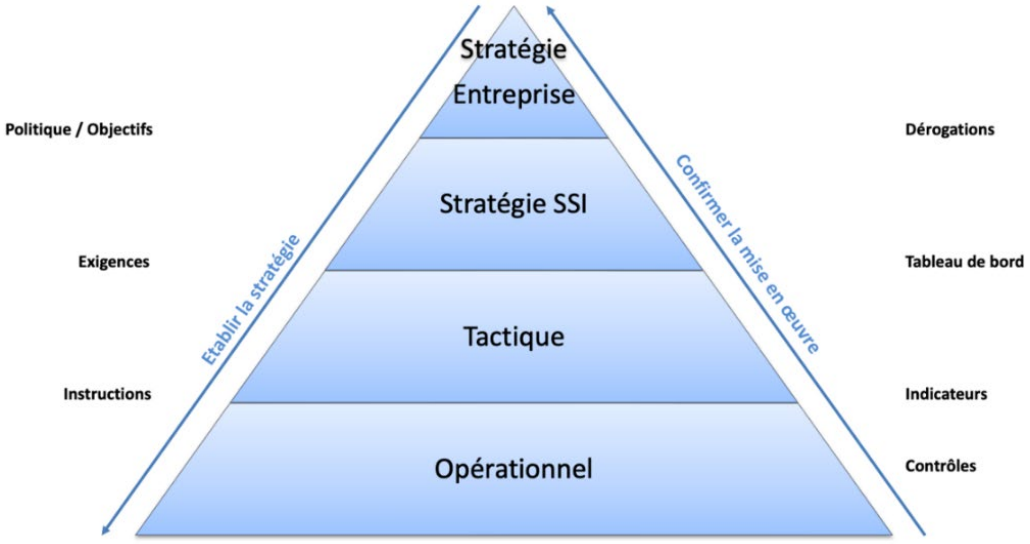


Figure 7 - Pyramide de la gouvernance

Source : Cours Organisation SSI – Laurent Barrat, MaCyb 07, EGE

- Alignement stratégique : comme cela est expliqué dans la figure ci-dessus, la gouvernance de la cybersécurité a pour vocation d'assurer un alignement étroit entre les objectifs de sécurité numérique et la stratégie totale de l'entreprise. Dans un contexte où les menaces sont de plus en plus rapides, sophistiquées et ciblées, cet alignement devient un levier fondamental pour garantir la performance durable et la résilience organisationnelle. En intégrant une approche continue de la sécurité, combinant exigences de conformité et réactivité face aux cybermenaces réelles, la

[15] Le rôle essentiel de la gouvernance dans la cybersécurité », 10 juillet 25p.

gouvernance ne se limite plus à un rôle de contrôle. Elle devient un vecteur d'agilité stratégique, permettant aux RSSI de piloter la sécurité comme une fonction métier à part entière, au service des enjeux de transformation numérique, d'innovation, et de compétitivité globale.

- Gestion des risques : La gestion des risques est un pilier central de la gouvernance de la cybersécurité puisque cette activité identifie et traite les évènements de sécurité et de sûreté qui pourraient porter atteinte à la liberté d'action de l'entreprise. Elle comprend l'identification, l'évaluation et la hiérarchisation des menaces et vulnérabilités susceptibles d'affecter la liberté d'action de l'organisation.
    - Ce processus implique :
        - L'inventaire des actifs informatiques / valeurs métiers critiques ;
        - L'analyse des menaces potentielles et des vulnérabilités existantes ;
        - L'évaluation de l'impact et de la probabilité des incidents ;
        - La mise en place de plans de prévention, de détection et de réponse aux incidents.
- Une mise en parallèle des démarches d'analyse de risque selon la méthode EBIOS Risk Manager et la norme ISO/IEC 27005 est fondamentale. Comme le mettent en évidence les deux approches complémentaires de la gestion des risques en cybersécurité décrites dans la figure ci-après : d'une part, EBIOS RM articule son processus autour de cinq ateliers structurés selon un enchaînement logique entre cycle stratégique et cycle opérationnel, visant à identifier les actifs critiques, les sources de menace, les scénarios d'attaque et les mesures de traitement associées ; d'autre part, la norme ISO 27005 repose sur un processus en cinq étapes de l'établissement du contexte à la mise en œuvre des traitements des risques encadré par des activités transverses de communication, de concertation, de surveillance et de revue. Cette comparaison illustre la complémentarité entre une approche orientée par les scénarios d'attaque (EBIOS) et une démarche plus normative et systématique (ISO 27005) dans la gouvernance des risques liés à la sécurité de l'information.

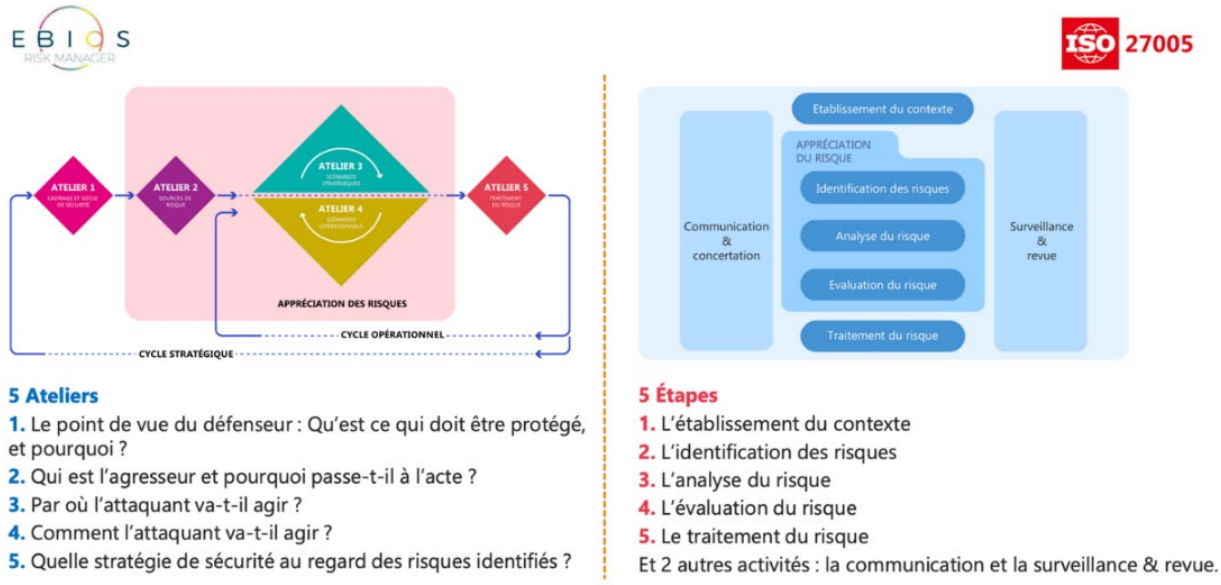


Figure 8 - EBIOS RM vs ISO 27005 : 2022

- Responsabilités et pilotage : La gouvernance attribue des rôles et responsabilités clairs à tous les niveaux de l'organisation. La direction générale, les comités spécialisés (audit, risques, sécurité) ainsi que les responsables de la sécurité (RSSI, DSI) participent activement à la définition des politiques, à la supervision et à la prise de décision en matière de cybersécurité. Ce pilotage transversal garantit une cohérence des actions, une répartition optimale des ressources et une capacité à répondre rapidement aux enjeux émergents. La gouvernance s'assure également que les responsabilités sont bien comprises et assumées par chaque acteur, favorisant ainsi la responsabilisation individuelle et collective.
- Culture de la sécurité : La diffusion d'une culture de la sécurité est essentielle pour renforcer la résilience de l'organisation face aux risques numériques, pour améliorer la réalisation du principe de sûreté. La gouvernance encourage et organise des programmes de sensibilisation et de formation pour tous les collaborateurs, du *top management* aux équipes opérationnelles[16]. Ces initiatives visent à :
    - Informer sur les risques et les bonnes pratiques (ex : gestion des mots de passe, vigilance face aux courriels suspects)
    - Développer les compétences techniques et comportementales nécessaires
    - Impliquer les partenaires externes dans la démarche de sécurité
    - Instaurer une vigilance partagée et un réflexe de signalement des incidents

Une culture de la sécurité bien ancrée permet à l'organisation de transformer chaque collaborateur en acteur de la cybersécurité et de réduire significativement les vulnérabilités humaines.

- Conformité et réglementation : La gouvernance de la cybersécurité veille au respect des réglementations (RGPD, NIS 2, ISO 27001, etc.), renforçant la confiance des parties prenantes et la réputation de l'entreprise.[17]

En résumé, la gouvernance de la cybersécurité constitue « en même temps » un prolongement naturel de la gouvernance d'entreprise puisqu'elle en est la déclinaison, et une condition de sa bonne réalisation puisqu'elle est indispensable pour protéger les actifs informationnels, assurer la conformité et soutenir la stratégie totale dans un environnement numérique en constante évolution.[18] C'est bien tout le sens que le général Beaufre donnait à ces stratégies « distinctes » mais « interdépendantes ».

[16] Aurélie Tavernier. « L'importance d'instaurer une culture de la sécurité au sein de votre entreprise », 15 juillet 2025. https://immersivefactory.com/fr/actualites/268-Limportance-dinstaurer-une-culture-de-la-s%C3%A9curit%C3%A9-au-sein-de-votre-entreprise.

[17] « Gouvernance en cybersécurité : principes essentiels pour les entreprises modernes », 16 juillet 2025. https://ami-gestion.fr/gouvernance-cybersecurite/.

[18] ANSSI. « Construire la gouvernance de sécurité numérique adaptée à son organisation », 23 mai 2024. https://cyber.gouv.fr/construire-la-gouvernance-de-securite-numerique-adaptee-son-organisation.

La stratégie totale d'une organisation appartenant au temps long, la gouvernance du risque numérique s'inscrit également dans une démarche de long terme et doit pouvoir trouver sa place dans le fonctionnement habituel de l'organisation. Le Système de Management de la Sécurité du Système d'Information (SMSI), tel qui va être présenté ci-après, apporte une solution à cette conciliation entre l'immédiateté du fonctionnement quotidien, et le temps long de la stratégie.

I.3 Rôle et intérêt d'un SMSI

Le **Système de Management de la Sécurité de l'Information (SMSI)**[19], conforme à l'esprit de la norme ISO/IEC 27001, est un cadre organisationnel intégrant politiques, processus et outils visant à garantir la confidentialité, l'intégrité et la disponibilité des informations, dans tous types d'organisations.

Le SMSI fait partie de l'arsenal à utiliser car cette approche conduit à se concentrer non plus sur le contenant, mais sur le contenu, c'est-à-dire le capital informationnel, c'est or blanc du XXIe siècle évoqué lors de l'introduction.

I.3.1 Rôle du SMSI

Le Système de Management de la Sécurité de l'Information (SMSI) joue un rôle central dans la protection des actifs informationnels de l'organisation. Il repose sur une approche structurée permettant de gérer les risques, d'assurer la conformité réglementaire et de renforcer la résilience face aux menaces, tout en favorisant une amélioration continue.

Quatre axes majeurs peuvent être mis en évidence :

- **Gestion proactive des risques :** le SMSI identifie, analyse et traite les risques liés à la sécurité de l'information, en instaurant des mesures de prévention adaptées selon la sensibilité des actifs ;
- **Protection globale de l'information :** il protège les données contre les accès non autorisés, les altérations ou pertes, grâce à une combinaison de dispositifs techniques (chiffrement, antivirus) et organisationnels (gestion des accès, sensibilisation) ;
- **Conformité réglementaire :** il facilite le respect des obligations légales (ex. RGPD) et soutient l'obtention de certifications, renforçant ainsi la confiance des partenaires ;
- **Amélioration continue et résilience :** grâce au cycle PDCA, le SMSI évolue face aux nouvelles menaces, tout en assurant la continuité et la reprise d'activité en cas d'incident.

[19] CSM. « Création d'un système de management de la sécurité de l'information (SMSI) conforme à la norme ISO 27001 », s. d. https://cybersecurite-management.fr/creation-dun-systeme-de-management-de-la-securite-de-linformation-smsi-conforme-a-liso-27001/.

I.3.2 Intérêt du SMSI en Intelligence Economique et Cybersécurité

Dans un contexte marqué par la montée des menaces numériques et la valeur croissante de l'information stratégique, le Système de Management de la Sécurité de l'Information (SMSI) constitue un levier essentiel pour réaliser ce principe de sûreté au service de la liberté d'action dans le cadre défini par la stratégie totale, puisqu'il (ré)concilie sécurité, compétitivité et performance organisationnelle.

Tout d'abord, il constitue un **atout stratégique à la lumière de l'intelligence économique** puisqu'il permet de mieux protéger les informations sensibles (brevets, savoir-faire, données concurrentielles…) et les échanges d'information, tout en limitant les risques liés à la coopération, l'innovation et la veille stratégique.

Ensuite, il représente une **réponse adéquate aux enjeux de cybersécurité** en offrant un cadre structurant pour anticiper, détecter et réagir face aux cyberattaques. Le tout en instaurant une culture de sécurité partagée à tous les niveaux de l'organisation.

Enfin, il **procure des avantages organisationnels et économiques** en optimisant la gestion de l'information, réduisant les coûts associés aux incidents de sécurité et renforçant la crédibilité de l'organisation auprès de ses clients, partenaires et autorités de régulation.

En conclusion, le SMSI constitue un moyen particulièrement efficace pour assurer la sûreté et la sécurité des actifs informationnels, soutenir la démarche d'intelligence économique, faire face aux cybermenaces et améliorer la performance globale de l'entreprise dans une logique d'amélioration continue. En assurant tout cela aux autres stratégies « distinctes et interdépendantes », donc au profit de la stratégie totale *in fine*, il contribue à créer une sorte de bulle de confiance au sein de laquelle les autres entités de l'entreprise pourront se mouvoir plus facilement, et surtout être plus concentrées sur la mise en œuvre de leur propre stratégie. C'est ainsi que le SMSI contribue à la liberté d'action de l'entreprise.

I.4 Une approche technico-financière dominante ?

Pour bien expliquer ce concept, il sera tout d'abord défini, avant d'en expliciter successivement les avantages et les inconvénients.

I.4.1 Définition

« Traditionnellement, la géopolitique était absente des stratégies numériques. Nos décisions reposaient surtout sur des critères métiers, techniques, financiers ou juridiques. »

Rapport du CIGREF, février 2025.

L'approche technico-financière en cybersécurité désigne une logique dominante qui réduit les enjeux sécuritaires à une équation économique optimisée, fondée sur le paradigme « problème = produit + budget = solution » avec pour atteindre les objectifs de l'entreprise (sécurité, règlementation, normatif), Cette vision consiste à considérer la cybersécurité comme un ensemble de « technologies » quantifiables financièrement, où les décisions d'investissement sont principalement guidées par le calcul du retour sur investissement (ROI)[20].

Cette approche privilégie l'acquisition de solutions technologiques standardisées en fonction de leur rapport qualité-prix-efficacité, transformant la sécurité informatique en un processus d'optimisation financière. Dans un contexte où « *les dépenses mondiales en produits et services de cybersécurité dépasseront 1,75 billion de dollars entre 2021 et 2025* »[21], elle répond à une logique de rationalisation des coûts face à la croissance exponentielle des investissements cyber.

L'approche technico-financière se caractérise par la prédominance d'indicateurs économiques dans l'évaluation des risques et la justification des mesures de protection, réduisant ainsi la complexité stratégique de la cybersécurité à des métriques financières mesurables et comparables entre organisations.

I.4.2 Principe

Le principe « technico-financier » envisage la cybersécurité comme un problème à deux dimensions :

- Technique : sécurisation des infrastructures numériques (pare-feu, détection d'intrusion, chiffrement, règlementation, normatif, audits, etc.).
- Financière : évaluation et maîtrise des coûts, ROI (retour sur investissement), calcul du budget alloué à la sécurité, tarification des sinistres et des assurances cyber.

[20] IBM et Palo Alto Networks. « How unified cybersecurity platforms add business value », 27 janvier 2025. https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/unified-cybersecurity-platform.

[21] Steve Morgan. « Top 10 Cybersecurity Predictions and Statistics For 2024 », Cybercrime Magazine, 8 janvier 2021. https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/.

I.4.3 Avantages de cette approche

L'approche technico-financière présente des avantages indéniables. Elle permet avant tout une quantification claire des investissements sécuritaires à travers le calcul du retour sur investissement (ROI), facilitant ainsi les arbitrages budgétaires.

L'approche facilite également la conformité réglementaire en proposant des solutions standardisées, permettent d'aider les entreprises à démontrer leur conformité tout en bénéficiant d'économies d'échelle.

Enfin, cette approche simplifie la prise de décision en proposant des solutions « clés en main » qui réduisent la complexité technique pour les dirigeants non-spécialistes. Elle permet une allocation rationnelle des ressources basée sur des critères financiers objectifs, facilitant ainsi la gouvernance de la cybersécurité au niveau organisationnel.

I.4.4 Limites et risques

Cette approche pose plusieurs **problèmes fondamentaux** (techniques, financiers, organisationnels), le premier étant la réduction de la sécurité à un « produit » plutôt qu'à un « processus », contredisant les principes établis par Bruce Schneier *« La sécurité est un processus, pas un produit. Les produits offrent une certaine protection, mais la seule façon de mener efficacement ses activités dans un monde instable est de mettre en place des processus qui tiennent compte de l'insécurité inhérente à ces produits. L'objectif est de réduire le risque d'exposition, quels que soient les produits ou les correctifs.»* [22]. Cette vision mécaniste ignore la nature évolutive et contextuelle des cybermenaces.

I.4.4.1 Technique

Cette vision conduit à une surconsommation de solutions techniques qui, loin d'améliorer la posture de sécurité, entraînent parfois une complexité opérationnelle accrue.

Cela se manifeste tout d'abord par **une dépense non optimisée** : configurations mal maîtrisées, sous-utilisation des outils acquis, redondances fonctionnelles coûteuses, perte d'efficacité opérationnelle. « *52 % des dirigeants affirment que la complexité est le principal obstacle à leurs opérations de cybersécurité* »[23].Ce phénomène illustre une forme de « dérive technologique » où la multiplication des solutions devient contre-productive.

Ensuite, cette approche technique – par les logiciels et outils numériques - génère **une illusion de protection**. Comme le souligne Vincent Strubel : *« C'est un peu troublant de se dire qu'on achète des équipements de sécurité qui se trouvent finalement être la porte d'entrée des attaquants mais, au-delà de ça, la réalité de la menace et de la capacité des attaquants à s'en saisir est quelque chose qui nous préoccupe. »* [24] Ce propos démontre qu'une approche technico-financière s'avère nécessaire mais non suffisante. En effet, celle-ci comporte des

[22] Bruce Schneier. « The Process of Security », Schneier on Security, 2000. https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html.
[23] IBM et Palo Alto Networks, « How unified cybersecurity platforms add business value ».
[24] Julien VERCHÈRE. « Cybersécurité : quel est l'état de la menace en France ? », Mesinfos, 11 mars 2025, sect. Société. https://mesinfos.fr/cybersecurite-quel-est-l-etat-de-la-menace-en-france-218061.html.

vulnérabilités cachées puisque les outils de cybersécurité présentent eux-mêmes des vulnérabilités d'ordre technique !

I.4.4.2 Financier

Chacun défend son périmètre (DSI, Finance, Risk Management), sans vision globale du « risk-adjusted return » de la cybersécurité. Les arbitrages financiers pénalisent parfois les projets à fort impact stratégique (ex : Zero Trust, gestion des identités) jugés trop coûteux à court terme. *« 62 % des RSSI ont déclaré que le report d'une mise à niveau en raison de coupes budgétaires a conduit à une attaque réussie* »[25]. On traite la cybersécurité comme un centre de coût, et non comme un investissement ou une source de résilience et d'opportunités (avantage compétitif, confiance clients).

I.4.4.3 Organisationnelle

Par ailleurs, cette logique privilégie souvent les solutions à court terme au détriment de la résilience à long terme. Elle néglige les aspects humains et organisationnels de la sécurité, pourtant cruciaux. Les parties prenantes, unités métiers (*marketing*, *supply-chain*…) ne sont pas intégrées dans la gouvernance de la sécurité. Cette situation limite l'agilité organisationnelle et expose les entreprises à des risques de critique pour leur valeur métier.

I.4.5 Exemple

L'approche technico-financière engendre également une dépendance technologique critique. L'affaire VMware démontre comment une solution dominante peut devenir un instrument de contrainte économique, avec des comportements qu'AT&T a qualifié de « *pratique de rançon* » [26]. Exemple que nous prendrons le temps de développer plus en détail dans la partie 2.

I.4.6 Une nécessité d'évoluer vers une vision plus stratégique

Cette approche génère de **nouveaux risques systémiques** particulièrement préoccupants. Le premier concerne l'émergence de cybermenaces géopolitiques, avec une « *montée en puissance de l'hacktivisme* » où des groupes pro-russes ont mené « *6600 attaques depuis début 2022, visant dans 96% des cas des pays européens* »[27]. Ces attaques ciblent spécifiquement les infrastructures critiques européennes, révélant la vulnérabilité des approches standardisées face à des menaces asymétriques. Les risques de chaîne

[25] « Splunk The CISO Report 2025 », Splunk, s. d. https://www.splunk.com/en_us/campaigns/ciso-report.html.

[26] Steve McDowell. « Why AT&T's Suing Broadcom Over Forced VMware License Charges », 6 septembre 2024, sect. Cloud. https://www.forbes.com/sites/stevemcdowell/2024/09/06/why-atts-suing-broadcom-over-forced-vmware-license-changes/.

[27] Ingrid Vergara. « Cybersécurité : les entreprises de plus en plus ciblées par les « hacktivistes » », Le Figaro, 5 décembre 2024, sect. Tech & Web. https://www.lefigaro.fr/secteur/high-tech/cybersecurite-les-entreprises-de-plus-en-plus-ciblees-par-les-hacktivistes-20241205.

d'approvisionnement numérique se multiplient également. Le secteur financier, *« fortement interconnecté* », voit « *la dépendance aux technologies tierces* » créer de nouveaux points d'entrée pour les attaquants.

En somme, la cybersécurité ne doit plus être traitée comme un simple problème technique à budgéter, mais comme un enjeu stratégique à appréhender avec la boîte à outils de l'Intelligence Économique (IE), pour passer d'une vision en silo à une démarche holistique et proactive.

L'Intelligence Économique (IE) propose une démarche transversale, intégrant :

- Les vulnérabilités métiers et non uniquement techniques ;
- La protection du patrimoine informationnel ;
- La cartographier hostile de leur écosystème et concurrentiel ;
- Permettant d'intégrer les dimensions cognitives, informationnelles et géopolitiques dans la cybersécurité.

Ces entreprises ne considèrent plus la cybersécurité comme une fin en soi, mais comme un vecteur de compétitivité, d'anticipation et d'adaptabilité face à un environnement géoéconomique instable.

Cependant, même parmi ces structures pionnières, on observe encore trop souvent une séparation nette entre les fonctions IE et cybersécurité. Cette scission nuit à la capacité de produire une lecture complète et convergente de l'environnement de menace, alors même que la convergence des disciplines est devenue essentielle pour une réelle sécurité de l'information.

Pour résumer cette première partie, il y a une différence entre ce que la stratégie de cybersécurité devrait être, et ce qu'elle est en réalité. Ou, du moins, si cette stratégie de cybersécurité est bien pensée comme une stratégie « distincte » de la « stratégie totale » et des autres stratégies, mais « interdépendante » de celles-ci, sa réalisation semble perfectible. Dans les faits, C'est plutôt une approche « technico-financière » de la cybersécurité qui prédomine, c'est-à-dire une approche cherchant à résoudre deux problèmes (la sécurité de l'information et la conformité au cadre légal, règlementaire et normatif) par la mobilisation de ressources financières. Il est clair que cette approche, lorsqu'elle est bien menée, se révèle efficace pour produire un état de cybersécurité. La différence ne se situe donc pas entre « efficace » et « inefficace », mais plutôt entre « autocentrée » et « subordonnée à la vision de l'entreprise ». C'est-à-dire que cette manière de produire de la cybersécurité ne produit-elle pas des dépendances, ne comporte-t-elle pas des limites, qui pèsent *in fine* sur la liberté d'action de l'entreprise ? Et donc qui peuvent rendre plus difficile la capacité de l'entreprise à mener sa grande stratégie ? C'est ce que nous allons démontrer dans cette deuxième partie.

II. Cybersécurité et stratégie d'entreprise

« La cybersécurité a fait rentrer la géopolitique dans les COMEX. »

Geoffroy ROUX DE BEZIEUX, président du Medef, 2024.

Le monde actuel se caractérise par une complexité croissante sur les plans économique, géopolitique, environnemental, technologique et informationnel. Ce contexte est communément désigné par l'acronyme VUCA (Volatilité, Incertitude, Complexité et Ambiguïté), concept développé initialement par l'armée américaine en 1998 pour clarifier les enjeux de la société moderne et s'y adapter efficacement. Dans ce monde en mutation constante, le cyberespace occupe désormais une place majeure et incontournable, tant au niveau étatique que privé, devenant le théâtre d'affrontements géopolitiques et économiques. Face à cette ultra-multipolarisation où l'hégémonie est disputée, où les guerres informationnelles et technologiques constituent le terrain préliminaire de toute opération, la cybersécurité devient un enjeu stratégique majeur. Elle ne vise pas uniquement à sécuriser les actifs numériques d'une entreprise, mais également à renforcer sa compétitivité et sa résilience dans un environnement hostile avec des opportunités.

A cause de son poids stratégique croissant, il convient de devenir particulièrement attentif à tout évènement, phénomène ou décision qui viendraient peser sur la cybersécurité, l'empêchant ainsi de réaliser le principe de sûreté pour lequel elle existe, nuisant donc à la liberté d'action de l'entreprise. Il convient alors d'identifier toute menace qui cherchera à mettre en défaut la stratégie de cybersécurité ; mais également toute dépendance qui, sans pour autant menacer la sûreté et la sécurité des données, désalignerait la stratégie de cybersécurité de la stratégie totale, créant alors un risque pour la liberté d'action (et la source de cette dépendance devenant une menace).

Au cours de cette partie, après une démonstration de la manière dont la cybersécurité crée ou non de la liberté d'action pour son entreprise, la notion d'intelligence économique sera introduite et présentée. Dans un troisième et quatrième temps, grâce à la méthodologie de l'intelligence économique, ces menaces pesant sur la stratégie de cybersécurité seront passées en revue. C'est ainsi que cette approche du réel par l'intelligence économique se révèle comme un outil indispensable pour concevoir la stratégie de cybersécurité, et la mettre en œuvre avec la gouvernance éponyme. Dans une cinquième et dernière sous-partie, toujours grâce à l'intelligence économique, le renforcement de la souveraineté numérique des entreprises sera présenté comme un remède à ces dépendances créatrices de menaces.

II.1 La liberté d'action de l'entreprise

II.1.1 Définition

Dans la partie précédente, la liberté d'action a été définie à partir de la pensée du maréchal Foch comme la capacité d'être autonome dans la prise de décisions, et de les mettre en œuvre sans entrave. Plus précisément, la liberté d'action de l'entreprise peut être définie comme sa capacité, à partir d'une perception claire de son environnement et de la conscience de ses forces et limites, à mettre en œuvre la stratégie totale telle qu'elle a été définie par la direction de l'entreprise. Dans cet environnement VUCA où les entreprises doivent non seulement développer leur capacité d'adaptation et de réaction, mais également anticiper les évolutions de leur écosystème, l'autonomie décisionnelle constitue un avantage concurrentiel déterminant. *A contrario*, toute dépendance vient brider cette capacité d'adaptation et de réaction, cette liberté d'action.

Pour cultiver cette autonomie dans l'agir, l'entreprise doit donc se soucier de toutes ses dépendances tant en amont de ses activités (chaîne d'approvisionnement, cadre légal, technologique…) qu'en aval (clients…). Conformément aux principes énoncés dans la première partie, elle devra également cultiver une stratégie de sûreté et de sécurité qui contribuera à sa liberté d'action. C'est à ce titre que la stratégie de cybersécurité influence de manière croissante cette stratégie de sûreté, elle-même au service de la liberté d'action de l'entreprise.

II.1.2 Impact croissant de la cybersécurité

Le niveau systémique du risque cyber (c'est-à-dire que la question n'est pas de savoir si l'entreprise sera attaquée, mais quand), la numérisation en cours d'activités toujours plus nombreuses grâce à l'intelligence artificielle et l'internet des objets, donne à la stratégie de cybersécurité un rôle croissant dans la sauvegarde de la sûreté de l'entreprise (notamment de ses actifs informationnels), donc de la liberté d'action totale, donc dans sa contribution à la réalisation de la stratégie totale.

Les données contenues dans le dernier rapport du Forum économique mondial sur la cybersécurité démontrent cette tendance : La cybersécurité influence désormais directement les décisions stratégiques des entreprises puisque « *54% des grandes organisations citent la gestion des risques liés aux tiers comme un défi majeu*r[28]*.* » Or, au cœur des risques liés aux tiers se trouvent les cyberattaques « par la *supply chain* », ainsi que la complexification des chaînes d'approvisionnement numériques créant de nouvelles dépendances qui limitent l'autonomie des entreprises, toujours selon le WEF.

[28] WEF Global Cybersecurity Outlook 2025, s.l., WEF, 2025 p.6.

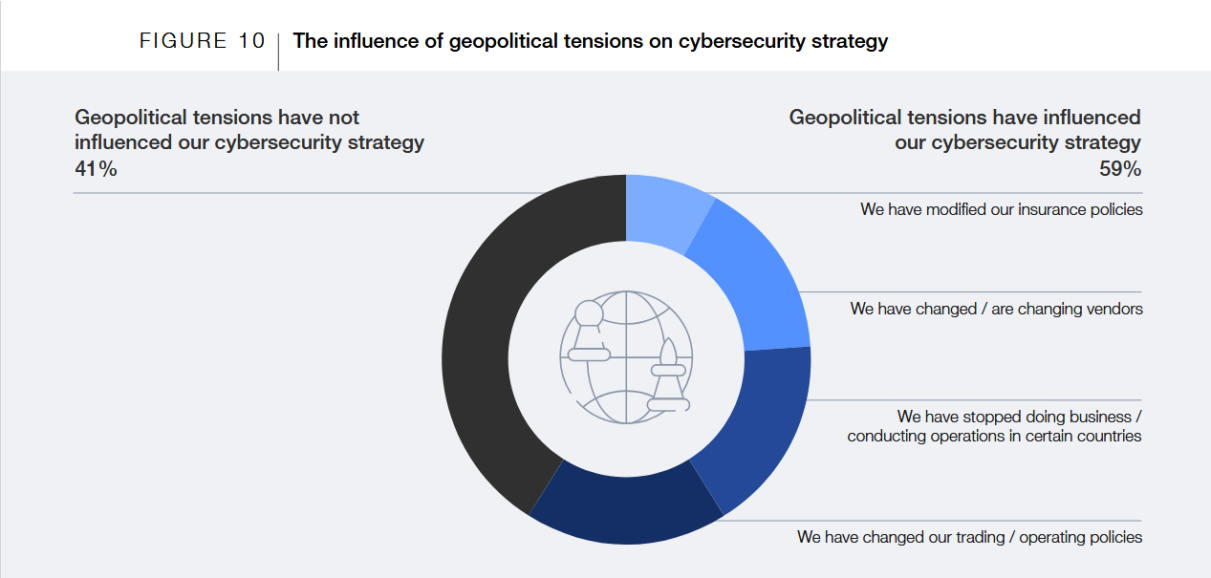


Figure 4 - Influence des tensions géopolitiques sur la stratégie de cybersécurité

Source : https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf, p.26.

La figure précédente, tirée du rapport 2025 du WEF sur la cybersécurité, démontre également cet impact de la stratégie de cybersécurité sur la grande stratégie, notamment comme préservation ou limitation de la liberté d'action. Ainsi, dans 17% des cas, l'impact des tensions géopolitiques sur la stratégie de cybersécurité s'est traduit par un arrêt des activités économiques dans certains pays. C'est-à-dire que, dans cette situation, face à l'incapacité à réaliser le principe de sûreté à cause de facteurs externes, l'entreprise a été confrontée à une restriction de sa liberté d'action l'obligeant à renoncer à des activités économiques.

II.2 L'Intelligence Économique, une méthodologie globale du dévoilement

« L'intelligence économique, c'est lorsque tu utilises des informations qui ne sont pas de ton domaine d'expertise pour mieux comprendre ton domaine d'expertise. »

Alfred Huot de Saint-Albin, responsable pôle fraude, Orange Cyberdéfense

Citée à plusieurs reprises depuis le début de ce document, l'intelligence économique constitue un outil d'analyse du réel encore assez méconnu. A cause de cette regrettable confidentialité, cette partie aura pour objet de mieux expliquer de quoi il s'agit dans un premier et deuxième temps. Puis de s'appuyer sur cet outil, pour mieux comprendre dans un troisième temps comment il se met au service de la mise en œuvre de la stratégie totale d'une organisation.

II.2.1 Une méthodologie du dévoilement

L'Intelligence Économique (IE) offre une grille de lecture permettant d'analyser le monde à travers plusieurs perspectives complémentaires - économique, politique, juridique et sociétale. Cette approche procure une vision plus complète, plus fine, de la situation mondiale et révèle la brutalité des rapports économiques internationaux. Cette compétition est présentée comme naturelle et bénéfique, alors qu'elle résulte d'un ordre construit où « *l'État n'est ni minimal ni résiduel, mais joue un rôle de créateur et de protecteur de l'ordre concurrentiel* »[29].

Parce qu'elle fait appel à ces perspectives « *distinctes et interdépendantes* », la méthodologie de l'intelligence économique aide à mieux comprendre une situation donnée, ses tenants et ses aboutissants. C'est parce qu'elle rend plus intelligible le réel qu'elle constitue par excellence la méthodologie de dévoilement du réel à ceux qui sont prêts à l'affronter. Car pour paraphraser une citation célèbre de Charles Peguy que l'on trouve dans *Notre jeunesse*, l'intelligence économique aide non seulement à « *dire ce que l'on voit* », mais encore plus à « *voir ce que l'on voit* », et selon l'écrivain c'est « *ce qui est plus difficile* ».

[29] Bruno Amable, Elvire Guillaud, et Stefano Palombarini, L'économie politique du néolibéralisme : le cas de la France et de l'Italie, Collection du CEPREMAP 26 (Paris : Éd. Rue d'Ulm, 2012), 24.

II.2.2 Une brève histoire

L'intelligence économique (IE) est un concept qui a émergé en France au début des années 1990, bien que ses racines remontent aux pratiques de renseignement militaire qui ont connu une mutation profonde après la chute du bloc soviétique. En l'absence d'adversaire étatique majeur, les États-Unis ont notamment réorienté leurs ressources vers l'espionnage économique.

Le rapport Martre [30] de 1994 constitue la pierre angulaire de l'intelligence économique en France. Henri Martre y définit l'IE comme *« l'ensemble des actions coordonnées de recherche, de traitement et de distribution, en vue de son exploitation, de l'information utile aux acteurs économiques* ». Ce rapport a permis d'analyser de façon comparée les systèmes nationaux d'intelligence économique les plus pertinents de l'époque (États-Unis, Japon, Allemagne, Grande-Bretagne) et a doté « *les acteurs publics et privés d'un langage commun, d'une culture partagée autour de l'intelligence économique* ».

Plusieurs figures emblématiques ont porté ce concept en France : Christian Harbulot, Bernard Carayon, Alain Juillet, nommé Haut responsable chargé de l'Intelligence économique auprès du Premier Ministre en décembre 2003 suite à la perte des fleurons français comme Gemplus et Péchiney ; ou encore plus récemment Frédéric Pierucci, victime emblématique de « l'affaire Alstom » qui a mis en lumière les pratiques de guerre économique des américains contre l'industrie française en 2014.

Malgré des phases de sursaut, le constat est là : la France a toujours manqué de constance sur le plan des institutions, et a souvent fait preuve d'une certaine naïveté face à la réalité de la guerre économique mondiale, parfois illusionnée par le concept de « *mondialisation heureuse* » [31] et « *l'entreprise sans usines* » [32]. Comme le souligne Bernard Besson : « *une politique publique d'intelligence économique est une remise en cause des certitudes, une saisie des opportunités et des menaces toujours renouvelées* » [33].

[30] Henri Martre. « Rapport du Groupe « Intelligence économique et stratégie des entreprises » » (Commissariat Général du Plan, 1994).

[31] Gilles Servient, Les pertes de souveraineté industrielle : cas d'école à la française, https://www.ege.fr/infoguerre/les-pertes-de-souverainete-industrielle-cas-decole-la-francaise , 12 décembre 2022.

[32] Anne de Guigné, « «L'entreprise sans usines» : Serge Tchuruk ou le symbole de la désindustrialisation », Le Figaro, 14 août 2024, sect. Conjoncture, https://www.lefigaro.fr/conjoncture/l-entreprise-sans-usines-serge-tchuruk-ou-le-symbole-de-la-desindustrialisation-20240813.

[33] Jacqueline Sala. « Entretien. Bernard Besson analyse les apports du Rapport Martre. "Intelligence économique et stratégie des entreprises" », Www.veillemag.com, s. d. https://www.veillemag.com/Entretien-Bernard-Besson-analyse-les-apports-du-Rapport-Martre-Intelligence-economique-et-strategie-des-entreprises_a4748.html.

II.2.3 Une méthodologie tournée vers l'action

L'intelligence économique, héritière du cycle du renseignement militaire, constitue fondamentalement une méthodologie d'action structurée en quatre phases principales : veille, analyse, traitement et influence. Cette approche systématique permet de transformer l'information en connaissance actionnable, puis en avantage stratégique. Il est intéressant de noter que l'intelligence économique a pour but de produire une meilleure connaissance d'une situation donnée, au service de l'action, tout comme la stratégie est « *l'art pour l'action* » selon les écrits du général Vincent Desportes cités auparavant. L'intelligence économique, c'est donc la connaissance au service des acteurs économiques afin qu'elle oriente leur action, leurs prises de décisions.

La définition proposée par Claude Revel précise que l'intelligence économique est **« *la maîtrise de l'information, le but étant de connaître son environnement extérieur et par conséquent d'adapter par avance sa conduite* ».** Elle se compose de trois volets complémentaires :

- Le traitement de l'information : recueillir les informations nécessaires, les trier et les valider pour obtenir une vision pertinente de son environnement concurrentiel international ;
- La sécurisation : protéger ses actifs, particulièrement immatériels, en anticipant les risques et les problèmes liés notamment à la propriété intellectuelle et à la réputation ;
- L'influence : savoir convaincre, négocier, faire du *lobbying* professionnel et exercer une influence normative en anticipant les règles internationales et en participant à leur élaboration (ce qui revient à renforcer sa puissance informelle, cf. conclusion de la première partie).

Cette démarche collective vise l'agilité par un usage stratégique de l'information. Elle met en musique des démarches de veille, de sécurité économique et d'influence, ce que les Anglo-Américains nomment justement "intelligence". Nicolas Moinet la décrit comme « *une partition qui s'appréhende en trois couleurs (blanc, gris et noir – une typologie de l'information et de son usage stratégique) et s'organise puis s'évalue suivant une méthodologie : le cycle du renseignement »*[34]*.*

[34] Nicolas Moinet, « L'intelligence économique, une culture du renseignement appliquée à l'entreprise », Conflits : Revue de Géopolitique (blog), 16 mars 2020, https://www.revueconflits.com/entreprise-renseignement-guerre-economique-abonne-nicolas-moinet/.

II.2.4 Fit for 55 en Europe, un cadre climatique qui a, de fait, favorisé la Chine ?

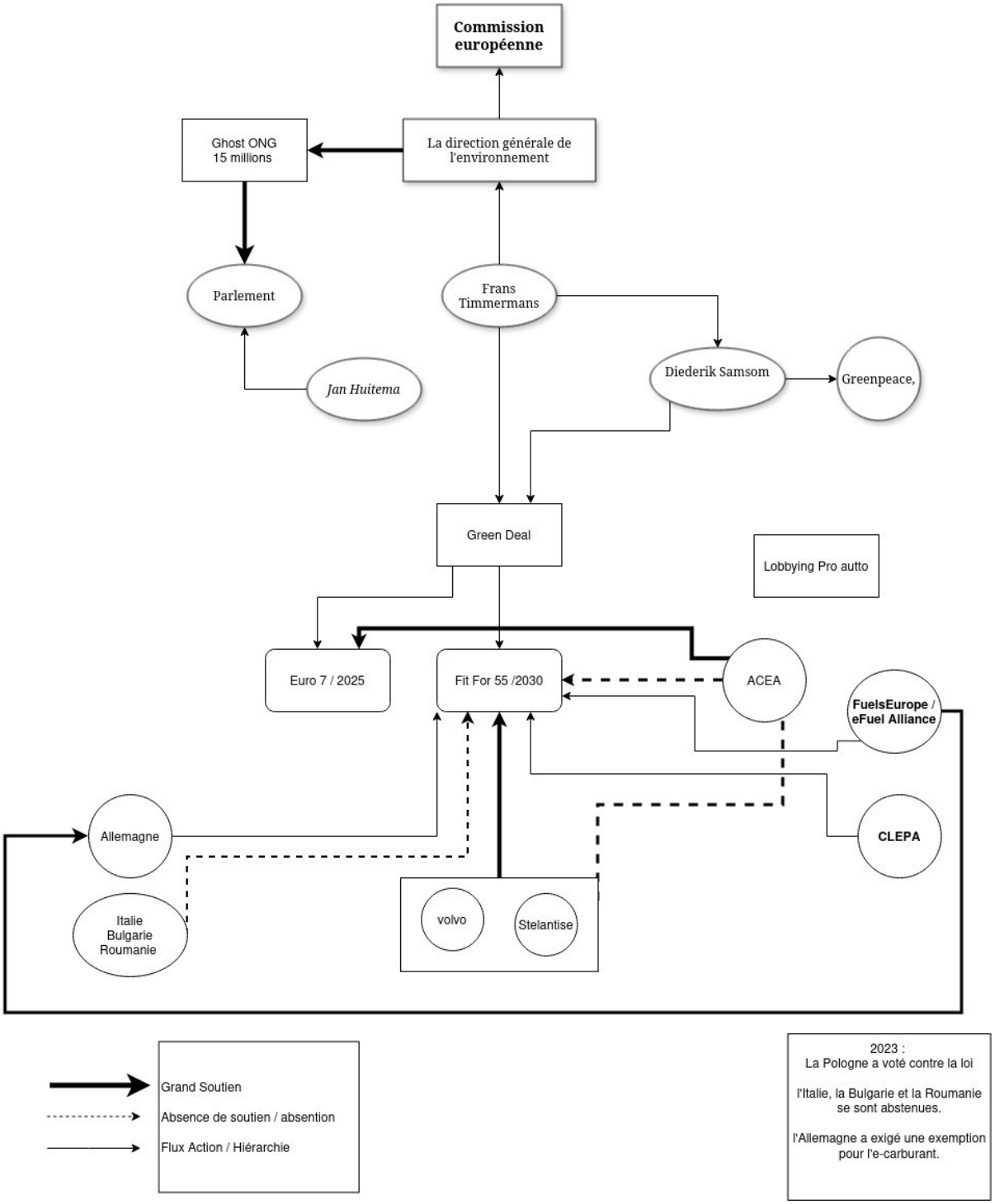


Figure 9 - carte des acteurs du plan *Fit for 55*

II.2.4.1 Constat 2025 – ce que dit (et ne dit pas) la norme

« Fit for 55 » (« ajustement à l'objectif 55 » en français) désigne un « paquet », c'est-à-dire un ensemble de dispositions législatives d'origine européenne visant à réduire les émissions de gaz à effet de serre de l'Union d'au moins 55 % d'ici à 2030, et à mettre l'UE sur la voie de la neutralité climatique d'ici à 2050. L'Union européenne a ainsi révisé en 2023 le règlement (UE) 2019/631 sur les standards CO_2 des voitures/vans vendus à l'état neuf : –55 % et –50 % de vente respectivement de voitures et vans dès 2030 (sur la base de l'année 2021), puis -100 % en 2035 (donc uniquement des véhicules « zéro émission à l'échappement »).

En parallèle, le règlement (UE) 2023/1804 du Parlement européen et du Conseil du 13 septembre 2023 dit « AFIR » (Alternative Fuels Infrastructure Regulation), adopté dans le cadre du paquet législatif « Fit for 55 », vise à accélérer le déploiement des infrastructures pour carburants alternatifs sur le territoire de l'Union européenne. Afin de permettre au secteur des transports de réduire son empreinte carbone, il fixe notamment des obligations pour déployer des infrastructures d'alimentation électrique à destination des aéronefs stationnés dans les aéroports. Entré en vigueur le 12 octobre 2023, ce règlement s'applique depuis le 13 avril 2024.

En théorie, cet alignement climat-infrastructures donne de la visibilité industrielle. En pratique, les années 2024 et 2025 ont vu la progression rapide des constructeurs chinois sur ce marché du véhicule électrique (coût unitaire des batteries faible, avantages d'une intégration verticale, offre « value for money ») et l'UE riposte par des droits antisubventions (droits définitifs annoncés en octobre 2024) et par un examen anticipé des objectifs 2035 en cette fin 2025[35]. La hausse de parts de marché des constructeurs automobiles BYD, MG, et SAIC d'une part, les réactions de Stellantis et Volkswagen d'autre part, confirme que la fenêtre ouverte par l'objectif fixé pour 2035 a surtout profité aux acteurs en ordre de marche… or il s'avère qu'ils sont essentiellement chinois.[36]

II.2.4.2 Origine, portage politique et « e-fuels »

La Commission européenne, dans le cadre du Green Deal, se trouve à l'origine de ce plan, dont le paquet législatif en constitue une des réalisations. L'accord politique entre le parlement européen et le Conseil date de la fin octobre 2022, pour une adoption finale mars-avril 2023. L'objectif était d'aligner le transport routier sur les exigences imposées aux particuliers, avec un objectif de neutralité carbone en 2050 et une diminution des ventes de véhicules neufs de 55 % dès 2030[37].

---

[35] Philip Blenkinsop. « EU brings forward review of 2035 zero emission vehicles target », *Reuters*, 12 septembre 2025, sect. Climate & Energy. https://www.reuters.com/sustainability/climate-energy/eu-brings-forward-review-2035-zero-emission-vehicles-target-2025-09-12/.

[36] « European Parliament approves watered-down Euro 7 rules | Air Pollution & Climate Secretariat. https://www.airclim.org/acidnews/european-parliament-approves-watered-down-euro-7-rules

[37] European Parliament. « Revision of CO2 emission performance standards for cars and vans, as part of the European Green Deal | Legislative Train Schedule », European Parliament. https://www.europarl.europa.eu/legislative-train/package-fit-for-55/file-co2-emission-standards-for-cars-and-vans-post-euro6vi-emission-standards?sid=5801.

Il est intéressant de préciser qu'en 2023, dans le cadre de cet accord politique, l'Allemagne a obtenu possibilité d'immatriculer après 2035 des véhicules MCI (moteur à combustion interne : fonctionnant exclusivement avec des e-carburants « CO_2-neutres »).

II.2.4.3 Lobbying : transparence, controverses et "lobbying fantôme"

En 2025, une enquête de la commission des finances de l'UE a mis au jour des pratiques jugées inappropriées au sein de la commission environnementale : des fonds publics auraient financé des ONG pour qu'elles mènent un lobbying ciblé auprès de députés en faveur des textes du Green Deal. Comme l'a déclaré le nouveau commissaire européen au Budget, le Polonais Piotr Serafin : « *Malheureusement, de telles pratiques se sont produites par le passé et doivent être éradiquées. Des mesures ont déjà été prises pour résoudre ce problème, et je peux assurer à tous qu'elles ne se reproduiront pas.* » Et d'ajouter : « *Il était inapproprié d'obliger les ONG à faire du lobbying auprès des membres du Parlement européen.* »

II.2.4.4 Euro 7, compromis et myopie financière

Au sujet de la norme Euro 7 visant à réduire la pollution atmosphérique, après un bras de fer entre l'association des constructeurs européens d'automobiles (ACEA) et l'UE, l'association a obtenu cinq ans de répit sur la mise en application d'Euro 7. Ainsi, l'accord final de 2024 a fortement assoupli la norme (proche d'Euro 6) et étalé le calendrier.[38] En échange, les constructeurs ont cessé de remettre en cause le plan « *Fit for 55* » et ses objectifs de réduction des émissions de CO_2 pour 2030.

Ce compromis a eu des effets mitigés. Si d'un côté il a eu pour effet de diminuer la dépense en capital des constructeurs en direction de la R&D et de la fabrication de véhicules électrique, il crée d'autre part un risque de retard de compétitivité sur le marché des véhicules électriques (alors que les concurrents extra-européens continuent d'y augmenter leur avantage comparatif).

La Commission a par ailleurs accordé une flexibilité pour atteindre les objectifs (2025-2027) face à la concurrence chinoise et à une demande en véhicules électrique qui peine à décoller.[39]

II.2.4.5 Le vrai problème : l'absence d'État stratège et la myopie collective

Ce paquet de textes législatifs sur le climat a été conçu comme une politique publique « horizontale ». Or, sans État stratège possédant la totalité des moyens régaliens pour

[38] Stefano Valentino, Lorenzo Di Stasi, et James Jackson. « Comment le lobby automobile a enfumé l'Europe sur les normes anti-pollution des voitures », Libération. https://www.liberation.fr/environnement/comment-le-lobby-automobile-a-enfume-leurope-sur-les-normes-anti-pollution-des-voitures-20231107_VROAW4FKQFEJHKGAZRBO4NRR6I/.

[39] Philip Blenkinsop. « EU gives automakers "breathing space" on CO2 emission targets », *Reuters*, sect. Autos & Transportation. https://www.reuters.com/business/autos-transportation/eu-propose-giving-automakers-three-years-meet-co2-emission-targets-2025-03-03/.

influencer, normaliser, financer et synchroniser les secteurs public-privé, ces ajouts de normes climatiques ont révélé une faiblesse industrielle préexistante plutôt que créé un avantage compétitif.

Pourtant, Henri Martre (1994 – président du groupe « Intelligence Economique et stratégie des entreprises » pour le commissariat général du plan) et Bernard Carayon (2003 - député) avaient documenté ces risques dans leurs rapports respectifs : la coordination des acteurs, l'optimisation des flux d'information public-privé et la réflexion préalable à la phase de normalisation se révèlent indispensables pour que ces implémentations législatives soient véritablement sources de développement économique et de puissance. Faute de quoi, l'entité politique concernée subit les cadres définis ailleurs. Ainsi, sans stratégie étatique clair, les entreprises optimisent localement (génération de cash-flow, avec un ROI à 3-5 ans) mais perdent globalement (liberté d'action, parts de marché, et donc puissance).

Sans cap authentiquement souverain, sans coalition État - filières industrielles – secteurs économiques concernés, le pays ou la région concernée s'exposent mécaniquement à une perte de puissance lors de ces phases de transitions normatives accélérées. La réponse à ces défis suppose de passer d'une intelligence économique défensive à une intelligence économique offensive afin que le triptyque vigie-bouclier-épée soit complet. Une stratégie industrielle claire et partagée doit aussi être pensée comme un facteur d'accroissement de puissance, qui passe hélas, bien souvent, par la diminution de puissance d'un ou plusieurs compétiteurs et adversaires.

Cette conflictualité est inhérente à la marche du monde. Le réel finit toujours par s'imposer. L'ignorer, c'est s'exposer à des échecs tel que celui de la transition énergétique imposée aux constructeurs automobiles européens.

II.3 Que dévoile l'IE à propos de la cybersécurité ?

Depuis plusieurs décennies, les praticiens de l'intelligence économique (IE) cherchent à sensibiliser les décideurs publics et privés à la réalité d'une guerre économique en temps de paix. Longtemps reléguée à l'arrière-plan, cette réalité est désormais une évidence, en particulier en 2025, à l'heure où la cybersécurité devient un enjeu géopolitique majeur. C'est dans ce contexte que l'intelligence économique, comme méthode de compréhension du cyberespace prend tout son sens (quels sont les différents cadres légaux qui s'y appliquent ? Pourquoi et comment les acteurs privés et publics y déploient-ils leur volonté de puissance ? Qui maîtrise quelles couches du cyberespace ? Quelles sont les relations entre les différents acteurs ? ...).

II.3.1 IE et analyse du risque : une approche intégrative

L'un des premiers apports de l'intelligence économique à la cybersécurité réside dans sa capacité à enrichir l'analyse des risques. Contrairement à une lecture technico-financière classique, l'IE propose une vision systémique, décloisonnée, qui permet de croiser les risques technologiques avec des dynamiques politiques, juridiques, économiques et géopolitiques.

Les phénomènes de propagation d'attaques par effet rebond ou par la chaîne d'approvisionnement (ex. : SolarWinds, NotPetya) illustrent parfaitement cette complexité. Dans ce contexte, une lecture géopolitique devient essentielle. Comme le souligne le rapport du World Economic Forum [40], les menaces les plus redoutables proviennent de groupes APT étatiques ou paraétatiques, comme les APT russes ou iraniens, ciblant les alliés de l'Ukraine ou Israël.

La dernière édition du rapport Cyber Power Index indique que les grandes puissances (Chine, Russie, États-Unis) intègrent de plus en plus la cybersécurité dans leurs stratégies de domination, y compris par l'exploitation de vulnérabilités *zero-day* [41] ou avec la capture des données sensibles via des logiciels de sécurité faussement neutres [42].

II.3.2 Révéler les contraintes géoéconomiques des solutions cyber

L'intelligence économique permet également de mettre en lumière les contraintes externes, souvent invisibles dans une approche strictement technico-financière. Prenons l'exemple des antivirus d'origine étrangère, souvent présentés comme discrets mais scannant l'ensemble d'un système. Derrière leur façade technique se cache parfois une logique de renseignement, voire d'ingérence. C'est pour cette raison notamment que l'Australie a décidé de mettre fin à l'utilisation des produits et services de l'éditeur de logiciels de cybersécurité russe Kaspersky dans ses agences, invoquant un « *risque de sécurité »* et des *« menaces*

[40] « WEF Global Cybersecurity Outlook 2025 ».
[41] Del Rosso Kristin et Dakota Cary. « Sleight of hand: How China weaponizes software vulnerabilities » (Atlantic council, 6 septembre 2023). https://www.atlanticcouncil.org/in-depth-research-reports/report/sleight-of-hand-how-china-weaponizes-software-vulnerability/.
[42] Alexander Martin. « Spain awards Huawei contracts to manage intelligence agency wiretaps », The record, 11 juillet 2025. https://therecord.media/spain-awards-contracts-huawei-intelligence-agency-wiretaps.

d'ingérence », quelques mois seulement après l'interdiction de l'antivirus pour toutes les sociétés et tous les consommateurs américains[43].

Lors de notre entretien avec le journaliste Martin Untersinger, nous avons pu évoquer la réalité des grandes entreprises américaines du secteur de la cybersécurité, comme **Crowdstrike**, **Mandiant** ou **FireEye**. Ces entreprises proposent des outils de cybersécurité, mais « *il est frappant de constater que dans l'ensemble de leur conseil d'administration (CA) et de leurs analystes, sont d'anciens membres des services de renseignement américains ».*

« *Toutes les données qui transitent par ces plateformes sont analysées par des analystes qui proviennent tous, ou presque, de la NSA. Par définition, ces solutions traitent un très grand volume de données, et leur cœur de métier consiste justement à les analyser. Cela ajoute un niveau supplémentaire à la problématique de l'extraterritorialité. [...] Si Google pose déjà problème en matière de données, ces entreprises opèrent à un niveau bien supérieur.* »[44]

Le cas du Royaume-Uni, marqué par une forte tradition de renseignement avec le Government Communications Headquarters (GCHQ), montre comment cette culture influence la conception et la diffusion de technologies à usage dual.

L'exemple le plus révélateur est sans doute **Darktrace** : « *en examinant son conseil d'administration, on constate que la moitié des postes décisionnels étaient occupés par d'anciens membres des services britanniques de renseignement* »[45] :

- CEO: Stephen Huxter (MI5)
- CA: Andrew France (GCHQ), Jonathan Evans (MI5), Jim Penrose (NSA)
- CTO: Dave Palmer (GCHQ)
- CSO: John Richardson (GCHQ)

« *Et pour avoir travaillé sur le dossier Snowden, on peut penser ce que l'on veut de la NSA, mais le GCHQ… lui,* ***n'a vraiment aucune limite, aucune limite*** *!* »[46]

[43] Yoann Bourgin. « L'antivirus russe Kaspersky désormais banni des agences gouvernementales australiennes », *Usine digitale*, 24 février 2025. https://www.usine-digitale.fr/article/l-antivirus-russe-kaspersky-desormais-banni-des-agences-gouvernementales-australiennes.
[44] Entretien avec Martin Untersinger, 8 avril 2025.
[45] Laurie Clarke. « Mike Lynch yacht disaster: Missing tycoon's ties to UK spy chiefs », *Politico*, 20 août 2024. https://www.politico.eu/article/missing-tech-tycoon-mike-lynchs-ties-to-uk-spy-chiefs/.
[46] Entretien avec Martin Untersinger.

II.3.3 La dépendance technologique, un enjeu stratégique

L'affaire VMware–Broadcom (rachat en 2023) a montré les dérives de l'approche technico-financière. Les entreprises clientes ont vu les tarifs exploser de 300 à 1800 %, créant une situation de dépendance critique. Comme le soulignait Syntec Numérique, VMware était devenue « *la meilleure solution pour tout le monde* », induisant un quasi-monopole technique.

De même, Microsoft a augmenté ses prix de 30 %, justifiant cela par son investissement dans OpenAI[47]. Le secteur financier, soumis à des réglementations comme DORA ou NIS2, est poussé vers des solutions standardisées, ce qui accroît sa vulnérabilité systémique.

Ces exemples démontrent que l'existence d'acteurs économiques nationaux ne résout pas tous les problèmes, puisque l'augmentation de prix des licences n'a rien à voir avec la nationalité de l'entreprise qui pratique cette augmentation. Toutefois, ils mettent correctement en exergue le risque de dépendance trop forte vis-à-vis d'un fournisseur et de ses solutions numériques (suites logicielles, etc), et donc une fois encore une stratégie de cybersécurité centrée sur une approche technico-financière, sur l'achat de briques logicielles *mainstream*. Ce qui était bon marché hier peut subitement devenir trop coûteux aujourd'hui, conduisant ainsi à une impasse budgétaire. Il faut alors soit changer de fournisseur, soit consentir à payer plus. Dans les deux cas, c'est la liberté d'action de l'entreprise qui a été impactée.

II.3.4 La souveraineté numérique en question

L'Europe se retrouve dans une situation paradoxale : malgré sa volonté d'autonomie stratégique, elle dépend massivement des acteurs extra-européens (notamment américains). Quentin Adam alerte sur le fait que les *hyperscalers* américain coûteraient 240 milliards à l'Europe. Voir, dans certaines configurations, coûteraient jusqu'à 10 fois plus que des solutions européennes[48].

Cette réalité pose la question de la soutenabilité économique d'un modèle où les données, les infrastructures et les services sont captifs de puissances étrangères.

En conclusion, l'apport de l'intelligence économique appelle à un dépassement d'une approche exclusivement défensive de la cybersécurité, au profit d'une vision d'« intelligence cyber » – une stratégie intégrée combinant renseignement, sécurité offensive et influence.

[47] Geoffroy Ondet. « Microsoft va augmenter le prix de son abonnement Microsoft 365 », *01net*, 17 janvier 2025. https://www.01net.com/actualites/microsoft-augmente-prix-abonnement-microsoft-365.html.

[48] Carine Guillemet. « Quentin Adam invité de Micode dans l'émission Underscore_ », Clever Cloud, 27 mars 2025. https://www.clever-cloud.com/fr/blog/entreprise/2025/03/27/quentin-adam-invite-de-micode-dans-lemission-underscore_/.

Cette transition vers une posture proactive et dynamique peut être facilitée par la mise en œuvre d'une « boussole stratégique » proposée par Yannick Pech [49]. Cet outil conceptuel permet d'orienter efficacement les acteurs de la cybersécurité grâce à une grille d'analyse pragmatique qui intègre simultanément des postures défensives et offensives.

Disposition mentale

1ère caractéristique : un domaine de réflexion interdisciplinaire qui s'appuie sur le paradigme de la complexité pour appréhender le « village global »
2e caractéristique : science en action et culture de l'intelligence rusée
3e caractéristique : une posture de combat fondée sur le triptyque patriotisme–unité–souveraineté

Dispositif opérationnel

4e caractéristique : une posture managériale transversale qui place l'information au centre du jeu stratégique
5e caractéristique : méthode opérationnelle globale de maitrise de l'information reposant sur trois champs d'activité : veille, sécurité et influence
6e caractéristique : un processus réticulaire basé sur des dispositifs intelligents visant l'agilité stratégique

***Boussole de disposition mentale* :**

1- Posture et intentionnalité
2- Culture et intelligence
3- Patriotisme et souveraineté
4- Organisation et cohésion

***Boussole du dispositif opérationnel* :**

5- Adaptabilité et transversalité
6- Méthodes et outils
7- Intégration et synergie
8- Plasticité et agilité

Figure 10 - L'intelligence cyber comme boussole stratégique par Yannick Pech

Ainsi définie, cette boussole peut constituer un premier pas pour changer durablement de posture en matière de cybersécurité. L'intelligence économique (IE) ne doit plus seulement être un outil de veille, mais une boussole stratégique permettant de comprendre les contraintes, les dépendances et les leviers d'action dans un cyberespace devenu un théâtre majeur de la guerre économique mondiale.

[49] Yannick Pech. « Intelligence cyber : intégrer les hackers dans une stratégie de sécurité numérique globale. Le modèle de l'intelligence économique » (Université de Poitiers, 2023). https://hal.science/tel-04563954.

II.4 Férocité de la compétition économique mondiale

Ali Laidi, docteur en sciences politiques et chercheur à l'Iris, a beaucoup étudié la réalité de la guerre économique, et en a notamment retracé son histoire à travers les âges, démontrant que « *la guerre économique est à l'économie ce que la science de la guerre est à la politique, un affrontement pour capter les ressources* » [50]. Son analyse historique permet de comprendre que « *le mythe libéral du « doux commerce » a toujours nié cette évidence : la politique n'a pas le monopole de la violence. Elle le partage avec l'économie* » [51].

En réalité, le marché dans lequel se développent les entreprises ne correspond pas du tout à la description d'Adam Smith et autres penseurs du libéralisme économique ! L'idéal d'une compétition équitable où le meilleur produit l'emporterait naturellement en rencontrant naturellement les acheteurs n'existe pas. Il s'agit plutôt d'intrications complexes entre acteurs privés et publics qui construisent des stratégies nationales pour dominer la concurrence. Comme le soulignent Dardot et Laval, « *le néolibéralisme est d'abord et avant tout un système de normes introduit à l'initiative de l'État dans les rapports sociaux et dans ses propres rouages* »[52]. Loin de disparaître, « *l'État est un acteur irremplaçable de la co-production des normes de compétitivité avec les grandes multinationales et les institutions internationales* »[53]. Cette réalité contredit fondamentalement la conception idéalisée portée par le libéralisme.

[50] Ali Laïdi, Histoire mondiale de la guerre économique (Perrin, 2016).

[51] Ali Laïdi. « Histoire mondiale de la guerre économique », *Hors collection*, 2023, 104-104.

[52] Pierre Dardot et Christian Laval, La nouvelle raison du monde. Essai sur la société néolibérale (La Découverte, 2010), 5. https://doi.org/10.3917/dec.dardo.2010.01.

[53] Juignet Patrick. « Néolibéralisme - De l'idéologie néolibérale à la pratique du gouvernement », 2020. https://philosciences.com/ideologie-neoliberale.

II.4.1 Importance du cadre juridique

Le cadre juridique constitue un levier stratégique dans l'articulation entre intelligence économique et cybersécurité, dépassant la simple fonction réglementaire pour devenir un instrument de souveraineté numérique. Prenons les cas européens et américains pour mieux comprendre cette réalité.

L'architecture réglementaire européenne comme réponse stratégique

La directive NIS 2 : Elle marque le passage « *d'une logique de sécurisation des sites à une logique de résilience, axée sur la continuité d'activité* »[54]. Cette directive élargit considérablement le périmètre des entités concernées par les obligations de cybersécurité.

Le règlement DORA : Selon Frédéric Hervo, secrétaire général adjoint de l'Autorité de contrôle prudentiel et de résolution (ACPR), ce règlement « *constitue une avancée bienvenue en posant un cadre unifié d'exigences en matière de gestion des risques informatiques et cyber », particulièrement crucial pour le secteur financier qui a subi « plus de 20 000 incidents en vingt ans et une perte de 28 milliards de dollars pour la seule période 2020-2024* ».

Le DMA et le DSA : Ces deux règlements illustrent la volonté européenne de « *durcir sa ligne* » face aux géants numériques en régulant les plateformes et en protégeant les internautes européens. Dans ce contexte de compétition économique sans pitié, l'agressivité dont l'Etat fédéral américain fait preuve dans ce dossier pour défendre la liberté d'action de ses entreprises nationales est particulièrement révélatrice[55] [56].

[54] « Au nom de la commission spéciale sur le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité (procédure accélérée) », (Sénat, 2025). https://www.senat.fr/rap/l24-393/l24-3931.pdf.

[55] Keren Lentschner. « Guerre commerciale : les Gafam au cœur du bras de fer transatlantique », *Le Figaro*, 2 avril 2025, sect. Conjoncture. https://www.lefigaro.fr/conjoncture/guerre-commerciale-les-gafam-au-coeur-du-bras-de-fer-transatlantique-20250402.

[56] Lucas Mediavilla. « Les législations européennes sur le numérique «ne feront pas l'objet d'un marchandage» avec Trump, assure Bercy », *Le Figaro*, 10 avril 2025, sect. Tech & Web. https://www.lefigaro.fr/secteur/high-tech/le-dsa-et-le-dma-ne-feront-pas-l-objet-d-un-marchandage-avec-donald-trump-assure-bercy-20250410.

L'extraterritorialité du droit : un enjeu d'intelligence économique

L'extraterritorialité du droit, notamment américain (Cloud Act, FISA), constitue un défi majeur pour la souveraineté et la sécurité économique européenne. Elle est perçue comme une forme de *lawfare* (guerre juridique), où le droit devient un instrument de puissance et de prédation économique. Comme l'explique la sénatrice Catherine Morin-Desailly, « *le FISA permet le transfert des données des Européens sur simple requête de l'État fédéral. Un Européen peut donc se voir transférer ses données sans avoir reçu de notification, contrairement à un Américain* »[57].

Les entreprises européennes sont ainsi exposées à des risques de fuite de données et à des procédures judiciaires initiées à l'étranger, pouvant les fragiliser ou même les pousser à la faillite, comme l'illustrent les cas de recours abusif à la propriété intellectuelle dans des contextes de concurrence internationale[58].

Face à ces menaces, la France et l'UE ont mis en place des outils défensifs (loi de blocage, conventions judiciaires d'intérêt public, dispositifs d'alerte du SISSE), mais la montée en puissance de ces risques impose une vigilance et une adaptation constante du cadre juridique.

[57] Michel Canévet, « CS Cybersécurité : compte rendu de la semaine du 10 février 2025 », 2025, https://www.senat.fr/compte-rendu-commissions/20250210/cs_cyber.html.
[58] Nicole Buyse. « Le rêve américain contrarié de la jeune pousse lilloise Vade Secure », *Les Echos*, 26 août 2021, sect. Tech - Médias. https://www.lesechos.fr/tech-medias/hightech/le-reve-americain-contrarie-de-la-jeune-pousse-lilloise-vade-secure-1341199.

Le cadre juridique comme outil d'intelligence économique

Le cadre juridique constitue évidemment un élément d'étude important pour l'intelligence économique dans la mesure où l'analyse du cadre légal, normatif et règlementaire se révèle indispensable à la bonne compréhension de nombreuses situations dans la sphère économique, ainsi que de ses enjeux. L'intelligence économique peut donc peut utiliser la connaissance du cadre juridique comme levier stratégique selon trois dimensions :

- La dimension défensive : comme le fait le Secrétariat général de la défense et de la sécurité nationale (SGDSN) pour les entreprises de la défense et pour les opérateurs d'importance vitale (OIV), et le Service de l'information stratégique et de la sécurité économiques (SISSE) dans une stratégie plus économique.
- La dimension normative : comme le rappelle Jean-Baptiste Lemoyne dans son rapport de 2023 [59] *« les entreprises ont donc tout intérêt à développer une stratégie d'influence normative : qui maîtrise la norme maîtrise le marché.* ». L'enjeu est crucial puisque « *90 % des normes actuelles sont élaborées au niveau international. Les états, via leurs organismes nationaux de normalisation, se mènent donc une concurrence rude* ».
- La dimension offensive : l'intelligence économique offensive dans sa dimension juridique consiste à maîtriser et exploiter stratégiquement le droit pour servir ses intérêts sur l'échiquier économique mondial. La maîtrise du droit permet de prendre l'initiative « *pour écarter un concurrent ou pour pénétrer un marché.* »[60]. Dans cette dimension offensive, le stade suprême réside dans la volonté, voire la possibilité, d'influencer le législateur pour créer un cadre légal favorable.

[59] Marie-Noëlle Lienemann et Jean-Baptiste Lemoyne. « Rapport d'information fait au nom de la commission des affaires économiques sur l'intelligence économique, » (Sénat, 2023), 40. https://www.senat.fr/rap/r22-872/r22-8721.pdf.

[60] Bertrand Warusfel. « Intelligence économique et droit », 1995.

II.4.2 Espionnage

L'espionnage, auparavant limité à des actions discrètes et ciblées, a été transformé par les technologies numériques en un dispositif massif, systémique et, souvent, invisible. Les États y consacrent des moyens considérables pour accéder à des données sensibles.

Les Etats-Unis d'Amérique en constituent un parfait exemple, représentant une pratique perpétuellement à l'état de l'art. Dans son ouvrage, *Espionner, mentir, détruire : comment le cyberespace est devenu un champ de bataille* [61] Martin Untersinger décrit comment, en s'appuyant sur les révélations d'Edward Snowden, l'exploitation de programmes tels que PRISM ou XKeyscore a permis aux agences américaines d'intercepter des métadonnées, des contenus de messageries, ou encore des historiques de navigation, grâce à la coopération (forcée ou volontaire) des grandes entreprises du numérique.

Toujours concernant les USA, outre ces programmes confidentiels, le cadre légal organise et assume l'espionnage à vocation économique. Ainsi, l'arrêt de la Cour de justice de l'Union Européenne du 16 juillet 2020, invalidant le *Privacy shield*, mentionne la section 702 du *Foreign Intelligence and Surveillance Act*, et l'*Executive order* 1233, permettant aux agences de renseignements américaines de pratiquer la collecte massive *à priori*, sans mandat judiciaire, des données des "*non US person*", physiques ou morales, dès lors que ces données sont hébergées dans une entreprise de droit américain. La Chine possède peu ou prou le même cadre légal grâce à la loi sur le renseignement national du 28 juin 2017[62].

Ce modèle d'espionnage systémique transforme l'information en ressource stratégique, notamment dans le domaine économique et industriel.

[61] Martin Untersinger et Martin Untersinger, *Espionner, mentir, détruire : comment le cyberespace est devenu un champ de bataille* (Grasset, 2024).

[62] *Cyberguerre d'état : entre discours et réalité*, (Riskintel média, 2023).

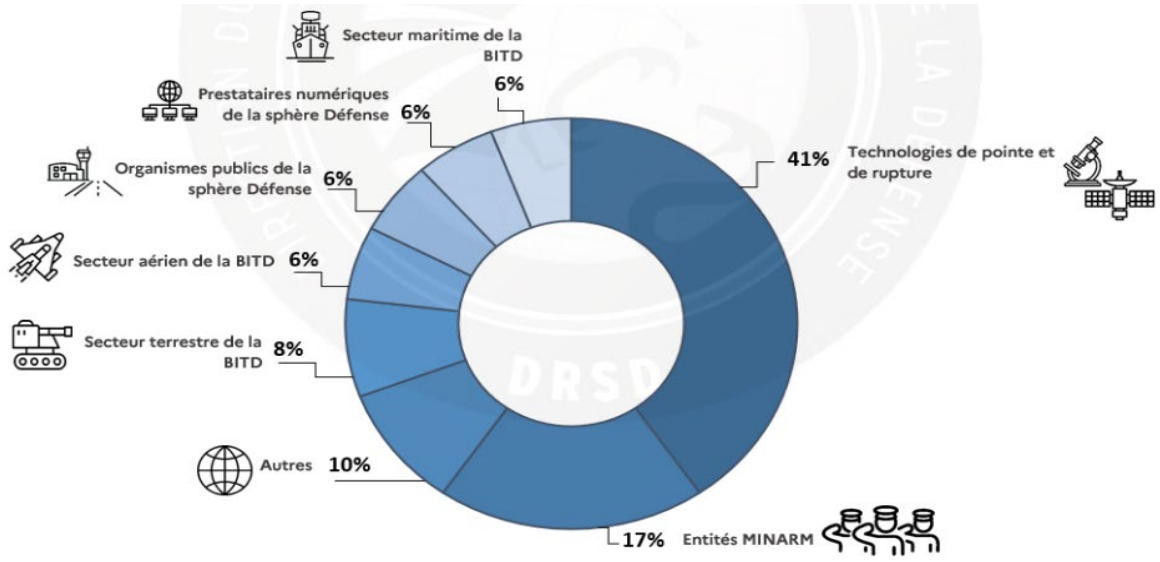


Figure 11 - Répartition des cyberattaques au sein de la BITD en 2023

Source : https://www.defense.gouv.fr/sites/default/files/drsd/LIE-16-Panorama-des-ingerences-a-l-encontre-de-la-sphere-defense-en-2023.pdf

Mais les activités d'espionnage *via* le cyberespace ne constituent pas la chasse gardée des Etats. Des entreprises concurrentes peuvent également opérer ainsi. Croire que les entreprises françaises seraient épargnées par ce phénomène constituerait une erreur d'analyse majeure, comme le démontre la figure ci-dessus. Elles sont la cible d'action d'espionnage économique certes à cause de leur dynamisme, d'un secteur économique particulièrement concurrentiel, de leur détention et création de brevets... mais surtout à cause de leur présence dans le cyberespace. Or s'agissant d'une atteinte à la confidentialité de leur or blanc informationnel, ces faits relèvent bien du champ de la cybersécurité. C'est pour les sensibiliser à ce type de menaces que la DGSE, la DGA, la DRSD communiquent régulièrement sur ces menaces[63], la dernière agence citée y consacrant même récemment un document en accès libre[64].

Ces actes sont tout à fait normaux dans un contexte de guerre économique que permet de dévoiler et décoder la pratique de l'intelligence économique.

[63] Pierre Sauveton. « La guerre de l'ombre contre l'industrie de défense française », 16 mai 2025. https://fr.linkedin.com/pulse/5-la-guerre-de-lombre-contre-lindustrie-d%C3%A9fense-pierre-sauveton-rkbpe.

[64] « L'IE dans la ligne de mire EURONAVAL » (DRSD, 2024). https://www.defense.gouv.fr/sites/default/files/drsd/LIE-Dans-la-ligne-de-mire-EURONAVAL-2024.pdf.

II.4.3 Emergences des menaces hybride

L'un des phénomènes les plus marquants de l'évolution contemporaine de la conflictualité se trouve dans ce changement de paradigme stratégique déjà évoqué dans la première partie, notamment illustré par le remplacement du continuum paix-crise-guerre par le continuum compétition-contestation affrontement. Ce dernier « décrit un schéma systémique où les trois *états interagissent continuellement, les acteurs restant les mêmes malgré les changements de phase*[65] ».

> *« On n'est pas sur une petite opération de cyberattaque, mais bel et bien sur une opération beaucoup plus structurée. »*
>
> Sébastien Lecornu, Ministre des Armées, lors de son audition au Sénat le 25 juin 2024.

La phase de compétition est permanente, s'exerçant dans les domaines économique, social, juridique, commercial et même culturel. Elle se caractérise donc notamment par cet état de guerre économique où les concurrents utilisent absolument l'ensemble des moyens licites, et parfois illicites, à leur disposition pour préserver ou accroître leur position dans un marché donné.

La phase de contestation se caractérise par l'existence de menaces hybrides, brouillant les frontières entre guerre, espionnage, influence et criminalité, « *où l'objectif n'est pas la destruction de l'adversaire mais sa dislocation par des attaques informationnelles ou des actions subversives*[66] ». Combinant actions étatiques directes, usage de groupes privés ou paraétatiques, le cyberespace se prête tout particulièrement à l'accomplissement de cet objectif puisqu'il rend beaucoup plus difficile l'attribution de l'attaque, en même temps que les réseaux sociaux et l'internet fonctionnent comme une caisse de résonance de ces attaques, amplifiant les dégâts des attaques selon une échelle exponentielle.

Une illustration centrale de cette hybridation est l'externalisation croissante de missions cyber offensives par certains États à des groupes de hackers ou entités paraétatiques, souvent désignés sous le terme APT (*Advanced Persistant Threat*). Ces groupes, présentés comme indépendants, sont en réalité étroitement connectés aux services de renseignement. On peut citer :

- APT28 (Fancy Bear), affiliée au GRU, le renseignement militaire russe ;
- APT10, liée au ministère de la Sécurité d'État chinois, responsable de vastes campagnes de vol de propriété intellectuelle.

On peut également penser à la campagne de dénigrement de l'avion Rafale français par des acteurs chinois, suite à la destruction supposée (mais non confirmée à ce jour) de plusieurs exemplaires lors d'une confrontation entre l'Inde et le Pakistan en mai 2025 [67].

---

[65] Nicolas Moinet. « Le nouveau paradigme stratégique : compétition-contestation-affrontement », *IH2EF*, 30 juin 2025. https://www.ih2ef.gouv.fr/le-nouveau-paradigme-strategique-competition-contestation-affrontement.

[66] Nicolas Moinet.

[67] Jules BOITEAU. « Info ou intox - Le Rafale victime d'une campagne de dénigrement dans la sinosphère », France 24, 2 juillet 2025. https://www.france24.com/fr/%C3%A9missions/info-ou-intox/20250702-l-avion-fran%C3%A7ais-rafale-victime-d-une-campagne-de-d%C3%A9nigrement-de-la-sinosph%C3%A8re.

Les travaux de Dakota Cary[68] sur la Chine mettent en exergue la capacité organisationnelle et législative de Pékin à exploiter ce modèle hybride (public, privé) à très grande échelle. Ainsi, à titre d'exemple, le système juridique chinois la réglementation chinoise (RMSV – 2021) oblige les entreprises à divulguer les failles qu'elles découvrent, tout en limitant leur exploitation commerciale ou académique, de manière à ce que les autorités puissent se réserver leur usage offensif à des fins stratégiques. Des entreprises comme Beckhoff, Omron ou Schneider Electric figurent sur la liste du MIIT[69]. Cela place la Chine dans une position singulière : celle d'un État qui construit un réservoir de vulnérabilités « réservées », activables en cas de besoin contre des cibles internationales, avec une coordination assumée entre sphère civile et militaire.

Cette instrumentalisation des vulnérabilités est directement évoquée dans le rapport de l'ANSSI 2025[70], qui alerte sur l'industrialisation de l'usage offensif des failles numériques par des puissances étrangères. Le rapport souligne que ces attaques n'ont plus simplement lieu à des fins lucratives, mais également à des fins de déstabilisation et d'espionnage.

Ainsi, les menaces hybrides s'inscrivent dans une dynamique globale où la cybersécurité ne peut plus être réduite à une simple fonction technique de défense. Elle comprend désormais une dimension stratégique, juridique, géopolitique et économique, nécessitant des entreprises une veille constante et une intégration de la logique d'intelligence économique dans leur gouvernance de la sécurité.

II.5 La souveraineté numérique, une solution ?

La guerre économique fait rage depuis longtemps dans l'espace physique. Mais considérant que « *là où il a de l'homme, il y a de l'hommerie* » comme l'a écrit Saint François de Sales, le cyberespace ne pouvait échapper à cette extension du domaine de la lutte pour la richesse, pour la puissance. Pour y déployer leur stratégie, les acteurs ont besoin d'une certaine liberté d'action qui peut être impactée par les actions malveillantes de leurs concurrents au mieux, de leurs adversaires au pire. Or pour préserver cette liberté d'action, ils mettent en œuvre ce principe de sûreté en instaurant des stratégies spécifiques. La stratégie de cybersécurité constitue le moyen de réaliser ce principe de sûreté dans le cyberespace, créant ainsi de la liberté d'action à utiliser par la stratégie totale. Au regard de toutes les menaces décrites précédemment, étudions comment la souveraineté numérique renforce tout d'abord le potentiel de la stratégie de cybersécurité. Puis comment elle en améliore la résilience.

[68] Del Rosso Kristin et Dakota Cary, « Sleight of hand: How China weaponizes software vulnerabilities », (Atlantic council, 2023).
[69] Andy Greenberg. « How China Demands Tech Firms Reveal Hackable Flaws in Their Products », Wired, 6 septembre 2023. https://www.wired.com/story/china-vulnerability-disclosure-law/.
[70] « Panorama de la cybermenace 2024 » (ANSSI, 2025).

II.5.1 Renforcer le potentiel de la cybersécurité ?

La souveraineté numérique désigne *« la capacité d'un État, d'une entreprise ou d'une organisation à contrôler totalement ses technologies, infrastructures et données stratégiques sans dépendre d'acteurs étrangers. Elle implique une indépendance maximale et repose sur le développement et l'adoption de solutions nationales, à l'abri des réglementations extraterritoriales comme le Cloud Act américain.*[71] »

La souveraineté économique réalise le plein potentiel d'une stratégie de cybersécurité parce que, toute chose étant égale par ailleurs (c'est-à-dire à niveau de performance équivalent), cette approche par la souveraineté permet le mieux d'assurer la confidentialité, l'intégrité et la disponibilité des données détenues, traitées et transmises par l'entreprise. En effet, il est tout à fait juste que les auteurs de l'étude, dans leur définition, citent le Cloud Act comme une menace puisque la souveraineté numérique sert en premier lieu à améliorer sa protection face aux acteurs étrangers qui utiliseraient le droit comme une arme. **En faisant le choix de solutions matérielles, cloud et logicielles souveraines, les acteurs économiques réalisent le principe de sûreté car ils se mettent à l'abri des coups adverses**, soit parce ceux-ci utiliseraient le droit, soit parce qu'ils fourniraient des machines comportant déjà des « portes dérobées » au moment de la vente.

II.5.2 Renforcer la résilience de l'entreprise ?

Pour comprendre la notion de résilience, il faut se tourner vers la mécanique des matériaux qui a, en premier, utilisé ce terme. Il s'agit de la capacité d'un matériau à retrouver sa forme initiale après avoir supporté un choc sans s'être brisé. Appliqué au monde de l'entreprise, on pourrait donc définir la résilience comme la capacité à retrouver un mode de fonctionnement nominal le plus rapidement possible, et avec le moins d'impacts négatifs possibles, après avoir affronté une situation particulièrement grave, quel que soit son origine. La cyber-résilience, qui constitue une sous-catégorie de cette résilience totale de l'entreprise, se définit par la capacité du système d'informations à retrouver un mode de fonctionnement nominal le plus rapidement possible, en ayant le moins de séquelles possibles, après avoir été confronté à une crise d'origine cyber.

La souveraineté numérique améliore la résilience de l'entreprise parce qu'elle la rend moins dépendante de solutions totalement intégrées, ou totalement étrangères. Ainsi, quand une organisation confie à une entreprise comme Microsoft la totalité de ses activités de bureautique (traitement de texte, espaces numériques de travail, visioconférence, partage de données…), il est certain que cela produit un certain confort, une praticité dans l'utilisation quotidienne, et pour cause puisque tous ces logiciels sont conçus pour fonctionner ensemble, et l' « expérience client » est d'autant plus satisfaisante que l'on utilise toutes les briques proposées par le même éditeur de logiciel. Toutefois, cette situation crée une véritable dépendance auprès de cet éditeur. Ça agit telle une sorte de drogue… car lorsque Microsoft augmente ses tarifs de 30%, on s'aperçoit alors que l'on a créé sa propre impuissance, sa propre dépendance. On peut également citer plus récemment la plateforme Wetransfer, largement plébiscitée par les professionnels de la création, qui a tenté de réécrire sa clause

[71] « Manifeste souveraineté technologique l'autonomie stratégique » (Innovator Makers Alliance, mars 2025). https://www.illuin.tech/wp-content/uploads/2025/03/Manifeste_Souverainete-Technologique-lAutonomie-Strategique_Innovation-Makers-Alliance_2025.pdf.

6.3, s'octroyant une licence « *perpétuelle, mondiale, non exclusive, gratuite, transférable et sous-licenciable* » sur tous les fichiers hébergés. Plus troublant encore : elle incluait le droit de « *reproduire, distribuer, modifier, créer des œuvres dérivées* », et précisait explicitement l'usage potentiel du contenu pour « *améliorer les performances des modèles d'apprentissage automatique servant à la modération* »[72]. Dernier exemple, prospectif cette fois : 70% des câbles sous-marins indispensables au bon fonctionnement d'internet appartiennent à des entreprises américaines, tandis que les Etats-Unis d'Amérique hébergent la grande majorité des *data centers* du monde entier. Qui peut aujourd'hui promettre que l'accès à ces data centers ne sera jamais dégradé ? Qui peut promettre que l'utilisation des câbles sous-marins ne deviendra jamais payante, même à un tarif symbolique ? Personne…

Chacune de ces situations a conduit, ou pourrait conduire, une entreprise dans une situation de crise, révélant ainsi sa dépendance ; coupant ainsi le crin de cheval retenant l'épée de Damoclès dont on ignorait l'existence, ou dont on minorait la taille, le poids, le tranchant… Faire le choix de la souveraineté numérique, toujours toutes choses étant égales par ailleurs, C'est la garantie d'une meilleure résilience parce que celle-ci diminue non seulement la probabilité de survenue d'une crise, mais aussi sa gravité d'impact.

Pour conclure cette deuxième partie, il faut commencer par rappeler que le « mode stratégique indirect » a pris le pas sur le « mode stratégique direct ». C'est-à-dire, comme cela a été expliqué dans la première partie, que nous nous trouvons dans une situation de guerre économique, traduisant le fait que la stratégie économique est devenue le facteur essentiel de la stratégie totale d'une nation.

Or le cyberespace se prête particulièrement bien au déploiement d'une stratégie **indirecte**, la généralisation de la transformation numérique s'étant accompagnée d'un degré croissant d'interconnexion entre les acteurs économiques, publics et sociaux. Pour mieux comprendre la conflictualité de ce continent immatériel, la méthodologie de l'intelligence économique s'avère indispensable puisqu'elle dévoile les coups que se portent les différents acteurs au travers de l'instrumentalisation du droit, de l'espionnage, de l'emploi de supplétifs cybercriminels, des manipulations informationnelles… Cette évolution du cyberespace a contribué à faire émerger un nouveau paradigme : le risque numérique ne relève plus exclusivement du périmètre technique, mais constitue désormais un facteur critique influant directement sur la continuité d'activité, la réputation et la performance des organisations. Dans ce contexte, les cadres dirigeants sont contraints de redéfinir leur approche de la gestion des risques afin d'intégrer les enjeux numériques au même titre que les dimensions stratégiques, économiques et juridiques classiques (ANSSI, 2021).

En conséquence, il y a deux enseignements à en tirer toujours grâce à l'apport de l'intelligence économique. Tout d'abord, la **souveraineté numérique renforce la stratégie de cybersécurité** en la rendant plus sûre, plus résiliente. Elle améliore la liberté d'action de l'organisation qui y a recours. *A minima*, puisque la souveraineté peut être difficile à atteindre, il est attendu que les acteurs recherchent par défaut une certaine autonomie stratégique qui « *ne vise pas l'indépendance totale, mais plutôt la capacité à choisir ses dépendances et à*

[72] Amandine Jonniaux. « Finalement, WeTransfer fait marche arrière sur l'utilisation de vos données », Journal du Geek, 17 juillet 2025. https://www.journaldugeek.com/2025/07/17/finalement-wetransfer-fait-marche-arriere-sur-lutilisation-de-vos-donnees/.

garantir des alternatives viables en cas de crise ou de rupture technologique. Elle repose sur une diversification des fournisseurs et une capacité à développer des solutions locales ou européennes pour éviter des situations de monopole ou de vulnérabilité.[73] ».

Deuxièmement, la gouvernance de la sécurité doit être exercée **au plus haut niveau de l'organisation**, notamment au sein de ses instances de direction et de pilotage stratégique. Cela implique une responsabilité partagée entre les différentes fonctions de l'entreprise, y compris les métiers, dans une logique d'**intégration transversale de la cybersécurité**.

Désormais, Dans ce contexte de mode stratégique indirect marqué par la prévalence de la stratégie économique, et par le rôle capital du cyberespace dans le degré de liberté d'action dont disposent les acteurs, il apparait clairement que la cybersécurité ainsi que l'intelligence économique sont les deux premiers piliers dans la recherche de puissance à la fois de l'État et du tissu industriel. La Cybersécurité Technique (appelé également cybersécurité technico-financière dans les parties précédentes de cette ouvrage) ainsi que l'Intelligence Économique seront en conséquence les deux premiers axes de notre modèle de maturité présenté dans la cinquième partie. En conséquence, nous détaillerons les différents niveaux de ces deux axes : de la Cyber Réactivité à la Cyber Résilience, et de l'IE Réactive à l'IE Influente.

Il est maintenant temps d'étudier le rôle de l'État français au service de la stratégie de cybersécurité des acteurs privés.

[73] « Manifeste souveraineté technologique l'autonomie stratégique », p.7

III. Etat et cyber-puissance au soutien de la souveraineté numérique

De la même manière que la gouvernance de la cybersécurité dans une entreprise constitue un sous-système de la grande stratégie de celle-ci, la stratégie cyber d'une nation constitue un sous-système de la grande stratégie nationale. Cette grande stratégie n'est jamais une fin en soi, mais au service de la puissance de l'organisation qui la met en œuvre, ici la puissance de la nation française. La trajectoire de puissance d'une nation impose de faire preuve de courage et de lucidité quant à ses dépendances et ses "lieux de souveraineté", et donc d'autonomie. Or si « l'Etat ne peut pas tout » pour reprendre ces mots devenus célèbres du premier ministre Lionel Jospin, les acteurs privés ne peuvent pas tout non plus. La recherche de puissance appelle une interdépendance assumée entre action publique, industrie et écosystèmes d'innovation. En France, l'enjeu est désormais d'articuler cette coopération autour d'un cap clair : reconquérir des marges de manœuvre dans les domaines qui conditionnent la compétitivité - du numérique à l'énergie - afin que, souverainement, l'économie contribue à l'accroissement de la puissance, dans le cadre d'une grande stratégie nationale.

L'histoire du Japon du milieu du XIX^{e} siècle offre un précédent éclairant, lorsqu'il fut brusquement « ouvert » par la diplomatie de la canonnière. L'expédition du commodore Perry (1853-1854) déboucha sur la convention de Kanagawa et une série de « traités inégaux » qui mirent à nu ses vulnérabilités. La restauration Meiji (1868) fut alors une réponse systémique : audit sans complaisance des faiblesses, importation rapide de savoirs et de technologies occidentales, hybridation avec les traditions nationales. Moins d'un demi-siècle plus tard, la victoire nippone sur la Russie (1904-1905) consacrait l'entrée du Japon parmi les puissances de premier rang. L'enseignement n'est pas de singer son adversaire ou compétiteur, mais d'apprendre de lui pour mieux se réinventer — ce que Nitobe s'employa à expliquer à ses lecteurs occidentaux en exposant l'éthique nippone et sa capacité d'adaptation dans son ouvrage Bushido : l'âme du Japon.

La France se trouve aujourd'hui dans une conjoncture analogue sur le fond : intensification de la concurrence internationale, dépendances critiques et risque de vassalisation par l'effet cumulé des normes, des plateformes et des chaînes d'approvisionnement dominées par d'autres puissances. Dans l'espace numérique — nouvelle profondeur stratégique — la souveraineté des données, la maîtrise des infrastructures (câbles, cloud, semi-conducteurs...) et des logiciels, tout comme la sécurité des chaînes de valeur, conditionnent la liberté d'action économique et politique. C'est le sens des travaux qui lient « souveraineté numérique » et sécurité nationale, plaidant pour une approche réellement géopolitique des choix IT et industriels.

Dès lors, il s'agit moins de « déplorer » la guerre économique que d'accepter, avec la brutalité du réel, un double mouvement : regarder ses adversaires et ses propres faiblesses tels qu'ils sont, pour décider. Concrètement, cela signifie :

(1) une gouvernance de l'intelligence économique assumée — protection, influence, diplomatie économique — au service d'une stratégie de compétitivité de long terme ;

(2) un partenariat public-privé offensif dans les technologies critiques (cloud, IA, cybersécurité, composants), avec diversification des dépendances et relocalisations ciblées ;

(3) une politique d'« intelligence » appliquée au cyber, articulant renseignement ouvert, sécurité offensive et influence, pour élever la résilience de l'écosystème productif. Ce sont là

des démarches déjà balisées par la littérature française sur l'IE (guerre économique, sécurité et compétitivité) et par les cadres stratégiques récents des directions du numérique.

En somme, redevenir un acteur économique de premier ordre suppose d'assumer un « moment Meiji » à la française : apprendre vite, adapter mieux, protéger ce qui compte, influencer ce que l'on ne contrôle pas — au service de la grande stratégie nationale, au service de la puissance.

A cet effet, cette partie commencera par présenter un modèle d'évaluation de la maturité de la stratégie de cybersécurité, puis elle se poursuivra par une rapide présentation des forces et faiblesses du modèle français. Dans un troisième temps, nous présenterons un certain nombre de recommandations pour la stratégie nationale française, au service de la souveraineté numérique des acteurs privés et publics, au service de la grande stratégie nationale française, au service de la puissance.

III.1 Modèle de maturité de stratégie de cyber-puissance

Afin d'évaluer la maturité des stratégies de cyber-puissance mises en œuvre par les acteurs publics et privés, des chercheurs et organismes ont proposé un modèle aidant à les situer. National Cyber Power Index 2022 (NCPI) du Belfer Center (Harvard Kennedy School)[74]. En 2022, NCPI classait la France **9e** sur **30** pays, avec un score global de 60,5 / 100. Cette évaluation s'appuie sur huit axes de cyber-puissance, chacun mesuré à travers des indicateurs de capacités (techniques, industrielles, de résilience) et d'intentions (stratégies, doctrines, budgets).

Comme le souligne la figure ci-dessous cette 9e place souligne une cyber puissance robuste en matière de défense et de normatif, en évolution constante.

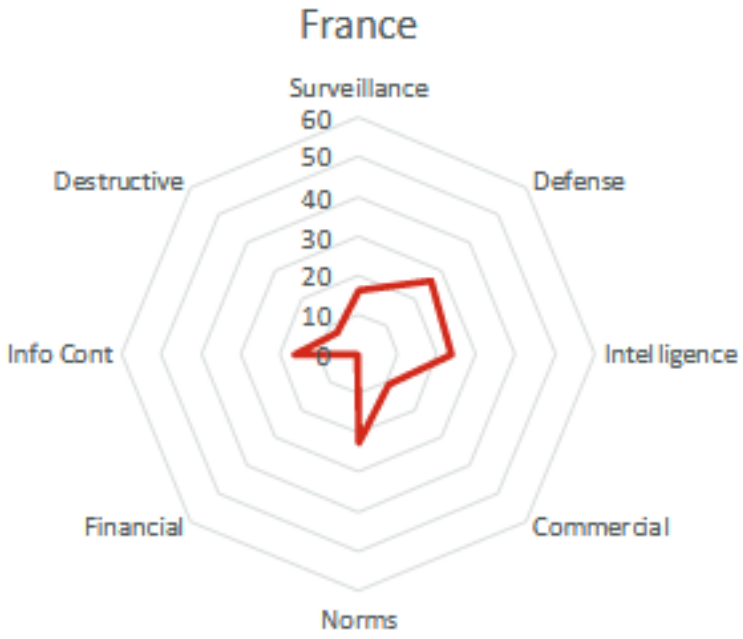


Figure 12 - Radars nationaux de puissance cybernétique par objectif

Source : Julia Voo, Irfan Hemani et Daniel Cassidy, « National Cyber Power Index 2022 », Belfer Center, 2022

Malgré des capacités défensives solides et une industrie cyber nationale dynamique, les ambitions françaises peinent parfois à se traduire en actions cohérentes. Ce qui s'exprime dans le graphique ci-dessous où la France n'arrive pas à se démarquer.

[74] Julia Voo, Irfan Hemani, et Daniel Cassidy. « National Cyber Power Index 2022 », Belfer Center, 2022. https://www.belfercenter.org/publication/national-cyber-power-index-2022.

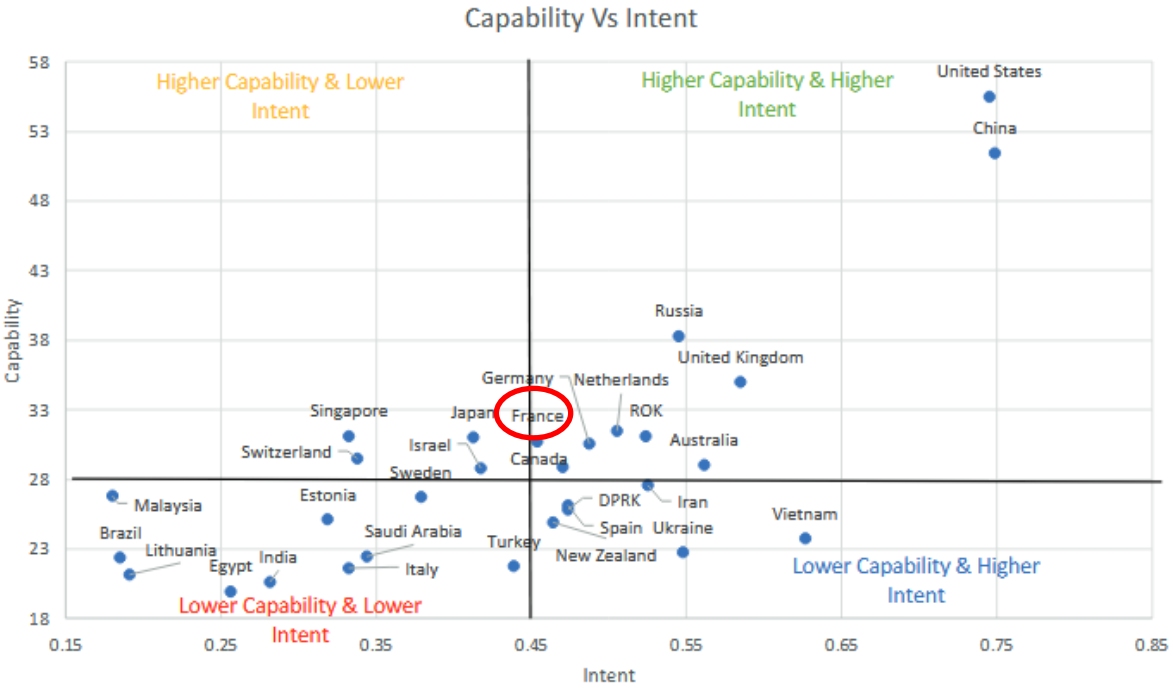


Figure 13 - Diagramme de dispersion « Capacité *vs* Intention »

Source : Julia Voo, Irfan Hemani et Daniel Cassidy, « National Cyber Power Index 2022 », Belfer Center, 2022

Deux leviers méritent une attention prioritaire : le financement pérenne des initiatives cyber et l'accompagnement commercial des acteurs du secteur. Le décalage entre ces capacités et les intentions se traduit par une trajectoire politique marquée par l'irrégularité.

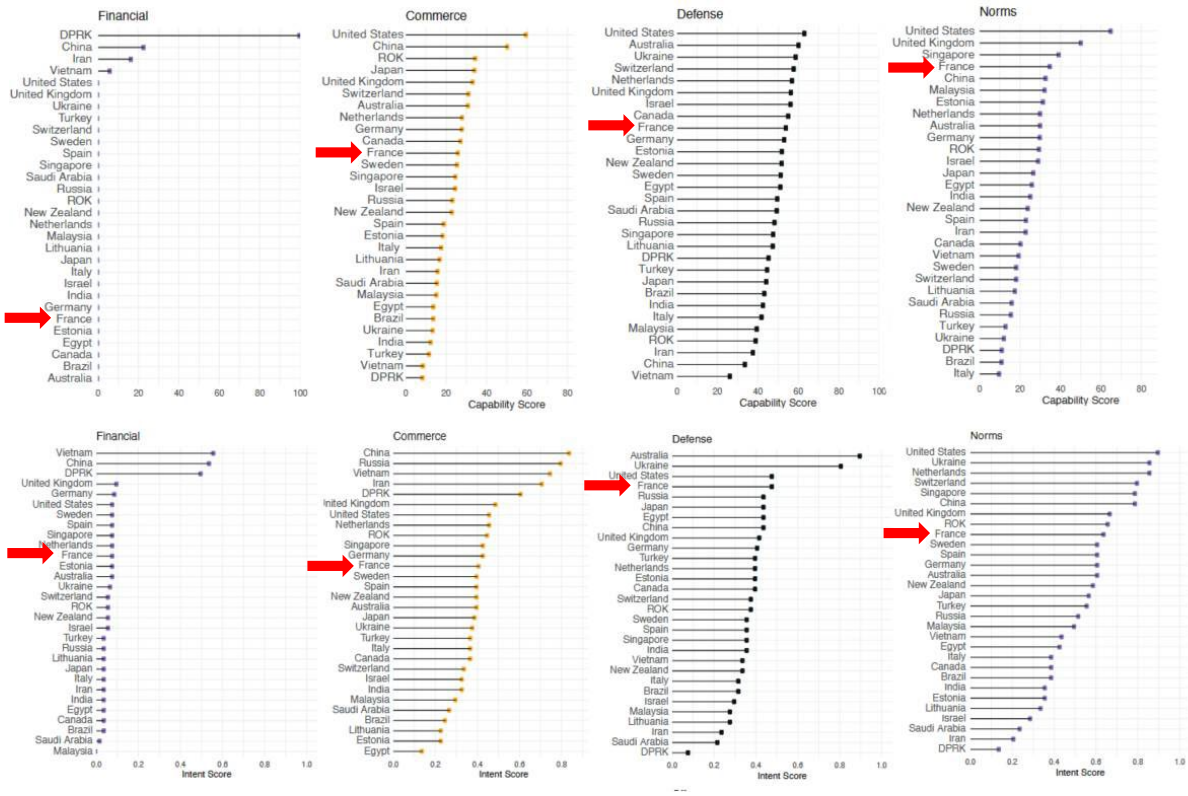


Figure 14 - Résultats par capacité et résultats par intention par secteur

Source : Julia Voo, Irfan Hemani et Daniel Cassidy, « National Cyber Power Index 2022 », Belfer Center, 2022

Dans ce contexte, l'intelligence économique constitue un pilier structurant de la cyber puissance française, agissant comme levier de compétitivité et de souveraineté technologique. En mobilisant la collecte, le traitement et la diffusion de l'information, elle construit un processus en réseau visant à maximiser la valeur ajoutée de chaque interaction humaine.

Tableau 1 : Trois dimensions de l'intelligence économique dans le NCPI

Source : Julia Voo, Irfan Hemani et Daniel Cassidy, « National Cyber Power Index 2022 », Belfer Center, 2022

Dimension	Finalité stratégique	Exemples de capacités/indicateurs suivis par le NCPI
Veille technologique & R&D	Soutenir l'autonomie et l'avance industrielle	Dépenses publiques/privées de R&D, effectifs de chercheurs cyber, volume de brevets nationaux
Espionnage industriel	Accélérer le transfert de technologies critiques	Incidents attribués d'exfiltration IP, implantation d'APT sectorielles, nombre d'opérations « supply-chain » majeures
Monétisation illicite	Financer l'État ou contourner des sanctions	Campagnes de rançongiciels étatiques, vols de crypto-actifs, braquages numériques de banques centrales (ex. activités du groupe cybercriminel Lazarus, considéré comme une APT nord-coréenne)

Ce modèle de maturité, tout comme les autres pouvant exister, se révèle intéressant car il permet d'objectiver une opinion ou une analyse par le biais de métriques. Celles-ci peuvent être débattues mais elles ont le mérite d'exister.

Pour gagner encore en finesse d'analyse d'une situation, d'évaluation d'un modèle, il apparaît judicieux de pondérer celui-ci soit avec un d'autres grilles d'analyses. En sus de cette approche, nous avons choisi de nous inspirer de la matrice **SWOT** (*strenghts, weaknesses, opportunities, threats*) pour compléter notre vision de la situation française.

III.2 Matrice SWOT du modèle français

Au regard de la volonté et de la nécessité d'améliorer la souveraineté numérique des acteurs privés et publics français, quelles sont les forces et les faiblesses du modèle français ?

Avant d'étudier chacune des composantes de la matrice SWOT (forces, faiblesses, opportunités et menaces), les voici résumées ci-dessous. Il convient également de préciser qu'une telle entreprise s'avère extrêmement ambitieuse et que cette sous-partie n'a donc pas pour ambition d'épuiser l'énumération du contenu de ces quatre composantes au sujet de la France. Le traitement du sujet ne sera donc pas exhaustif. Nul doute que les lecteurs trouveront donc de quoi compléter chacun des éléments de la matrice.

Forces	Faiblesses
• Volonté politique forte • L'expertise technique reconnue des différentes agences • Initiatives législatives nombreuses • Politique énergétique	• Comportement des acheteurs publics • Manque d'autorité et de coordination interministérielle • Manque de doctrine juridique
Opportunités	**Menaces**
• Développement du leadership numérique en Europe • Renforcement de l'attractivité territoriale	• Colonisation numérique • Overdose législative et cadre limitant

Figure 15 - Matrice SWOT

III.2.1 Forces

Sans notion de classement par ordre d'importance, **la volonté politique de constituer une puissance dans le cyberespace apparaît comme la première des forces**. En effet, Même si le langage n'est pas performatif, la prise de conscience de l'existence d'un territoire cyber comme enjeu de puissance constitue bien le préalable à toute vision réfléchie de la France dans ce territoire. Cette volonté politique s'est traduite, entre autres nombreuses réalisations, par la publication de la Revue stratégique de cyberdéfense en 2018[75], puis par l'intégration des enjeux liés au cyberespace dans la Revue nationale stratégique de 2022 (objectif stratégique n°4[76]) puis son actualisation en 2025 (objectif stratégique n°4[77]). Les nombreuses traductions en actes de ces documents ont contribué au durcissement de la protection des systèmes informatiques de l'État et des organismes d'importance vitale, et au renforcement de la sécurité numérique pour les citoyens, les institutions et l'ensemble des

[75] « Revue stratégique de cyberdéfense » (SGDSN, 2018). https://www.sgdsn.gouv.fr/files/files/Publications/20180206-np-revue-cyber-public-v3.3-publication.pdf.
[76] « Revue nationale stratégique » (SGDSN, 2022). https://www.sgdsn.gouv.fr/files/files/Revue%20nationale%20strat%C3%A9gique%20-%20Fran%C3%A7ais.pdf.
[77] « Revue nationale stratégique 2025 » (SGDSN, 2025). http://www.sgdsn.gouv.fr/publications/revue-nationale-strategique-2025.

acteurs qui participent du dynamisme économique, industriel, social et culturel. En parallèle de cette volonté politique, les acteurs économiques français de l'IT et du cyber se distinguent par une forte capacité à se regrouper dans des associations de lobbying, leur permettant de présenter un front uni aux décideurs politiques à même d'éclairer leurs décisions (CIGREF, HEXATRUST, CAMPUS CYBER, FAB8…).

Une autre force du modèle français réside dans l'expertise technique reconnue des différentes agences qui ont progressivement été créées pour répondre aux besoin toujours plus importants et diversifiés. L'ANSSI bien sûr, chef de file de la cybersécurité en France, abritant en son sein le CERT-FR qui, outre son rôle d'assistance technique aux opérateurs d'importance vitale, permet aussi de créer et animer une communauté. Plusieurs ministères ont également investi le cyberespace tels que :

- le Ministère des Armées qui s'est doté à partir de 2017 d'un Commandement dans le cyberespace spécialisé dans la cyberdéfense. Les excellents résultats des militaires engagés dans les différentes éditions des exercices cyber de l'OTAN Lockedshield démontrent leur haut degré de compétences : 2e en 2018[78], 1er en 2019[79], 3e en 2024[80], 2e en 2025[81] ;
- le Ministère de l'Intérieur qui l'a suivi en créant un service éponyme en 2023, spécialisé dans la lutte contre la cybercriminalité, améliorant l'efficacité de services d'enquête à compétence nationale comme l'Office français anti-cybercriminalité (OFAC) pour la police nationale et l'Unité nationale cyber (UNC) pour la gendarmerie nationale. L'échantillon des enquêtés élucidées par ces unités en 2024, tel que rapporté par le Commandement du ministère de l'Intérieur dans le cyberespace (COMCYBER-MI) dans son rapport annuel[82], témoigne encore une fois de l'expertise des membres de ces unités ;
- le Ministère de la Justice qui, au sein de la Juridiction Nationale de Lutte contre la Criminalité organisée (JUNALCO) a créé le Parquet « J3 » spécialisé dans la direction des enquêtes les plus complexes et les plus sensibles en matière de cybercriminalité. La spécialisation de magistrats dans ce contentieux a constitué un pari gagnant au regard des résultats déjà évoqués supra.

[78] « Locked Shields – La France, première nation au classement de l'exercice de Cyberdéfense organisé par l'Otan | ANSSI », 12 mai 2025. https://cyber.gouv.fr/actualites/locked-shields-la-france-premiere-nation-au-classement-de-lexercice-de-cyberdefense.

[79] Laurent Lagneau. « Otan : La France remporte l'édition 2019 de l'exercice de cyberdéfense Locked Shields », Zone Militaire, 13 avril 2019. https://www.opex360.com/2019/04/13/otan-la-france-remporte-ledition-2019-de-lexercice-de-cyberdefense-locked-shields/.

[80] « L'équipe franco-estonienne sur le podium de l'exercice international Locked Shields | Ministère des Armées », 29 avril 2024. http://www.defense.gouv.fr/comcyber/actualites/lequipe-franco-estonienne-podium-lexercice-international-locked-shields.

[81] « Locked Shields 2025 : l'équipe franco-polonaise remporte la 2ème place | Ministère des Armées », 12 mai 2025. http://www.defense.gouv.fr/comcyber/actualites/locked-shields-2025-lequipe-franco-polonaise-remporte-2eme-place.

[82] « Rapport annuel cybercriminalite » (COMCYBER-MI, 2025). https://www.interieur.gouv.fr//sites/minint/files/medias/documents/2025-07/rapport_annuel_cybercriminalite_2025-COMCyber_MI.pdf.

Les initiatives législatives pour réguler l'activités des entreprises dans le cyberespace, principalement d'origine européenne, constituent une autre force du modèle français. En effet, ce corpus législatif, tels que le RGPD (règlement général sur la protection des données), DMA (Digital Market Act) et DSA (Digital Service Act), limite l'autonomie de grandes entreprises étrangères qui profitent de leur situation d'oligopole pour imposer une certaine manière de traiter les données de leurs clients, ou dont le cadre légal national ne protège pas suffisamment le caractère personnel des données qu'elles stockent. Ces textes, parce qu'ils sont contraignants et prévoient des sanctions en cas de manquement, améliorent une forme de souveraineté passive.

Au service de la souveraineté active, au niveau infra-règlementaire, l'État développe et promeut un certain nombre d'initiatives pour aider des entreprises nationales à émerger dans le secteur du numérique. On peut ainsi citer la stratégie nationale cybersécurité France 2030, la doctrine de *cloud* de confiance « SecNumCloud », avec la création de labels de cybersécurité et le financement de centres d'excellence…

Après avoir considéré, de manière non exhaustive, quelques forces du modèle français, il faut observer quelles sont ses lacunes.

Enfin, la politique énergétique française constitue la dernière force qui sera abordée. Grâce aux effets cumulés du choix de l'énergie nucléaire, d'un opérateur historique public, d'un territoire bien maillé et d'infrastructures résilientes, le pays est capable non seulement de fournir un énergie bon marché par rapport à ses voisins, mais aussi de produire un excédent d'électricité (l'an passé, le pays a engrangé un surplus de 89 TWh, exportés chez les voisins). Cette double capacité constitue un avantage énorme pour répondre aux besoins grandissants en énergie des entreprises du numérique, spécialement celles reposant sur l'usage massif de l'intelligence artificielle, et donc de centre de données.

EDF a des objectifs visant à pousser encore sa production. « La France, avec une électricité bas carbone déjà disponible et un réseau largement reconnu comme très robuste, est en capacité d'alimenter une forte croissance des usages numériques, sans rivalité d'usage avec l'industrie et sans sacrifier la décarbonation des usages existants », martelait il y a quelques jours Thomas Veyrenc, Directeur général de pôle en charge de l'économie, de la stratégie et des finances chez RTE.[83]

[83] Lucas Mediavilla. « Investissements massifs, sites sécurisés... En France, les projets de construction de data centers IA battent leur plein », *Le Figaro*, 29 octobre 2025, sect. Tech & Web. https://www.lefigaro.fr/secteur/high-tech/investissements-massifs-sites-securises-en-france-les-projets-de-construction-de-data-centers-ia-battent-leur-plein-20251029.

III.2.2 Faiblesses

« La dépendance des leaders de l'industrie nationale et européenne aux grands acteurs du numérique, dont les capacités (Cloud, IA) sont aujourd'hui indispensables pour rester dans le rythme des innovations des autres industriels extra-européens, constitue également une fragilité importante. »

Revue nationale stratégique 2025, paragraphe 150.

Déjà longuement évoqué auparavant, **le déficit chronique de souveraineté numérique des acteurs privés et publics, mais encore plus leur difficulté à organiser leur autonomie stratégique**, constitue une faiblesse majeure. Ainsi dans un rapport de 2025[84], le Club informatique des grandes entreprises françaises (CIGREF) met en exergue les conséquences de cette dépendance aux géants technologiques étrangers :

- le montant annuel des achats de services de *cloud* et logiciel effectué par les entreprises européennes au bénéfice de l'économie américaine s'élève à 264 milliards d'euros ;
- ces achats européens se traduisent par la génération de 1,9 million d'emplois aux Etats-Unis ;
- le nombre d'emplois supplémentaires qui pourraient être créés dans l'Union Européenne si elle produisait 15% des services *cloud* et logiciel actuellement importés des Etats-Unis s'élève à 463 000 ;
- en cas de poursuite de la hausse des prix de ces services de *cloud* et logiciel, l'amélioration du solde de la balance courante américaine sur dix années pourrait s'élever à 421 milliards d'euros ;
- le gain de productivité total que pourrait générer le développement du secteur des services numérique en Europe s'élève à 1,2%.

Une autre faiblesse française réside dans le comportement des acteurs publics pénalisant l'achat de services de *cloud* et de logiciels d'entreprises françaises, donnant ici corps au concept d'« Etat profond » qui ferait obstruction aux décisions et volontés des décideurs.

Les entreprises françaises du secteur numérique font face à des difficultés majeures pour accéder aux appels d'offres publics, malgré la prise de conscience des enjeux de souveraineté numérique au plus haut sommet de l'Etat. Lors de l'audition d'Hexatrust devant la commission d'enquête sénatoriale sur la commande publique en 2025, Jérôme Lecat, président-directeur général de Scality, a souligné un paradoxe préoccupant : « *les responsables des achats publics en France ont peur de faire confiance à des sociétés françaises* »[85].

[84] « Etude Asteres La dépendance technologique aux services de cloud et logiciels americains » (Asterès, 20 avril 2025). https://www.cigref.fr/wp/wp-content/uploads/2025/04/Etude-Asteres-La-dependance-technologique-aux-services-de-cloud-et-logiciels-americains-avril-2025.pdf.

[85] Stéphane Blanc et al. Commande publique : audition d'Hexatrust, Sénat, 30 avril 2025. https://videos.senat.fr/video.5325612_681113606a372.commande-publique--audition-dhexatrust.

D'abord, la complexité administrative et la multiplicité des guichets créent un labyrinthe procédural dissuasif pour les PME françaises. Les contraintes de la réglementation européenne alourdissent considérablement les démarches. Selon Jean-Marc Joannès, les risques juridiques paralyseraient les acheteurs publics (*« la responsabilité de l'acheteur est d'ordre pénal donc ils vont au moins risqué et par habitude le moins risqué c'est ce que font les autres* »). Toutefois, selon d'autres personnes ayant tenu cette fonction d'acheteur public, la mise en avant du risque pénal semble exagérée. Enfin, un défaut de formation des agents[86] perpétue un cercle vicieux où « *80% des achats de l'État se font auprès d'acteurs américains* »[87]. Cette situation révèle un dysfonctionnement majeur du système d'achat public français qui, malgré les intentions affichées de favoriser les acteurs nationaux, maintient *de facto* une dépendance technologique vis-à-vis des géants américains, compromettant ainsi les objectifs de souveraineté numérique et de cyber-puissance de l'État[88].

A leur décharge, ce comportement repose en partie sur la notion de délit de favoritisme qui rend les agents très prudents et les conduit, pour ne pas prendre de risque, à préférer passer commande à des entreprises américaines. Cette définition du délit de favoritisme, propre au droit français, est donc devenue un problème proprement français. Également, il faut pointer du doigt les organisations publiques consacrant beaucoup de temps, et donc d'argent, au développement de leur propres solutions plutôt que de recourir à des entreprises françaises proposant non seulement des produits de qualité, mais immédiatement disponibles et moins sujets aux risques d'obsolescence programmée. C'est récemment le cas de la Direction interministérielle du numérique (DINUM) qui a lancé un appel d'offres de 120 millions d'euros pour se faire accompagner par un cabinet de conseil avant de développer sa solution « La suite numérique », un projet d'alternative libre à Microsoft 365[89]. Or cette décision est problématique pour plusieurs raisons :

- elle conduit l'Etat à pratiquer une concurrence directe et déloyale à des entreprises françaises déjà bien avancées ;
- il s'agira peut-être d'un cabinet de conseil étranger qui bénéficiera de ce contrat de 120 millions d'euros d'argent public pour conseiller l'Etat ;
- les agents publics de la DINUM vont par la suite être mobilisés pour essayer de faire mieux que des entreprises françaises, et alors même qu'un rapport de la Cour des comptes de juillet 2024 se montrait critique sur sa gestion logicielle[90].

[86] Jean-Marc Joannès. « Une commande publique « sans totem ni tabou », est-ce possible ? », Achatpublic.info, 11 juillet 2025. https://www.achatpublic.info/actualites/editos/2025/07/09/senat-commission-enquete-commande-publique-rapport-mapa-36536.

[87] Stéphane Blanc et al., Commande publique : audition d'Hexatrust.

[88] Jean-Marc Joannès. « Alerte rouge sur les achats publics de solutions numériques », Achatpublic.info, 9 mai 2025. https://www.achatpublic.info/actualites/editos/2025/05/01/alerte-achats-publics-solutions-numeriques-souverainete-commande-publique-36140.

[89] Thomas Morel. « Comment l'État snobe les entreprises numériques françaises », *Valeurs actuelles*, 18 juin 2025. https://www.valeursactuelles.com/clubvaleurs/economie/120-millions-pour-reinventer-la-roue-comment-letat-snobe-les-entreprises-numeriques-francaises.

[90] « Le pilotage transformation numerique-Etat par direction interministerielle du numérique » (Cour des comptes, 2024). https://www.ccomptes.fr/sites/default/files/2024-07/20240710-S-2024-0754-Pilotage-transformation-numerique-Etat-par-direction-interministerielle-du-numerique.pdf.

Troisième faiblesse, le manque d'autorité et de coordination interministérielle. En effet, la Cour des comptes a publié en juin 2025 un rapport particulièrement critique sur la réponse de l'État aux cybermenaces. Le pilotage interministériel, théoriquement placé sous la houlette du Premier ministre *via* le SGDSN, souffre d'un « manque d'autorité »[91] et ne dispose pas des moyens humains et budgétaires suffisants, mais aussi de l'autorité nécessaire pour imposer une vision unifiée aux différents ministères.

Quatrième et dernière faiblesse à être présentée, le manque de doctrine juridique unifiée. Le cadre juridique européen, s'il s'avère relativement solide (cf. annexe 2.2) en imposant des obligations fortes aux entreprises y compris extra-européennes, et en délivrant des amendes élevées, a également créé une relation conflictuelle avec les agents économiques privés. Lorsqu'ils sont extra-européens, ils s'insurgent contre ce cadre légal contraignant, avec l'appui de leur Etat parfois (c'est le cas de l'Etat fédéral américain). Lorsqu'ils sont intra-européens, ils subissent ces règles, et le coût de conformité augmente au détriment d'investissements dans d'autres activités[92].

Dans ce contexte, la France souffre d'un déficit de structure juridique nationale cohérente spécifiquement dédiée au droit de la donnée. La CNIL, surchargée entre missions classiques et contrôle de l'IA, ne peut actuellement pas assurer cette mission. Parallèlement, les entreprises françaises demeurent exposées aux lois américaines au-titre de l'extraterritorialité, comme le Cloud Act et la FISA Section 702, qui autorisent l'accès aux données stockées à l'étranger par des fournisseurs américains. Comme le révèle très bien l'audition d'Anton Carniaux, directeur des affaires publiques et juridiques de Microsoft France, par la commission d'enquête sénatoriale sur la commande publique[93] : *« Microsoft France n'est pas en mesure de garantir la confidentialité des données des citoyens français qu'elle héberge. ».*

[91] Roger Romani. « Au nom de la commission des Affaires étrangères, de la défense et des forces armées sur la cyberdéfense » (Sénat, 8 juillet 2025). https://www.senat.fr/rap/r07-449/r07-4491.pdf.
[92] Jérôme Valat. « La Commission européenne continue de clouer le cercueil de l'innovation numérique », *Le monde*, 7 mai 2024. https://www.lemonde.fr/idees/article/2024/05/07/la-commission-europeenne-continue-de-clouer-le-cercueil-de-l-innovation-numerique_6232047_3232.html.
[93] Simon Uzenat et Dany Wattebled. « Les coûts et les modalités effectifs de la commande publique et la mesure de leur effet d'entraînement sur l'économie française, » (Sénat, 8 juillet 2025).

III.2.3 Opportunités

La première opportunité réside dans la possibilité de devenir le pays moteur de l'Union européenne en matière de services et produits numériques véritablement respectueux de la confidentialité des données des utilisateurs. La France s'affirme progressivement comme un acteur et un promoteur majeur de la souveraineté numérique européenne, portée par une stratégie ambitieuse et des investissements massifs[94]. Le pays bénéficie d'une position privilégiée avec son classement de leader européen dans la préparation à l'intelligence artificielle selon Oxford Insights, avec un score de 79,36[95]. Cette excellence se matérialise par la création du plus grand campus européen dédié à l'IA en Île-de-France, porté par un consortium rassemblant MGX, Bpifrance, Mistral AI et NVIDIA.

L'ambition française se concrétise également par des investissements de 40 milliards d'euros annoncés lors du sommet Choose France, témoignant d'une dynamique économique forte. La stratégie France 2030 pour la cybersécurité, dotée d'un budget dépassant le milliard d'euros dont 720 millions d'euros d'argent public, vise à positionner la France comme champion européen de la cybersécurité. Cette stratégie ambitionne de tripler le chiffre d'affaires de la filière (de 7,3 à 25 milliards d'euros) et de doubler les emplois (de 37 000 à 75 000).[96]

Dans le domaine des infrastructures, la France excelle avec une couverture en très haut débit de 81,4% et en 5G de 93%, au-dessus des moyennes européennes[97]. L'objectif de fibrage intégral du territoire français pour 2025 représente cinq ans d'avance sur l'objectif européen, renforçant ainsi l'attractivité technologique du pays.[98]

Le numérique comme levier stratégique d'attractivité territoriale constitue une deuxième opportunité, à cause des effets de ruissellements de cette attractivité sur de nombreux autres indicateurs économiques et sociaux. Ainsi, l'attractivité territoriale permet aux

---

[94] « Souveraineté technologique : la France renforce ses ambitions européennes », *A2 Consulting* consulté le 1 novembre 2025. https://a2consulting.fr/actualites/souverainete-technologique-la-france-renforce-ses-ambitions-europeennes/.

[95] « La France, leader européen dans la préparation à l'IA selon Oxford Insights (A. Hié, Excelia) », News Tank Éducation & Recherche, consulté le 1 novembre 2025. https://education.newstank.fr/article/view/383496/france-leader-europeen-preparation-ia-selon-oxford-insights-hie-excelia.html.

[96] Fabrice Deblock. « Cybersécurité : l'image de la France sur la scène internationale monte en puissance », *INCYBER NEWS*, 30 novembre 2022. https://incyber.org/article/cybersecurite-limage-de-la-france-sur-la-scene-internationale-monte-en-puissance/.

[97] Olivier Devillers. « Bonne élève de l'UE sur les infrastructures numériques, la France invitée à accélérer sur la formation et les entreprises », *Banque des territoire*, banquedesterritoires.fr, 2 juillet 2024. https://www.banquedesterritoires.fr/bonne-eleve-de-lue-sur-les-infrastructures-numeriques-la-france-invitee-accelerer-sur-la-formation.

[98] Bertrand Lemaire. « La France veut renforcer son leadership numérique », *Républik IT Le Média*, 26 mars 2024, sect. DÉCIDEURS IT. https://www.republik-it.fr/decideurs-it/gouvernance/la-france-veut-renforcer-son-leadership-numerique.html.

collectivités de développer leur rayonnement économique et démographique. L'aménagement numérique est reconnu comme décisif pour l'attractivité, la compétitivité et l'égalité des territoires, offrant aux administrés, entreprises et services publics une connectivité indispensable.[99]

Au niveau national, la France mobilise 25% du plan France Relance (soit 25 milliards d'euros sur 100) pour la transition numérique, avec des investissements dirigés vers l'inclusion numérique et la formation de 400 000 personnes aux métiers du numérique. Cette approche renforce l'attractivité du territoire français pour les talents et les entreprises internationales.[100]

III.2.4 Menaces

La dépendance technologique actuelle qui touche la quasi-totalité des acteurs privés et publics constitue une menace majeure pour la souveraineté française. Le risque étant que cette situation de dépendance ne fasse de la France une colonie numérique des entreprises américaines, et donc de la puissance américaine si l'on se remémore la prévalence du mode stratégique indirect, au regard du rôle de la stratégie économique dans celui-ci. L'Europe subit une véritable colonisation numérique avec 83% des dépenses numériques européennes captées par des acteurs extra-européens, représentant 264 milliards d'euros annuels qui échappent à l'écosystème européen. Cette situation place la France en position de vulnérabilité stratégique, déléguant la maîtrise de ses actifs numériques critiques à des entreprises étrangères.[101]

Les GAFAM déploient des stratégies agressives pour maintenir leur hégémonie, incluant l'attraction des talents français (cf. l'expression de « French Mafia » de l'IA dans la Silicon Valley), le verrouillage technologique et des campagnes de lobbying massives[102]. Ces géants ont dépensé près de 100 millions d'euros par an en lobbying au sein de l'Union européenne, influençant directement les décisions politiques européennes.[103]

L'absence de champions européens pouvant rivaliser avec les géants américains (Amazon, Microsoft, Google détiennent 65% du marché cloud européen) amplifie cette dépendance. Même les projets européens comme Gaia-X subissent l'influence insidieuse des

---

[99] « L'aménagement numérique des territoires », *Arcep*consulté le 1 novembre 2025. https://www.arcep.fr/nos-sujets/lamenagement-numerique-des-territoires.html.

[100] « Le soutien à la transition numérique en France - Représentation en France », consulté le 1 novembre 2025. https://france.representation.ec.europa.eu/strategie-et-priorites/les-politiques-cles-pour-la-france/le-soutien-la-transition-numerique-en-france_fr.

[101] « Souveraineté numérique de l'État : sortir de la dépendance technologique », *Antemeta*, 25 juin 2025. https://www.antemeta.fr/souverainete-numerique-de-letat-sortir-de-la-dependance-technologique/. /

[102] « La guerre informationnelle des GAFAM pour conserver leur hégémonie numérique en Europe », *Ecole de Guerre Economique*, 19 mai 2025. https://www.ege.fr/infoguerre/la-guerre-informationnelle-des-gafam-pour-conserver-leur-hegemonie-numerique-en-europe.

[103] Kenza L. « GAFAM en Europe : la souveraineté numérique européenne en péril », *Portail de l'IE*, 5 décembre 2024. https://www.portail-ie.fr/univers/2024/gafam-en-europe-la-souverainete-numerique-europeenne-en-peril/.

acteurs américains via leurs partenaires européens, compromettant l'objectif initial de souveraineté.[104]

Le risque d'overdose législative qui va être explicité ci-après constitue une menace importante dans la mesure où elle peut impacter négativement la compétitivité et la capacité d'innovation des entreprises françaises. En effet, le rapport que les acteurs économiques entretiennent au cadre légal au sens large doit être étudié de manière quantitative et qualitative.

De manière quantitative tout d'abord parce que plus le nombre de textes auquel une entreprise doit se soumettre est important, plus cela génèrera des coûts, une utilisation des ressources qui ne pourra pas être allouée ailleurs. Ce qui conduira à dégrader la compétitivité des entreprises proposant des solutions *cloud* et logiciel (de cybersécurité ou non), et donc dégradera leur position concurrentielle sur un marché donné, et donc augmentera la probabilité que d'autres entreprises ayant besoin de ce type de solutions se tournent vers des acteurs étrangers plus compétitifs.

Or il semble que la France soit aujourd'hui dans une situation où le nombre de textes encadrant les activités dans le cyberespace a cru si vite que cela place les entreprises dans de grandes difficultés quant à leur capacité d'intégration de ces normes. Ainsi, depuis le début de la décennie numérique 2020-2030, une vingtaine de textes au moins ont vu le jour (cf. annexe 2). Même si on salue leur cohérence, même si on pense que l'on doit soutenir ces textes sur le fond parce qu'ils entérinent le niveau systémique du risque cyber, même si on suppose que toutes les organisations ne sont pas soumises à toutes ces normes, leur rythme, leur volume, et la production d'autres textes qui en découle (règlement d'application, lignes directrices…), interroge… Selon Michel Séjean, cette situation génère un « *état infractionnel généralisé*[105] » pour la plupart des entreprises d'une part, et un « *coût de mise en conformité* » qui pénaliserait la compétitivité des petites entreprises d'autre part, permettant régulièrement à de plus grosses entreprises de les racheter pour écarter notamment leur innovation. La France serait donc dans une situation où elle s'auto-infligerait des blessures en matière de production d'innovations, et l'Union Européenne dans une position où il pourrait devenir compliqué d'infliger des amendes à des entreprises extra-européennes sans devoir les infliger également aux entreprises européennes.

De manière qualitative ensuite, parce que dans la mesure où, en matière de cybersécurité, l'Union Européenne constitue la source principale du droit, se pose la question de la surtransposition. La surtransposition peut être définie comme *« l'adoption ou le maintien de mesures législatives ou réglementaires allant au-delà des exigences minimales d'une directive de l'Union européenne*[106] ». Or Michaël Barthellemy, Directeur du risque cyber et de la gestion des actifs du groupe Airbus, a attiré l'attention de la commission sénatoriale « cybersécurité » sur les conséquences négatives de cette pratique en matière de

[104] Margaux Vulliet. « Quel avenir pour le cloud souverain européen ? », *Challenges*, 11 janvier 2025, sect. Tech - Numérique. https://www.challenges.fr/entreprise/tech-numerique/quel-avenir-pour-le-cloud-souverain-europeen_595864.

[105] Entretien avec Michel Séjean, le 2 mai 2025.

[106] « Qualité du droit : la surtransposition des directives européennes », 26 mars 2019. https://www.vie-publique.fr/en-bref/19813-qualite-du-droit-la-surtransposition-des-directives-europeennes.

compétitivité et d'investissements : « *il ne nous semble plus envisageable aujourd'hui que ce type de mesures soient véhiculées par une directive. Elles devraient impérativement faire l'objet d'un règlement européen. Imaginez en effet la difficulté pour un groupe comme Airbus, présent dans la quasi-totalité des États membres de l'Union, de devoir appliquer vingt-sept réglementations différentes. (…) L'augmentation des sanctions fera également peser une pression financière sur nos entreprises. Nos concurrents internationaux, y compris européens, qui ne sont pas soumis à ces règles, seront avantagés. Veillons à ne pas créer par surtransposition une opportunité de dumping de cybersécurité pour les autres États membres.*[107] »

Les réglementations NIS 2 et DORA, bien que nécessaires pour la sécurité, imposent des obligations de mise en conformité coûteuses aux entreprises. Cette complexité administrative peut pousser certaines entreprises à s'implanter dans des juridictions moins contraignantes, réduisant l'attractivité numérique française.[108]

Ce risque d'overdose législative est accentué par l'inadéquation entre le rythme des mutations technologiques et celui du droit. Cette discordance crée incertitude et frilosité chez les investisseurs, particulièrement dans des secteurs innovants comme l'intelligence artificielle où la réglementation européenne (AI Act) peut être perçue comme prématurément restrictive.[109]

La division des États membres européens sur l'approche réglementaire complique également la situation. Alors que la France et l'Allemagne prônent une autonomie stratégique numérique forte, les Pays-Bas et pays baltes s'inquiètent d'une régulation trop contraignante freinant l'innovation, créant des tensions au sein de l'écosystème européen.[110]

Après ce panorama des principales forces et faiblesses du modèle français pour promouvoir la souveraineté numérique, on peut en déduire plusieurs recommandations.

[107] Cyberdéfense : Airbus, Orange et Thales, Sénat, 11 février 2025. https://videos.senat.fr/video.5040919_67ab8dadc65cb.cyberdefense--airbus-orange-et-thales.
[108] Juliette Françaix. « France 2030 : un nouvel appel à projet et 12 lauréats pour renforcer l'offre industrielle en matière de cybersécurité », *Presse - Ministère des Finances*, 22 novembre 2024. https://presse.economie.gouv.fr/france-2030-un-nouvel-appel-a-projet-et-12-laureats-pour-renforcer-loffre-industrielle-en-matiere-de-cybersecurite/.
[109] « Assemblee-nationale.fr/dyn/opendata/RIONANR5L17BTA0019.html », consulté le 1 novembre 2025. https://www.assemblee-nationale.fr/dyn/opendata/RIONANR5L17BTA0019.html. l
[110] « Souveraineté numérique UE 2025 : l'Europe cherche à reprendre le contrôle face aux géants du numérique - L'Europe à Contre-Courant », 19 juillet 2025. https://europeacontrecourant.eu/europe-souverainete-numerique-ue-2025/.

III.3 Recommandations pour l'Etat

> *« Ce qui manque, c'est le marché, le levier de l'investissement et la commande publique »*
>
> Guillaume Tissier, directeur général du Forum InCyber.

L'Etat représente le principal acteur de la puissance nationale, soit comme acteur direct lorsqu'il définit la stratégie totale et la met œuvre, soit comme acteur indirect lorsqu'il soutient des organisations et des projets au service de sa volonté de puissance. C'est dans cette deuxième perspective que son rôle doit se concevoir lorsqu'il soutient la souveraineté numérique des personnes privées, physiques ou morales, en France, cette souveraineté particulière se situant elle-même au service d'une gouvernance de la cybersécurité alignée avec la grande stratégie d'entreprise. Quatre manières pour l'Etat de renforcer la souveraineté numérique des acteurs privés vont être exposées : le rôle de la commande publique, le soutien au capital-risque, l'établissement d'un cadre concurrentiel équitable, le rôle du législateur.

III.3.1 Mesure 1 : rôle de la commande publique

La première mesure que pourrait prendre l'Etat, au sens « prioritaire » du terme, c'est de mieux et plus diriger la commande publique vers des entreprises françaises du secteur du numérique. En effet, selon Jérôme Lecat[111]: « *80 % des dépenses de l'État en matière de cloud et de logiciels sont effectuées auprès de fournisseurs américains* ».

Or ces dépenses possèdent un effet d'entraînement très important puisqu'elles constituent un outil de passage à l'échelle pour les entreprises clientes, leur offrant une caution et une validation de produit incomparable sur le marché. C'est ainsi que peut être initié un cercle vertueux, puisque ces produits deviennent également plus abordables pour les entreprises cherchant à rendre leur cybersécurité plus souveraine et plus résiliente. La commande publique permet par ailleurs de promouvoir des solutions coconstruites avec les acheteurs publics pour ouvrir de nouveaux marchés vers le privé et l'export.

Pour mieux comprendre le rôle de la commande publique, on doit étudier le cas américain, une nouvelle fois riche d'enseignements. La DARPA (Defense Advanced Research Projects Agency), une agence fédérale comparable à la DGA, a pour objet principal de réaliser des investissements stratégiques dans des technologies de rupture pour renforcer la sécurité nationale américaine, démontrant ainsi un biais pro-technologies assumé. Par exemple, quand Amazon Web Services (AWS) a été choisie en 2013 pour le cloud de la CIA, un contrat de 600 millions de dollars, elle n'était pas le géant qu'elle est devenue (notamment grâce à ce contrat). De la même manière, SpaceX n'aurait pas existé sans les contrats de la NASA puisque lorsque cette agence a passé un premier contrat avec cette entreprise, elle n'avait alors fait voler aucune fusée.

Toutefois, allouer une part importante de la commande publique aux entreprises nationales ne suffit pas, Il faut allouer une part la plus importante possible aux TPE-PME pour les raisons évoquées plus haut. Ainsi il existe aussi outre-Atlantique une attitude en faveur des petites entreprises dans la commande publique comme le démontre le Small Business Act, qui réserve une part des marchés publics aux petites entreprises. Tandis qu'en France, comme

[111] Stéphane Blanc et al., Commande publique : audition d'Hexatrust.

en témoignent Alain Juillet[112], ancien directeur de la DGSE, et Quentin Adam[113], fondateur et CEO de Clever Cloud, l'absence d'un tel cadre légal sur-représente les grandes entreprises dans les marchés publics, qui rognent sur les marges des TPE-PME dans les cas de sous-traitance, avec tous les effets négatifs que cela provoque.

Pour conclure, vient de se finir au Sénat un cycle d'auditions menées par la commission d'enquête sénatoriale sur les coûts et les modalités de la commande publique. Elle a publié une liste de 67 recommandations dont certaines ont beaucoup de sens pour le rôle de la commande publique au service d'entreprises proposant des services *cloud* et logiciels souverains[114] (ces recommandations spécifiques sont présentées dans l'annexe 1).

III.3.2 Mesure 2 : soutenir le capital-risque :

Le capital-risque (*venture capital* ou *VC*) correspond à une prise de participation par un ou des investisseurs, généralement minoritaire(s), au capital de sociétés non cotées. L'objectif de l'investisseur est de réaliser une plus-value substantielle lors de la cession de ses titres. Pour le créateur bénéficiant de cet apport, l'augmentation des fonds propres consolide la structure financière de l'entreprise sans l'endetter, à un moment de la vie de l'entreprise où la banque sera moins encline à accorder un prêt par manque de solvabilité du bénéficiaire.

Or cette capacité à lever des fonds revêt une grande importance dans l'économie de marché contemporaine, notamment dans le secteur du numérique où les investissements initiaux à réaliser peuvent s'avérer particulièrement élevés. A l'échelle d'un marché, d'un pays ou d'une région, la possibilité de bénéficier d'investisseurs aura donc un rôle important dans l'émergence d'entreprises locales proposant des offres souveraines. Cette capacité explique en partie la sur-représentation des entreprises américaines et israéliennes dans le secteur des nouvelles technologies. Selon le journaliste Keren Lentschner, « *[l'] industrie israélienne du numérique a continué à démontrer son attractivité. Elle a levé 12,2 milliards de dollars l'an passé (+ 31 %), dont 15 « méga-opérations » totalisant 4 milliards* »[115]. Le montant s'élève à plus de 4 milliards de dollars si l'on s'en tient aux entreprises israéliennes du secteur de la cybersécurité, représentant un tiers des levées de fonds au niveau mondial (Union Européenne + Israël + Etats-Unis) pour ce secteur d'activité.

---

[112] Alain Juillet. Commande publique : audition d'Alain Juillet, Sénat, 8 avril 2025. https://videos.senat.fr/video.5274762_67f579d885772.commande-publique--audition-dalain-juillet.

[113] Carine Guillemet, « Quentin Adam invité de Micode dans l'émission Underscore_ ».

[114] « Liste des recommandations de la commission d'enquête sur les coûts et les modalités de la commande publique » (Sénat, 8 juillet 2025). https://www.senat.fr/fileadmin/cru-1750816532/Structures_temporaires/commissions_d_enquete/CE_Commande_publique/Liste_recommandations_CE_CP.pdf.

[115] Keren Lentschner. « IA, cybersécurité, agroalimentaire… Comment la tech israélienne résiste à l'épreuve de la guerre », Le Figaro, 16 février 2025, sect. Entreprises. https://www.lefigaro.fr/societes/ia-cybersecurite-agroalimentaire-comment-la-tech-israelienne-resiste-a-l-epreuve-de-la-guerre-20250216.

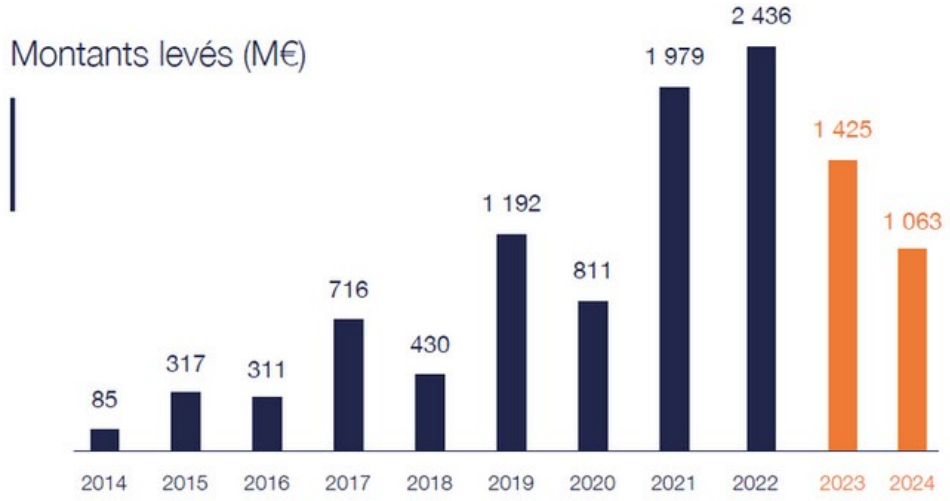


Figure 16 - Montants levés par les entreprises européennes (cybersécurité)

Source : https://www.usine-digitale.fr/article/la-france-devient-championne-europeenne-des-levees-de-fonds-en-cybersecurite.N2228586

Mais c'est toujours beaucoup plus important que les entreprises françaises qui ont levé 342 millions d'euros, permettant tout de même à la France de détenir la première place en Europe, bien que le montant soit en baisse de 25% par rapport à 2023[116]. Outre la part du gâteau particulièrement faible revenant aux entreprises européennes en général, et françaises en particulier, il faut s'inquiéter de ce qu'elle diminue depuis deux années dans des proportions importantes, comme le montre le diagramme ci-contre.

Cet état de fait conduit Thomas Fauré, président-fondateur de la plateforme collaborative pour entreprises Whaller, à écrire : « *Pour faire face à ses défis vitaux pour l'avenir de l'Europe, elle doit mettre en place les conditions d'émergence d'un « écosystème » numérique à même de lui faire recouvrer sa souveraineté numérique. À ce sujet les besoins financiers sont gigantesques. Clé de voûte des futurs succès, il faut avoir la capacité de financer la R&D et les futures licornes européennes.* ***Actuellement, il manque en Europe les fonds d'investissements capables de mettre plus de 100 millions d'euros dans une startup prometteuse pour permettre son développement et retenir ses talents*** *- encore aspirés par la Silicon Valley. Il faut donc favoriser le financement des startups et des ETI des nouvelles technologies. Car ce sont elles qui seront les licornes de demain et les Blue Chip d'après-demain.*[117] »

Pour comprendre comment résoudre cette disparité d'accès aux financements, il faut comprendre d'où vient cette disparité. Le modèle français repose en partie sur une fiscalité très lourde captant une part importante de la richesse privée, et qui est en partie réinjectée

[116] Yoann Bourgin. « La France devient championne européenne des levées de fonds en cybersécurité », *Usine digitale*, 7 mars 2025. https://www.usine-digitale.fr/article/la-france-devient-championne-europeenne-des-levees-de-fonds-en-cybersecurite.N2228586.

[117] FAURÉ, Thomas. Saison 10 : l'Europe à l'avant-garde. In : Après Facebook, rebâtir. Les éditions de Passy, 2022. p. 148

sous forme de pensions de retraite, dans le cadre d'un modèle « par répartition ». Au contraire, les Etats-Unis s'illustrent par une fiscalité beaucoup moins importante et un modèle de retraite « par capitalisation ». Il ne s'agit pas ici d'émettre un jugement de valeur sur ces choix, mais simplement d'en décrire les effets sur l'économie réelle. Car dans un système par capitalisation, les actifs confient leur épargne à des tiers pour la faire fructifier en vue de leur retraite, et ces tiers sont en partie constitués de fonds d'investissement qui placent l'argent confié dans des entreprises à l'occasion de levées de fonds. Au contraire, en France, la part prélevée est si importante que les fonds restants pour être confiés à des fonds d'investissement ne suffisent pas à couvrir les besoins des entreprises françaises.

Pour conclure, à la lumière de ce bref exposé, il y aurait deux grandes manières de résoudre cette difficulté d'accès au capital-risque : d'une part réussir à capter un pourcentage plus important de l'argent mis à disposition par les fonds d'investissement étrangers, d'autre part diminuer la part de la richesse française prélevée par l'Etat afin qu'elle soit réinjectée dans l'économie privée par le biais de fonds d'investissement.

III.3.3 Mesure 3 : promouvoir une concurrence équitable

Une des forces des entreprises américaines repose dans leur capacité à s'adresser à un marché homogène de 347 millions de consommateurs. Homogène parce que soumis au même cadre légal, et aux mêmes *habitus* culturels. Un enjeu de taille pour les entreprises françaises consiste donc à pouvoir accéder à un marché le plus grand possible, leur permettant d'accroître le chiffre d'affaires afin de gagner en notoriété, en compétitivité et d'investir plus dans des activités de R&D. Grâce à ces trois éléments, plus d'entreprises françaises seront séduites par leurs produits, plus leur autonomie stratégique en sortira accrue.

On peut opposer à cette taille du marché américain le marché unique européen rassemblant 512 millions de consommateurs. Si en effet le marché unique a fait tomber de nombreuses barrières commerciales tarifaires et non tarifaires entre les Etats membres, l'intégration aussi poussée que d'autres marchés nationaux demeure un objectif à réaliser. Et ce pour plusieurs raisons. Tout d'abord parce que les Etats conservent une autonomie (réduite) en matière de production de normes et qu'ils arrivent ainsi à mettre en œuvre une politique de protectionnisme à bas bruit. C'est par exemple le cas de la part des dépenses publiques qui doivent être allouées à des entreprises nationales, et qui est régie en France par le code des marchés publics. Ce problème se retrouve à l'échelle européenne si l'on en croit Thomas Fauré : « *Par ailleurs, il serait normal, comme cela se pratique à l'étranger, notamment aux États-Unis, que l'Union européenne impose une part d'achats de biens européens dans les marchés publics. Elle doit favoriser les solutions locales et non brandir comme un totem l'« open source » au motif que choisir un fournisseur européen équivaudrait à faire du favoritisme. Il existe encore une défiance du service public à l'égard du secteur privé fondée sur l'idée que l'enrichissement des entrepreneurs est condamnable. Elle pourrait adopter une clause de préférence communautaire pour les entreprises européennes*

concourant sur les marchés publics européens. Ceux-ci sont ouverts à 90 % aux entreprises étrangères, alors qu'ils ne le sont qu'à 30 % aux États-Unis et 16 % au Canada.[118] »

Ensuite, les rivalités entre Etats européens (ceux-ci conservant une partie de leur souveraineté et divergeant sur leurs intérêts stratégiques) se recyclent dans la sphère économique par une rivalité entre acteurs nationaux et s'expriment par une préférence nationale. Ainsi, dans la compétition entre acteurs économiques sur le marché de la cybersécurité, on peut déclarer qu'une solution d'origine allemande serait meilleure que celle d'une entreprise américaine dans la mesure où l'approche retenue, la philosophie générale de son action, en matière de confidentialité / intégrité / disponibilité de la donnée sera beaucoup plus proche de celle française. Mais pour autant, il serait préférable qu'une entreprise française soit choisie.

Pour continuer de tendre vers un marché unique de 512 millions de consommateurs, il ne faut donc pas tomber dans le travers d'une politique protectionniste assumée qui, en plus de faire l'objet d'actions auprès de l'OMC sur la forme, s'avèrerait contre-productive sur le fond. Toutefois, les décideurs politiques ne sont pas condamnés à l'inaction comme le relève Thomas Fauré : « *Dans le secteur numérique comme ailleurs, le rôle du législateur consiste à démanteler toutes les entraves législatives et règlementaires à la liberté du commerce et de l'industrie, et en même temps à s'assurer que tous les concurrents puissent jouer. En aucun cas la législation ne peut se borner à être neutre si on veut que la concurrence s'exprime. Méfions-nous de cette idée que « l'interventionnisme [est] considéré comme inefficace et l'innovation comme forcément positive. »* [119]»

Les décideurs doivent donc travailler tout autant à l'homogénéité toujours plus poussée du marché européen afin qu'il corresponde toujours moins à l'addition de marchés nationaux, qu'à la promotion, en son sein, des acteurs économiques locaux.

[118] FAURÉ, Thomas. Saison 10 : l'Europe à l'avant-garde. In : Après Facebook, rebâtir. Les éditions de Passy, 2022. p. 149

[119] FAURÉ, Thomas. Saison 9 : pourquoi s'opposer aux GAFAM. In : Après Facebook, rebâtir. Les éditions de Passy, 2022. p. 138

III.3.4 Mesure 4 : Rôle de la législation

Comme cela a été étudié dans le cadre des menaces pesant sur le modèle français d'accroissement de puissance par l'économie, et plus particulièrement le secteur du numérique, il apparaît que nous sommes à un moment important. Soit les autorités prennent conscience de l'effort important que nécessite cette digestion des nombreux textes produits, soit elles continuent de légiférer au risque de dégrader leur compétitivité et la capacité d'innovation.

> « *Tout l'argent que les entreprises mettront à démontrer qu'elles sont conformes, elles ne l'emploieront pas autrement.* »
>
> Michaël Barthellemy, Airbus

Il semble que la commission ait bien pris en compte cet enjeu puisque lors de l'audition de Claire Chappaz, ministre déléguée pour l'intelligence artificielle et le numérique, par cette même commission, son rapporteur le sénateur Michel Canévet l'a alerté : *« Par ailleurs, vous savez certainement, madame la ministre, que le Sénat entend le plus possible éviter les surtranspositions. Or c'est clairement le cas pour les sociétés de financement. Il ne peut évidemment être question de méconnaître les risques cyber, mais intégrer ces sociétés pose des difficultés particulières : d'une part, hormis deux gros acteurs, il s'agit de structures de petite taille pour lesquelles le coût du processus sera élevé ; d'autre part, ce marché est particulièrement concurrentiel au niveau européen et international et nous ne pouvons pas mettre des boulets aux pieds de nos seules entreprises*. [120]». Claire Chappaz, très engagée dans la transposition dans le droit français des directives NIS2 et DORA, semble partager cet avis : *« En veillant à une transposition au plus proche des textes européens, nous limiterons les frictions juridiques et garantirons une concurrence loyale entre les entités couvertes par NIS 2 dans les différents États membres de l'Union européenne.* [121] »

Pour conclure cette partie sur le rôle des Etats, l'Etat constitue bien un acteur essentiel au service de la cybersécurité des entreprises nationales. En effet, comme cela a été étudié par le prisme (non exhaustif) du rôle de la commande publique, du soutien au capital-risque, de la création d'un cadre concurrentiel équitable et de la fabrication de normes, l'Etat crée une atmosphère au sens scientifique du terme. C'est-à-dire qu'il crée un milieu réunissant les conditions favorables à l'émergence d'un phénomène, ici une gouvernance de la cybersécurité qui, ayant conscience des enjeux de souveraineté de la donnée, crée de la liberté d'action au service de la grande stratégie de l'entreprise.

Or il s'avère que la France dispose pour cela d'un certain nombre d'atouts et de faiblesses qui la placent parmi les cyber-puissances moyennes. En plus de tout ce qui a été évoqué précédemment, voici quelques exemples de réalisations françaises soulignant son statut de puissance moyenne :

[120] Cybersécurité : audition de Clara Chappaz, Sénat, 2025. https://videos.senat.fr/video.4986271_679762adce8d6.cybersecurite--audition-de-clara-chappaz.
[121] Cybersécurité : audition de Clara Chappaz.

- 315 *data centers* en service (dont le campus de Marseille devenu 6e *hub* internet mondial[122]), s'appuyant sur une stratégie nucléaire bas coût et bas carbone ;
- Concernant la propriété de câbles sous-marins, grâce à quelques entreprises françaises (Orange et Agence des Participations de l'Etat), la France est particulièrement dynamique dans ce secteur d'activité indispensable au fonctionnement de l'internet contemporain. Ainsi, ces deux entreprises représentent 35% du marché de la fabrication, réparation et maintenance de ces câbles[123]. Par ailleurs, ces entreprises sont propriétaires d'une cinquantaine de câbles dans le monde, soit 10% environ du volume total ;
- La capacité à former les meilleurs mathématiciens pour travailler dans l'IA [124];
- nombre élevé de mathématiciens français de haut niveau dans la Silicon Valley[125].

Toutefois, la grande dépendance actuelle aux *cloud* et logiciels étrangers en font *de facto* une colonie numérique. Perspective encourageante : les entreprises françaises du même secteur (et du numérique en général) se sont bien organisées en associations et, à force de lobbying, réussissent à obtenir quelques succès symboliques auprès de l'Etat. Conjugués à une relation transatlantique abîmée par un gouvernement américain assumant (enfin) très explicitement son égoïsme économique, cette mobilisation pourrait payer ces prochaines années.

Si la notion de « colonie numérique » demeure valable, c'est parce que celle d'« empire numérique » l'est également. En effet, pour toute nation atteignant un certain seuil de puissance, l'empire constitue un point à atteindre intemporel, une sorte de tentation démiurgique. Le concept d'empire n'est jamais désuet, Il s'agit uniquement des modalités pratiques de son existence qui évoluent en fonctions de multiples critères propres à chaque époque. Aux XXIe siècle et suivants, prenant acte de l'existence et du rôle croissant du continent numérique comme territoire innervant tous les autres (maritime, terrestre, aérien, spatial), il n'est pas déraisonnable de penser que les empires seront numériques ou ne seront pas. Pour reprendre la sémantique de David Todd et Joseph Felix dans leur ouvrage *Un empire de velours*, cet empire pourrait être caractérisé par sa dimension « formelle » dans le cyberespace, au service de sa dimension « informelle » dans les autres espaces. Selon les auteurs, cet impérialisme dit « informel » repose sur l'influence économique, culturelle et diplomatique, tandis que l'impérialisme « formel » repose sur la domination territoriale directe.

---

[122] Camille Auchère. « Marseille, plaque tournante du trafic Internet entre l'Afrique et le reste du monde », Futura, 17 mai 2024. https://www.futura-sciences.com/tech/actualites/internet-marseille-plaque-tournante-trafic-internet-afrique-reste-monde-113484/.

[123] Aurélie Lebelle. « « Un marché multiplié par deux en trois ans » : les câbles sous-marins, un business fructueux pour la France », *Le parisien*, 18 janvier 2025, sect. /economie/business/. https://www.leparisien.fr/economie/business/un-marche-multiplie-par-deux-en-trois-ans-les-cables-sous-marins-un-business-fructueux-pour-la-france-18-01-2025-QY7LYRL5KBEOZGTOJSAX7W2PCQ.php.

[124] Philippe Leroy. « Luc Julia : « Les français sont les meilleurs du monde dans l'IA » », *Silicon*, 7 février 2025. https://www.silicon.fr/Thematique/data-ia-1372/Breves/luc-julia-francais-meilleurs-monde-l-ia-467477.htm.

[125] Margaux Vulliet. « Comment les Français sont devenus les rois de l'IA... dans la Silicon Valley », BFMTV, 16 avril 2023. https://www.bfmtv.com/tech/intelligence-artificielle/comment-les-francais-sont-devenus-les-rois-de-l-ia-dans-la-silicon-valley_AV-202304160025.html.

Or la domination territoriale directe dans le cyberespace reviendra à celui qui y maîtrisera les infrastructures numériques (*hardware, OS, software, data*), les flux de données et la production de normes de référence.

En résumé, appliquée à la France contemporaine, sa stratégie totale ne pourra se réaliser si une certaine liberté d'action ne lui est pas garantie dans le cyberespace. Pour devenir une cyber-puissance formelle, respectée et résiliente, et ainsi défendre ses intérêts stratégiques en continuant de compter parmi le concert des grandes nations, la France doit donc améliorer sa souveraineté dans le cyberespace. Or celle-ci ne pourra être atteinte qu'en « *associant une commande publique exemplaire, un financement renforcé et une structuration industrielle forte, tout en s'appuyant sur une stratégie européenne cohérente et ambitieuse*[126] ».

La vision et le positionnement singulier, à la fois de l'état français mais également des entreprises françaises, représente ainsi le troisième pilier de la recherche de puissance. Il sera en conséquence le troisième axe de notre modèle de maturité. Nous expliciterons en détail ce concept et nous proposerons une définition détaillée de différents niveaux en partant du niveau **Dépendant et Contraint** jusqu'au niveau **Autonome et Référent**.

Après avoir précisément étudié le rôle de l'Etat dans cette vision de cyber-puissance formelle (appuyé par la vision de l'intelligence économique), nous allons étudier en quoi consiste plus précisément, et plus concrètement, cette gouvernance rénovée et mixte de la cybersécurité pour les entreprises.

[126] « Manifeste souveraineté technologique l'autonomie stratégique »., p.120

IV. Une Gouvernance rénovée et mixte de la cybersécurité

Face à l'ampleur croissante des menaces numériques et à l'imbrication des systèmes d'information dans les chaînes de valeur, la cybersécurité ne peut plus être pensée de manière cloisonnée. Elle doit désormais s'inscrire dans une approche de **gouvernance élargie, intégrée à la stratégie globale de l'organisation**. Cette gouvernance rénovée repose sur une hybridation des logiques : économique, industrielle, réglementaire, technologique et informationnelle. Elle implique une responsabilisation accrue des dirigeants, une intégration transversale des enjeux cyber dans les processus métiers, ainsi qu'une coordination fine avec les partenaires de l'écosystème.

Ce paradigme renouvelé s'incarne dans des pratiques combinant **intelligence économique**, **gestion des risques**, **évaluation de la maturité organisationnelle et pilotage orienté performance**. Cette partie explore donc les différents leviers permettant d'ancrer durablement la cybersécurité dans la gouvernance stratégique des entreprises.

IV.1 Apports de l'Intelligence Economique et de la gestion des risques

Dans un contexte de menaces cybernétiques en constante évolution et de concurrence économique intense, les entreprises doivent intégrer l'intelligence économique (IE) dans leur gouvernance de cybersécurité pour renforcer leur résilience. IE et cybersécurité forment un duo stratégique concourant à la réalisation du principe de sûreté cher à tous les stratèges : l'IE assure une veille stratégique (collecte et analyse d'informations sur l'environnement concurrentiel et les menaces), tandis que la cybersécurité protège les actifs informationnels contre les cyberattaques et l'espionnage industriel. L'objectif de cette synthèse est de montrer, de manière stratégique et opérationnelle, comment l'IE peut apporter une valeur ajoutée à la cybersécurité au sein de la gouvernance, à travers quatre services clés de l'entreprise : ressources humaines, juridique, communication, financière, gestion des risques.

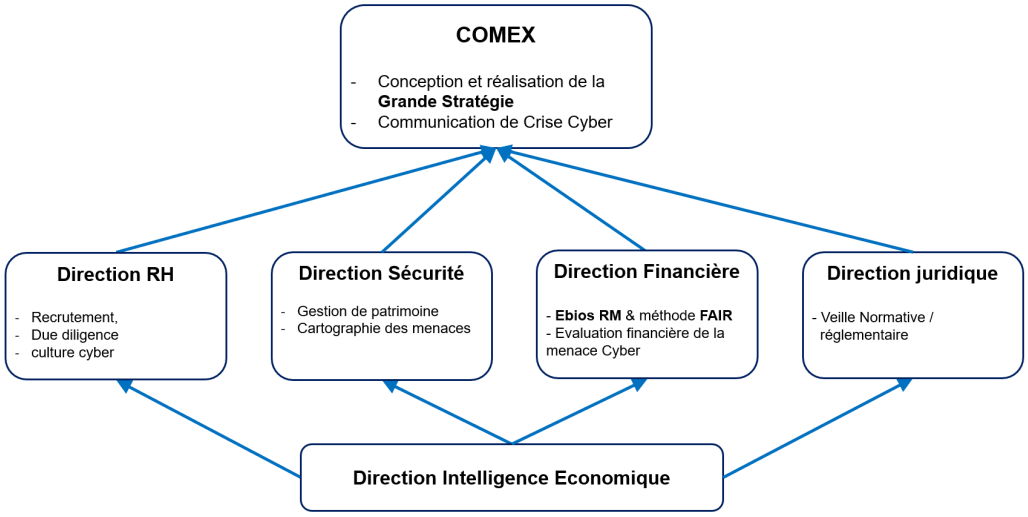


Figure 17 - les apports de l'IE au service de la Grande Stratégie

Pour chaque domaine, nous détaillons les enjeux spécifiques de cybersécurité, les apports de l'IE, des exemples concrets d'actions ou bénéfices, ainsi que les limites ou contraintes de mise en œuvre. Cette approche permettra aux décideurs de comprendre comment une démarche d'intelligence économique bien articulée peut anticiper les menaces, protéger les actifs stratégiques et améliorer la gouvernance de la sécurité numérique de l'entreprise.

IV.1.1 Direction des Ressources humaines : du recrutement à la culture cyber

L'être humain représente l'une des premières protections pour la cybersécurité, et l'intelligence économique peut apporter une valeur ajoutée significative aux ressources humaines sous plusieurs aspects. *« l'IE permet aux organisations de gérer plus efficacement leurs talents, d'anticiper les tendances du marché du travail et de se protéger contre les menaces internes et externes* »[127]

Recruter les bons profils

L'Intelligence Économique révolutionne le processus de recrutement en permettant une veille RH stratégique pour identifier et attirer les talents cyber les plus qualifiés. Grâce aux techniques d'OSINT, les recruteurs peuvent analyser les profils techniques sur les réseaux sociaux professionnels, les contributions sur GitHub, ou encore les participations dans des forums spécialisés en cybersécurité. Cette approche proactive permet de détecter les experts avant même qu'ils ne soient en recherche active d'emploi. L'IE offre ainsi une longueur d'avance dans un marché de l'emploi cyber particulièrement concurrentiel où les compétences techniques rares sont disputées.

***Due diligence* & analyse comportementale**

L'intelligence économique renforce considérablement les processus de vérification et d'évaluation des candidats en croisant de multiples sources de données pour identifier les signaux faibles ou les comportements potentiellement à risque. Un service d'IE permet d'évaluer l'intégrité des candidats en recoupant leurs déclarations avec les informations disponibles en sources ouvertes. Cette démarche préventive contribue à sécuriser l'organisation dès l'étape du recrutement en évitant l'intégration de profils présentant des risques de sécurité interne. Cette approche permet de détecter d'éventuels future *insiders* à travers des techniques de *profiling*, l'analyse des antécédents professionnels et personnels, positionnant donc l'entreprise dans une action proactive face au risque de fuite ou de vol d'information.

Lutter contre le débauchage

Elle peut jouer un rôle crucial dans l'anticipation et la prévention des campagnes de débauchage orchestrées par la concurrence, particulièrement dans les secteurs stratégiques où les compétences cyber sont critiques. En surveillant les mouvements du marché, les stratégies RH des concurrents et les signaux précurseurs de campagnes de recrutement ciblées, l'IE permet aux organisations de prendre des mesures proactives pour retenir leurs

[127] Jonathan Chaste. « L'Intelligence économique au cœur des ressources humaines : une approche offensive », Portail de l'IE, 22 juillet 2024. https://www.portail-ie.fr/univers/business-development-innovation-et-start-up/2024/lintelligence-economique-au-coeur-des-ressources-humaines-une-approche-offensive/.

talents clés. Cette veille concurrentielle inclut l'analyse des offres d'emploi, le *monitoring* des réseaux professionnels et la détection des approches directes visant les collaborateurs sensibles. L'anticipation de ces menaces permet de mettre en place des stratégies de rétention adaptées et de protéger les actifs humains stratégiques de l'entreprise.

Sensibilisation

L'intelligence économique enrichit significativement les programmes de sensibilisation à la cybersécurité et en facilite la diffusion en apportant le bon contenu à la bonne personne. L'IE contribue ainsi à développer une **véritable culture cyber** au sein de l'organisation, transformant chaque employé en acteur conscient et responsable de la sécurité informatique.

IV.1.2 Direction de la sécurité et gestion des écosystèmes étendu

Dans un contexte où les outils et les chaînes d'approvisionnement se complexifient constamment, la **cartographie de l'écosystème** étendu devient cruciale pour une gestion efficace des risques. L'intelligence économique (IE) offre des méthodes et outils permettant aux RSSI d'appréhender cette complexité croissante et d'adopter une **posture proactive** face aux menaces.

Un retard préoccupant dans la gestion du patrimoine informationnel

Le baromètre 2022 du CESIN révèle une lacune majeure dans la maturité des entreprises françaises concernant la gestion de leur patrimoine informationnel. En effet, *« 40% des RSSI déclarent n'avoir entrepris aucune action concernant le processus de gestion du patrimoine informationnel »*[128], révélant un angle mort critique dans les stratégies de cybersécurité. Cette situation est d'autant plus préoccupante que le patrimoine informationnel constitue souvent la cible privilégiée des attaquants, qui recherchent des informations stratégiques telles que la propriété intellectuelle[129] . L'absence de cartographie et de protection de ces actifs immatériels expose les organisations à des risques de cyber-espionnage et de vol de données critiques : *«11,2 % des incidents motivés par le cyber espionnage »* [130].

Cartographie du patrimoine informationnel et des dépendances critiques

La méthode d'intelligence économique permet d'analyser l'ensemble de l'écosystème organisationnel, incluant fournisseurs, sous-traitants et partenaires, pour identifier les dépendances critiques. Cette approche systémique aide les RSSI dans la cartographie complète de leur environnement, permettant de déterminer tous les biens informationnels et leurs interdépendances. L'apport de cette méthodologie réside dans l'amélioration de l'efficacité opérationnelle et la réduction des angles morts traditionnels de la sécurité. Cette approche proactive s'avère particulièrement pertinente face aux risques juridiques liés à la législation européenne, notamment le RGPD et la directive NIS 2, qui imposent une responsabilité étendue sur la chaîne de valeur.

---

[128] « Les instantanés 2022 » (CESIN, 2022). https://cesin.fr/document.php?d=64a586188565c.

[129] Albane Girollet. « Protection du patrimoine informationnel : regard sur le cyber-espionnage », *Almond*, 13 décembre 2022. https://almond.eu/cybersecurity-insights/protection-du-patrimoine-informationnel-regard-sur-le-cyber-espionnage/.

[130] « Cyber Espionage » (ENISA, 2020). https://www.enisa.europa.eu/sites/default/files/all_files/ETL2020%20-%20Cyber%20Espionage%20A4.pdf.

L'enjeu des tiers dans l'écosystème de sécurité

Guillaume Poupard, directeur général de l'ANSSI, soulignait en 2019 cette problématique en déclarant : *"Si les entreprises ont appris au fil des années à protéger leur SI, qu'en est-il des tiers ?"* Cette interrogation met en lumière la nécessité d'étendre le périmètre de sécurité au-delà des frontières traditionnelles de l'organisation. Les fournisseurs, sous-traitants et partenaires constituent autant de vecteurs d'attaque potentiels qui peuvent compromettre la sécurité globale du système d'information. La multiplication des interconnexions et des échanges de données avec l'écosystème étendu crée de nouveaux défis sécuritaires qui nécessitent une approche holistique de la gestion des risques.

Intégration de l'IE dans la *cyber threat intelligence*

La *cyber threat intelligence* (CTI) devient un outil indispensable pour anticiper les menaces et donner une posture proactive à la cybersécurité, mais peut parfois se limiter à des aspects trop techniques, créant des lacunes dans l'analyse globale des risques. L'intégration de IE dans les processus de CTI permet de diminuer les angles morts en croisant des sources d'information contextuelles et stratégiques. Cette approche enrichit l'analyse traditionnelle des indicateurs de compromission (IOC) en apportant une dimension géopolitique et économique aux menaces identifiées. La combinaison de ces deux disciplines offre une vision plus complète du paysage des menaces, permettant aux organisations d'adapter leurs stratégies défensives en fonction du contexte stratégique et concurrentiel de leur secteur d'activité.

IV.1.3 Fonction financière : rationalisation et pilotage stratégique

La cybersécurité s'impose aujourd'hui comme un enjeu stratégique majeur. Si la place du RSSI au sein du COMEX se renforce, il demeure néanmoins difficile d'obtenir un budget réellement aligné sur la montée en puissance des menaces.

Dans ce contexte, l'intelligence économique (IE) joue un rôle clé en facilitant la collaboration entre les différents services de l'entreprise. En croisant des méthodologies issues de la gestion des risques et de la veille stratégique, l'IE permet de mieux objectiver les risques immatériels — qu'ils soient financiers, juridiques, réputationnels ou géopolitiques. Elle contribue ainsi à une évaluation plus fine des besoins en cybersécurité, notamment en matière d'assurance.

Parmi les outils mobilisables, la méthode **FAIR** (Factor Analysis of Information Risk) se distingue en traduisant les risques cyber en valeurs financières concrètes. Elle permet, par exemple, d'estimer les pertes potentielles liées à une attaque par rançongiciel et de les comparer aux coûts de mitigation ou à une prime d'assurance. Cette approche facilite un dialogue chiffré et structuré entre le RSSI et la direction financière, et aide à justifier les investissements en cybersécurité sur des bases objectives. Cette approche fait évoluer l'analyse de la cybersécurité, qui passe d'une évaluation qualitative (repose sur des évaluations non numériques) à une mesure plus quantitative (utilise des données pour estimer la fréquence d'occurrence) plus précise pour chiffrée les risques financiers [131].

[131] Taylor Maze. « Qualitative vs. Quantitative Analysis for Cyber Risk: What's the Difference? », *FAIR institute*, 29 octobre 2018. https://www.fairinstitute.org/blog/qualitative-vs.-quantitative-analysis-for-cyber-risk-whats-the-difference.

Un exemple marquant de cette approche se trouve dans l'entreprise C-RISK avec la possibilité de combiner la méthode **EBIOS RM** et **FAIR** qui fait le lien parfait entre la cybersécurité et le financier dans un seul objectif être un vecteur de création de valeur.

Enfin, la mise en place d'indicateurs clés de performance (KPI) pertinents, autour d'un retour sur investissement de la sécurité (ROSI), aligne les dépenses cyber avec des objectifs *business* concrets. La veille concurrentielle et le benchmark des investissements cyber complètent cette démarche, aidant la fonction financière à optimiser chaque euro dépensé pour réduire les risques de façon mesurable.

IV.1.4 Communication et gestion de crise : la réactivité par IE

La veille réputationnelle permet de surveiller en continu les réseaux sociaux, forums, avis clients et presse en ligne afin d'identifier les signaux faibles, alertes potentielles ou critiques émergentes. Cette approche proactive anticipe les atteintes à la réputation pour pouvoir agir avant qu'elles ne s'amplifient. Disposant ainsi d'informations fiables pour mieux gérer sa communication avec ces parties prenantes.

Réseau d'alerte rapide

L'intelligence économique intègre la collecte continue d'informations, leur recoupement et une diffusion interne fluide pour une réaction rapide face à une crise. Un système interne bien structuré permet de partager en temps réel des données pertinentes. Ce partage transverse entre services assure une vision unifiée et cohérente aux équipes métier.

Informations utiles pour les crises

Cette réactivité informationnelle facilite des choix éclairés et une communication adaptée avec les parties prenantes. Le recoupement d'informations provenant de sources multiples (interne, externe et technique) améliore la prise de décision.

IV.1.5 Service juridique : conformité augmentée par l'IE

Dans un contexte marqué par la prolifération des normes et la fragmentation réglementaire à l'échelle mondiale, le service juridique joue un rôle stratégique dans la gouvernance de la cybersécurité. Selon le Forum Économique Mondial, « plus de 76 % des RSSI estiment que la fragmentation des règles entre juridictions complique fortement la capacité de leur organisation à rester conforme » [132].

L'intelligence économique vient renforcer les capacités du service juridique à travers une veille normative et réglementaire renforcée. Celle-ci ne se limite pas à un simple suivi des textes (RGPD, DORA, NIS2, … ou encore des lois extraterritoriales comme le Cloud Act), mais intègre également une analyse stratégique des impacts juridiques sur l'organisation. Il s'agit d'anticiper les évolutions du paysage légal, d'adapter les dispositifs internes, et de prévenir les risques de non-conformité.

Ainsi outillé, le service juridique devient un acteur agile et proactif, capable d'assurer une lecture fine des obligations légales tout en s'inscrivant dans une dynamique d'anticipation. L'IE agit ici comme catalyseur d'adaptation et de réactivité face à un environnement normatif

[132] « WEF Global Cybersecurity Outlook 2025 ».

en constante mutation, permettant à l'entreprise de réduire ses risques juridiques, donc d'accroître sa liberté d'action.

Différenciation concurrentielle

La sécurité devient un avantage compétitif lors des appels d'offres, dans la relation clients-fournisseurs et pour l'attractivité des investisseurs, ancrant la gouvernance cyber dans les leviers de performance organisationnelle.

La cybersécurité ne peut plus être confinée à la DSI. En impliquant chaque service clé dans une logique proactive, l'intelligence économique rend la gouvernance cyber plus agile, anticipative et intégrée. Elle en fait un levier de résilience collective et d'avantage stratégique durable.

IV.1.6 L'organisation et l'affectation des moyens, le quatrième pilier

Cette rénovation de Gouvernance montre clairement l'influence transversale de l'intelligence économique qui irrigue toute l'entreprise et impact à la fois l'organisation et l'affectations des moyens de l'entreprise.

C'est pourquoi le niveau d'organisation et d'affectation des moyens en intelligence économique mais également en cybersécurité représente donc le quatrième pilier de notre démonstration.

Ce sera le quatrième et dernier axe de notre modèle de maturité de la Cybersécurité Stratégique ou de la Recherche de Puissance, du niveau **Organisation non dédiée** jusqu'au niveau **Organisation intégrée**.

IV.2 Modèle de maturité et pilotage de la performance de l'entreprise

L'utilisation de modèles de maturité permet de suivre et gérer l'amélioration de la performance d'un système donné.

Dans notre cas, il doit permettre de suivre la performance globale de la gouvernance de la cybersécurité ainsi que la mise en place et l'amélioration de l'efficacité et efficience des activités de cybersécurité.

Les mécanismes d'**Amélioration Continue** liées à la roue de Déming (PDCA, Plan Do Check Act ou Planifier Déployer Contrôler Améliorer) sont clés dans les modèles de maturité.

Figure 18 - La roue de Deming - PDCA

IV.2.1 Rappel sur le CMMI ou Capability Maturity Model Integration

« CMMI a été créé à l'origine par le département de la défense US (DoD) pour assurer le suivi des développements et des budgets sous l'appellation CMM (Capability Maturity Model). Par la suite, en absorbant d'autres spécifications relatives, le référentiel s'est adjoint la lettre I pour Intégration. CMMI a pour finalité essentielle de mesurer la capacité des projets à s'achever correctement en termes de délais, de fonctionnalités et de budget.[133] »

Il est important de noter que ce modèle développé par le Software engineering institute (SEI) en réponse à la demande du DoD concernait initialement le génie logiciel. Le SEI a fait plusieurs fois évoluer son modèle en englobant des bonnes pratiques d'autres modèles.

En 2011 sort la dernière version à date du modèle, il s'agit de la version 1.3.

Sans vouloir chercher à « coller » dans le détail au modèle, nous avons pris l'option de nous inspirer des idées fondatrices de ce modèle, qui passe pour être le « père » de la majorité des modèles de maturité.

[133] Alain Fernandez. « Qu est-ce que CMMI ? Le modèle de maturité pour la gouvernance du SI Capability Maturity Model Integration », *Management et Performance, piloter.org*, 22 septembre 2017. https://www.piloter.org/gouvernance/CMMI_gouvernance_SI.htm.

IV.2.2 Les 5 niveaux du CMMI

Les niveaux du CMMI sont les suivants :

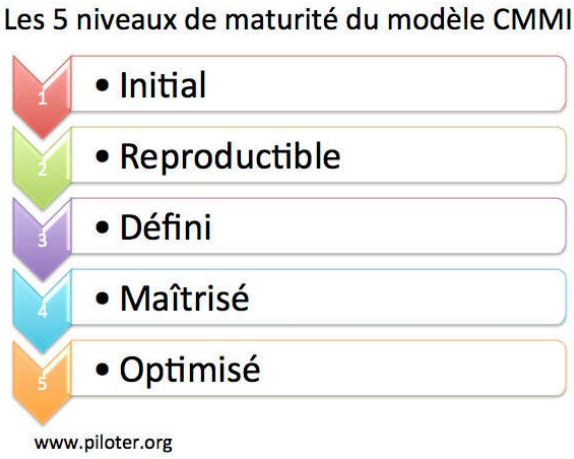


Figure 19 - Les 5 niveaux de maturité du modèle CMMI
Source : https://www.piloter.org/gouvernance/CMMI_gouvernance_SI.htm

Suivant les différentes traductions du modèle en français, le niveau 2 peut être appelé « Géré » et le niveau 4 peut être appelé « gestion quantitative », nous proposons également le terme « Mesuré ».

En conséquence, voilà une description succincte des niveaux que nous retenons :

Tableau 2 : CMMI, le Modèle de maturité de référence

Niveau	Description du niveau
1 - Initial	Au niveau 1, les organisations ont des processus imprévisibles qui sont mal contrôlés, mal définis et souvent **réactifs**.
2 - Géré	Au niveau 2, les organisations commencent à mettre en œuvre des pratiques de gestion de projet de base, en se concentrant sur les processus disciplinaires de base pour atteindre les objectifs de coût, de calendrier et fonctionnels.
3 - Défini	Au niveau 3, les **processus sont documentés** et **standardisés** dans **toute l'organisation** pour garantir la cohérence pendant les périodes difficiles.
4 - Mesuré	Au niveau 4, les organisations mettent l'accent sur **la prise de décision** basée sur les **objectifs mesurables** pour prédire le coût, la qualité et le calendrier d'un produit logiciel.
5 - Optimisé	Au niveau 5, les organisations s'efforcent **continuellement d'améliorer leurs processus** par des améliorations techniques et managériales progressives et innovantes. (PDCA) Les retours d'expérience des projets actuels et passés permettent d'affiner et d'améliorer en permanence les normes et les processus de l'organisation.

IV.2.3 Un Modèle de maturité multiaxe afin d'évaluer la Cybersécurité Stratégique

Les différents processus évoqués dans le modèle CMMI sont regroupés au sein de quatre catégories :

- **Gestion de projet** (activités quotidiennes de gestion de projet)
- **Ingénierie** (activités liées à la conception et la réalisation d'applications informatiques)
- **Support** (activités support aidant la gestion de projet)
- **Gestion des processus** (activités de l'organisation pour favoriser le déroulement de ses projets).

D'une manière analogue, nous pensons que la maturité en **cybersécurité** est fonction des plusieurs **axes spécifiques et complémentaires** de l'entreprise.

Ainsi, nous présentons dans le chapitre suivant notre propre modèle de maturité de Cybersécurité Stratégique et nous détaillons les axes - et leur niveaux - permettant le calcul d'un **Cyber Score Stratégique**.

IV.2.4 Pilotage de la performance de l'entreprise

Il va de soi que la notion même de modèle de maturité intègre intrinsèquement la notion de performance de l'entreprise.

Ainsi, Lord William Thomson KELVIN (1824 - 1907) affirmait déjà au XIXème siècle : « *Si vous ne pouvez pas le mesurer, vous ne pouvez pas l'améliorer.* » Cette phrase est reprise par Edwards DEMING (MIT, 1900 - 1993), et elle est depuis utilisée pour tout ce qui concerne l'**amélioration continue des processus**.

Le but d'un modèle de maturité est donc bien d'objectiver et mesurer un niveau, une maturité dans l'optique ultérieure de faire progresser l'entreprise.

Pour conclure, la mise en œuvre d'une gouvernance mixte et rénovée de la cybersécurité constitue une réponse pragmatique aux défis systémiques auxquels sont confrontées les organisations. Le recours à l'intelligence économique, la gestion du risque de Cybersécurité au sens large et l'adoption de modèles de maturité structurants permettent de transformer la cybersécurité en levier de compétitivité, de résilience et d'innovation.

Ce **changement de posture** appelle une transformation en profondeur des modes de pilotage, où la cybersécurité n'est plus une contrainte, mais un **facteur clé de performance** durable. En articulant rigueur méthodologique et vision stratégique, les organisations peuvent ainsi bâtir une gouvernance cyber robuste, adaptée à la complexité du monde numérique contemporain.

V. Modèle de maturité opérationnel d'une cybersécurité stratégique

L'objectif de cette partie est, en se nourrissant des parties précédentes, de proposer une approche opérationnelle pour faire monter en performance la cybersécurité de l'entreprise, pour la rendre plus efficace et idéalement, plus efficiente. Pour aider la stratégie de cybersécurité à mieux réaliser le principe de sûreté au service de la liberté d'action en ne créant pas de dépendances préjudiciables.

Pour ce faire, et comme annoncé dans le paragraphe IV.4, nous proposons un modèle de maturité de la **cybersécurité stratégique** à destination des organisations. Le but de ce modèle de maturité opérationnel, dans la droite ligne des parties précédentes, est de dépasser une approche de cybersécurité « technico-financière » pour aller vers une **cybersécurité stratégique**, et à terme atteindre la **cyber-puissance**.

La démarche proposée est la suivante :

- Présentation détaillée du modèle de maturité (les 4 axes individuels, la notion de Cybersécurité Stratégique et le calcul du Cyber Score Stratégique)
- Evaluation du panel d'entreprises pour tester le modèle
- Plan de montée en maturité et démarche d'amélioration continue de la Cybersécurité Stratégique

Pour finir nous verrons que les projets permettant la montée en maturité doivent s'intégrer dans la gouvernance globale de la cybersécurité et des transformations.

V.1 Un modèle mixte multiaxes / multivariables

Le modèle proposé s'appuie sur **plusieurs** axes de réflexions et nous proposons d'évaluer le niveau de l'entreprise par rapport à ces différents axes sur une échelle de 1 à 5, conformément à la grande majorité des modèles de maturité inspirés du CMMI.

Nous avons identifié les axes ou variables suivantes :

- **Cybersécurité Technique** (présentée dans la partie **II**)
- **Intelligence Économique** (présentée dans la partie **II**)
- **Positionnement** de l'entreprise (présentée dans la partie **III**)
- **Organisation & Moyens** (affectations IE et Cyber) (présentée dans la partie **IV**)

Conformément aux premières parties, nous pensons que l'**Intelligence Economique** est nécessairement une composante de la Cybersécurité Stratégique.

Enfin la recherche de **Positionnement** de l'entreprise doit obligatoirement être pris en compte pour le calcul de la Cybersécurité Stratégique

Nous avons fait le choix de faire de l'**Organisation et des Moyens** - de la **Cybersécurité** et de l'**Intelligence Economique** - un axe à part parce que cela nous donnait plus de latitude par la suite.

C'est la raison pour laquelle, et conformément aux premières parties, le niveau de **Cybersécurité Stratégique** est fonction du niveau de **Cybersécurité technico-financière**, d'**Intelligence Économique**, de **Positionnement** et enfin d'**Organisation & Moyens** de l'entreprise.

Le calcul de la Cybersécurité Stratégique peut donc finalement se ramener à la formule suivante :

$$Y_{CS} = f(x_{CT}, x_{IE}, x_{OM}, x_{AP})$$

Nous partons du **postulat** que ces quatre axes sont globalement **indépendants** les uns des autres. Cela revient à dire qu'une activité spécifique est traitée globalement dans un axe et un seul.

Dans le même temps, ce choix est motivé par le fait que chaque axe pourrait être porté par une personne différente : le responsable de la **Cybersécurité**, le responsable de l'**Intelligence Economique**, le **Directeur Financier** par exemple ou le **Directeur Opérationnel** et finalement le **DG** ou le **Comex**.

Limites de notre modèle

L'indépendance des axes n'est, sans doute, pas totale mais cela nous semblait une bonne approximation.

Néanmoins, une meilleure "**Cybersécurité Technique**" peut être influencée par des investissements permis par une "**Organisation & Moyens**" plus mature, tandis que "l'**Intelligence Économique**" peut éclairer les décisions concernant le "**Positionnement**" et vice & versa. Ainsi un score élevé en **Positionnement** pourrait entrainer un score plus élevé en **Organisation & Moyens** qui pourrait également entrainer des scores plus élevés en **CT** et/ou **IE**.

Dans le modèle qui suit nous avons cherché à illustrer et détailler notre propos mais ce modèle bien qu'opérationnel n'a pas l'ambition d'être exhaustif et ce globalement par manque de temps.

En particulier, le détail des différentes activités mériterait sans doute d'être approfondi et le sera ultérieurement.

En général, ce type de modèle doit être est complété par des questionnaires permettant une évaluation objective du niveau de chacun des axes.

De même, ce modèle a été testé de manière assez légère et il mériterait une série de test en situation réelle afin de le valider complètement.

V.1.1 Axe Cybersécurité Technique

Afin de proposer les termes des niveaux de Cybersécurité Technique, nous nous sommes appuyés sur un schéma tiré de l'ANSSI qui se trouve page 14 : « Structurer ses mesures de sécurité » : Gouvernance, Protection, Défense et Résilience

Cette variable a pour objectif de modéliser les différents niveaux de Cybersécurité Technique :

- Au niveau **1-Initial**, nous parlerons de **Cyber Réactivité**. La stratégie en manière de cybersécurité n'est ni formalisée ni homogène.
- Au niveau **5-Optimisée**, l'entreprise est devenue **Cyber Résiliente**.

Tableau 3 : Axe Cybersécurité Technique

N	Cybersécurité Technique	Description
1	Survivre **Cyber Réactivité**	L'organisation ne possède aucune stratégie de cybersécurité formalisée, agit de façon totalement réactive, et la sécurité dépend de l'expertise individuelle. **Exemple** : Des sensibilisations à la Cybersécurité peuvent être mises à disposition des collaborateurs qui le souhaitent/demandent.
2	Anticiper et prévenir **Cyber Gouvernance**	La gouvernance du risque numérique a pour objectifs d'anticiper la menace, de suivre le niveau de sécurité et de renforcer en continu un dispositif adapté. Elle s'inscrit dans une **démarche continue**. Exemple : une **première organisation** est en place avec des processus et des procédures simples (sauvegarde, mot de passe)
3	Apprendre, se protéger **Cyber Protection**	Des mesures ou actions de **protection** standardisées permettent de se **prémunir** contre les attaques en rendant le SI et son écosystème les **moins vulnérables** et **exposés** possibles. (Réduction de la surface d'attaque) Ex : Politiques formalisés, Rôles et responsabilités clairs, étude de la Norme **ISO 27001**, audits internes etc.
4	Se défendre **Cyber Défense**	La cyber défense répond à la nécessité d'orienter la détection des incidents numériques afin d'**anticiper** et **optimiser** la réponse d'une organisation. Il s'agit de concevoir et formaliser une capacité de supervision de la sécurité (**SOC**) qui s'intégrer avec un dispositif de **CSIRT/CERT** pour structurer la chaine de réponse aux incidents de sécurité, de la détection à la remédiation. Ex : Tableaux de Bord de sécurité, métriques de conformité, tests réguliers etc.
5	Se relever plus fort **Cyber Résilience**	Ce volet concerne la **continuité** d'activité avec un niveau de dégradation tolérable en cas de **crise**, puis la reprise nominale progressive pour minimiser les impacts stratégiques et métiers. La culture de la cybersécurité irrigue l'entreprise et s'intègre dans chaque projet et décision. L'organisation utilise des indicateurs de mesure de l'efficacité de sa cybersécurité, afin anticiper les risques et les menaces, améliorer continuellement ses pratiques et devenir encore **plus résiliente**. Ex : détection de menaces, incidents et crises : Rapport **BIA**, **CTI**, **PCA** et **PRA**. Optimisation du SMSI, programme de certification ISO 27001, EBIOS RM etc.

V.1.2 Axe Intelligence Économique

Cette variable a pour objectif de modéliser les différents niveaux de connaissances / compétences d'une organisation en matière d'**intelligence économique**.

- Au niveau **1-Initial**, l'Intelligence Économique est **Réactive**.
- Au niveau **5-Optimisée**, l'Intelligence Économique devient **Influente** ou **Prospective** pour permettre l'anticipation

Le tableau suivant détaille les différents niveaux de cette variable

Tableau 4 : Axe Intelligence Économique

N	Intelligence Économique	Description
1	**IE Réactive** et non structurée	L'IE est inexistante et pas organisée, certaines personnes font de l'IE sans le savoir. **Veille** uniquement **opportuniste** et peu structurée.
2	**IE Émergente** « intuitu personae »	**Veille** grâce à **l'IE ponctuelle** et **localisée** à un petit département, en réponse à des besoins immédiats, souvent par intuition ou par opportunisme. C'est globalement le fait d'individualités qui commencent à structurer une démarche et **conçoivent les premiers processus** d'intelligence économique pour le besoin spécifique du département. Prise de **conscience de l'état de guerre économique** par ces individualités.
3	**IE Informative** et structurée	Les processus d'IE se formalisent et se généralisent au niveau d'une BU au minimum. Cela suppose une compréhension plus générale du besoin et des apports globaux de l'intelligence économique afin d'**informer** et **dévoiler** le contexte réel de l'entreprise Les différentes activités d'Intelligence Economique se structurent au sein de l'entreprise.
4	**IE Protectrice** (mesurable)	L'intelligence économique est pleinement intégrée à la **grande stratégie de l'entreprise** qui se traduit en **actions mesurables**, faisant intervenir activement les parties prenantes internes et externes à travers des mécanismes collaboratifs pour **protéger l'entreprise**. Exemple : Le Comex s'appuie **régulièrement** sur les travaux de l'IE pour définir la **stratégie totale** de l'entreprise.
5	**IE Influente** et Prospective	L'IE éclaire et donne le sens global, elle sert de **phare** et de **boussole** à l'entreprise. L'organisation utilise systématiquement l'intelligence économique comme levier stratégique d'anticipation, d'innovation et d'**influence active** sur son environnement concurrentiel et institutionnel, avec des processus dynamiques et adaptatifs qui sont régulièrement revus et repensés pour les optimiser.

V.1.3 Axe Autonomie et Positionnement de l'entreprise

Cette variable a pour objectif de modéliser le **positionnement de l'entreprise** au sein de son écosystème.

- Au niveau **1-Initial**, l'entreprise est **dépendante** des contraintes qui pèsent sur elle. Elle reste globalement **isolée**
- Au niveau **5-Optimisée**, l'entreprise est **Souveraine**, elle participe largement aux règles de son secteur

Tableau 5 : Axe Autonomie & Positionnement

N	Positionnement	Description
1	Entreprise **dépendante et contrainte**	L'organisation fonctionne de manière **isolée**, sans prise en compte des interactions avec son écosystème ni anticipation des influences externes qu'elle subit souvent sans en avoir conscience. Elle est **contrainte**. Aveuglement ou naïveté, « Tout ça ne me concerne pas »
2	Entreprise **Lucide et Éveillée**	Prise de conscience de la **guerre économique** et des impacts de l'environnement. L'entreprise s'éveille et prend **conscience** qu'il faut surveiller et tenir compte de son l'écosystème, même si la veille est souvent réduite à un petit département.
3	**Consciente des rapports de force**	L'entreprise interagit de façon régulière et structurée avec son écosystème, elle prend en compte les influences et **interdépendances géopolitiques** dans ses décision stratégique. Elle s'affirme comme un acteur de son **écosystème**. Le **juridique** au sein de l'entreprise devient **clé** en particulier pour comprendre l'écosystème cyber et, entre autres, les règles d'extra-territorialité et les **rapports de force**. Stratégie du faible au fort.
4	**Marge de Manœuvre** En recherche de liberté d'action	L'entreprise établit des **partenariats stratégiques** solides et collabore avec son écosystème, facilitant une liberté d'action accrue et maîtrisée Le **Comex** recherche une autonomie, des **marges de manœuvre**, permettant d'atteindre une liberté d'action stratégique pour l'entreprise. Ainsi il demande **explicitement** à la cybersécurité de faire ce qu'il faut pour s'affranchir des contraintes externes (techniques, juridiques etc.).
5	Entreprise **Autonome et Référente** Leader innovant et influent	L'entreprise **pilote et influence** son écosystème global pour maximiser sa liberté d'action et sa souveraineté. Elle maîtrise globalement la géopolitique de sa sphère d'influence afin d'anticiper et de gérer ses dépendances. Elle contribue à **définir les règles** de son secteur et donc à en définir une **Entreprise Référente**. Stratégie du fort au faible

Le niveau 4 permet la gestion des contraintes externes. En effet à ce niveau-là l'entreprise **dépasse les contraintes et les transforme en opportunités**.

Ainsi les normes telle que **NIS2** ou **DORA** sont vues comme des opportunités afin de se démarquer de ses concurrents.

V.1.4 Axe Organisation & Moyens intégrant hommes et processus

Cette variable a pour objectif de modéliser l'Organisation et les moyens dédiés à la cybersécurité et à l'intelligence économique.

- Au niveau **1-Initial**, l'organisation est **non dédiée** et ne comporte pas de sachants ou d'experts du domaine.
- Au niveau **5-Optimisée**, l'organisation en matière de **Cybersécurité** et d'**Intelligente Economique** est **intégrée** et apprenante.

Tableau 6 : Axe Organisation & Moyens

N	Organisation & Moyens	Description
1	O & M **non dédiées** et de faibles ampleurs	Pas d'organisation **spécifique** pour la cybersécurité ou encore moins pour l'intelligence économique. Pas de sachant ou de spécialiste. **Exemple** : initialement, la cybersécurité fait souvent partie de la DSI. Le responsable informatique est en charge. L'IE est inexistante et incomprise.
2	O & M **externalisée**, en compréhension du sujet	Compréhension que l'organisation n'est pas suffisamment structurée malgré une bonne volonté évidente. Prise de conscience qu'il faut se faire aider. **Externalisation** partielle.
3	Organisation **internalisée**, adaptée et standardisée	Une nouvelle organisation apparait, le Comex fait évoluer la gouvernance et reprend le *lead* sur la cybersécurité. Création d'une direction de la **sécurité** qui centralise la cybersécurité au niveau de l'entreprise. Les processus décisionnels sont établis et les responsabilités sont clairement attribuées au sein de l'organisation.
4	Organisation **pilotée**	L'efficacité de l'organisation est mesurée et pilotée à travers des indicateurs précis. Le Comex valorise les travaux de l'IE et lui donne son organisation propre et **un responsable IE.**
5	Organisation **intégrée et apprenante**	La gouvernance est agile et **proactive**, capable d'anticiper les changements externes et internes, et utilise des **mécanismes d'amélioration continue** basés sur un apprentissage organisationnel systématique. **Exemple :** intégration de l'IE et de la Cyber dans une **structure commune pilotée par le Comex**. **Organisation jointe efficiente**

V.2 La Cybersécurité Stratégique

La Cybersécurité Stratégique peut être vue comme la résultante des 4 axes précédents : **Cybersécurité Technique**, **Intelligence Economique**, **Positionnement** et finalement **Organisations & Moyens**.

V.2.1 Présentation des niveaux des différents axes

Tableau 7 : Récapitulatif des niveaux des différents axes

Niveau	Cybersécurité Technique	Intelligence Economique	Positionnement	Organisation & Moyens	Cybersécurité Stratégique
Initial	**Cyber Réactivité**	**IE Réactive**	**Contrainte**	Organisation **Non dédiées**	**Embryonnaire**
Géré	**Cyber Gouvernance**	**IE Émergente**	**Lucide et Éveillée**	Organisation **Externalisée**	**Émergente**
Défini	**Cyber Protection**	**IE Informative**	**Rapport de Force**	Organisation **Internalisée**	**Apprenante**
Quantifié	**Cyber Défense**	**IE Protectrice**	**Marge de manœuvre**	Organisation **Pilotée**	**Globale**
Optimisé	**Cyber Résilience**	**IE Influente**	**Référent et Autonome**	Organisation **Intégrée**	**Cyber Puissance**

V.2.1.1 Calcul du Cyber Score Stratégique d'une entreprise

Afin de calculer la valeur de la Cybersécurité Stratégique d'une entreprise, la première étape est d'évaluer individuellement les 4 variables :

- **Cybersécurité Technique**
- **Intelligence Économique**
- **Positionnement de l'entreprise**
- **Organisation & Moyens** (autour de l'IE et la Cyber)

La **Cybersécurité Stratégique** est le **barycentre** des 4 variables.

Nous avons pensé initialement utiliser simplement la moyenne. Néanmoins et afin de tenir compte de l'importance de la **Cybersécurité Technique** ainsi que de la **proximité** des trois autres variables, nous proposons de donner un poids de **2** à la **CT** et **1** pour les autres variables.

Dans le cas contraire la note de cybersécurité technique nous semble avoir un impact trop faible.

En conséquence, le calcul de la **Cybersécurité Stratégique** est le suivant :

$$CS = \frac{2xCT + IE + OM + AP}{5}$$

Nous présentons dans le tableau suivant les différents niveaux de la **Cybersécurité Stratégique**.

Tableau 8 : Les niveaux de la Cybersécurité Stratégique

	Cybersécurité Stratégique	Description
1 < CS 1,5	CS **Embryonnaire**	Pas plus de deux variables à 2, le reste à 1. L'entreprise a très peu de maturité que ce soit en cybersécurité, en IE ou en recherche d'autonomie qui n'est pas vu comme une nécessité.
1,5 < CS < 2,3	Cybersécurité **Émergente**	Quelques initiatives de cybersécurité existent, mais elles sont ponctuelles et peu structurées ou lorsque la cybersécurité Technique est plus forte, la prise de conscience de l'état du monde n'est pas encore faite.
2,3 < CS < 3,4	Cybersécurité **Apprenante**	La cybersécurité est en cours d'intégration dans les processus, l'organisation apprend à s'adapter. La volonté de reprendre son destin en main commence à se faire sentir.
3,4 < CS < 4,5	Cybersécurité Stratégique **Globale**	La Cybersécurité est un **pilier** de l'entreprise, à la fois comme ligne de défense mais également dans une approche offensive et d'influence.
>= **4,5**	**Cyber Puissance** Stratégique	Au moins 3 variables à 5 et l'autre est à 4. La cybersécurité est devenue le centre névralgique de l'entreprise et le siège de sa **puissance.**

V.2.1.2 Définition de la Cyber Puissance Stratégique

La **Cyber Puissance** est le niveau le plus élevée de la **Cybersécurité Stratégique**. Pour atteindre ce niveau, chacune des variables des différents axes doit être à 4 ou 5.

Tableau 9 : Libellé des composantes de la cyber puissance

Cyber sécurité Technique	Intelligence Economique	Positionnement	Organisation et Moyens
Cyber Défense	**IE Protectrice**	**Marge de manœuvre**	Organisation **Pilotée**
Cyber Résilience	**IE Influente**	**Référent et Autonome**	Organisation **Intégrée**

Ainsi La **Cybersécurité Technique** est de niveau **Cyber Défense** ou **Cyber Résilience**, l'entreprise fait régulièrement de l'analyse de risque afin d'identifier les menaces, les scénarios et chemins d'attaque et évaluer le risque financier. La Cybersécurité est **efficiente** en **Défense**

L'**Intelligence Economique** est **Protectrice** ou **Influente**, elle permet d'éclairer la situation et d'influencer l'écosystème dans lequel navigue l'Entreprise. La Cybersécurité devient une arme **Offensive**.

L'**Organisation** de l'entreprise est **Pilotée** ou **Intégrée** et la Cybersécurité et l'Intelligence Economique sont vus comme **stratégiques**. Elles ont enfin les moyens de leurs ambitions, en général, à travers une **organisation commune**. La cybersécurité devient **Intégrée**.

Le **Positionnement** de l'entreprise est en recherche de **Marge de manœuvre** ou **Référent**. L'entreprise intègre les risques **systémiques juridiques** et considère que la **souveraineté** et la **liberté d'action** est son objectif. La cybersécurité doit y contribuer en s'appuyant sur des **offres souveraines** : **SecNumCloud** par exemple.

V.2.2 Evaluation du panel d'entreprises pour « tester » le modèle

Afin de faire les premiers tests, nous avons constitué un **panel d'entreprises** fictives. Elles ont été évaluées *via* notre modèle. Une partie de ces évaluations ont été réalisées lors d'entretiens avec des cadres d'entreprises réelles. Les six premières entreprises sont des **Grands Comptes** pouvant faire partie du CAC40.

Les résultats des deux premières entreprises viennent de nos interviews préparatoires, il s'agit donc de **données réelles**, même si le questionnaire a été relativement sommaire.

Les autres résultats sont **fictifs** pour illustrer nos propos. Ce qui explique que le calcul de la **Cybersécurité Stratégique** soit identique - 2,6 - pour les quatre ligne dans une approche pédagogique.

Les résultats sont listés dans le tableau de la page suivante :

Tableau 10 : Évaluation de la Maturité de la CS de notre panel d'entreprise

	Cybersécurité Technique 1	Cybersécurité Technique 2	Intelligence Economique	Organisation	Positionnement	Cybersécurité Stratégique
Cyber	5	5	2	3	3	3,6
Défense	4	4	3	3	4	3,6
ESN	4	4	1	2	2	2,6
Automobile	3	3	2	3	2	2,6
Luxe	2	2	3	2	4	2,6
Santé	3	3	1	4	2	2,6
PME	2	2	1	2	2	1,8

Nos constatations :

L'entreprise de **Cybersécurité** et l'entreprise de **Défense** ont un niveau de **Cyber Score Stratégique** équivalent à **3,6** - soit une Cybersécurité Stratégique **Globale** - en partant d'évaluations individuelles différentes. De même, les quatre autres entreprises - ESN, Automobile, Luxe et Santé - ont le même CSS de **2,6** - soit une Cybersécurité Stratégique **Apprenante** - en partant d'évaluations individuelles différentes. Finalement notre PME est logiquement moins mure que les Grands Comptes mais le modèle reste pertinent pour cette cible spécifique. Elle affiche un **Cyber Score Stratégique** de **1,8** et donc une Cybersécurité Stratégique **émergente**.

Nous en dérivons un radar dont la surface est, bien sûr, fonction de la Cybersécurité Stratégique de l'entreprise.

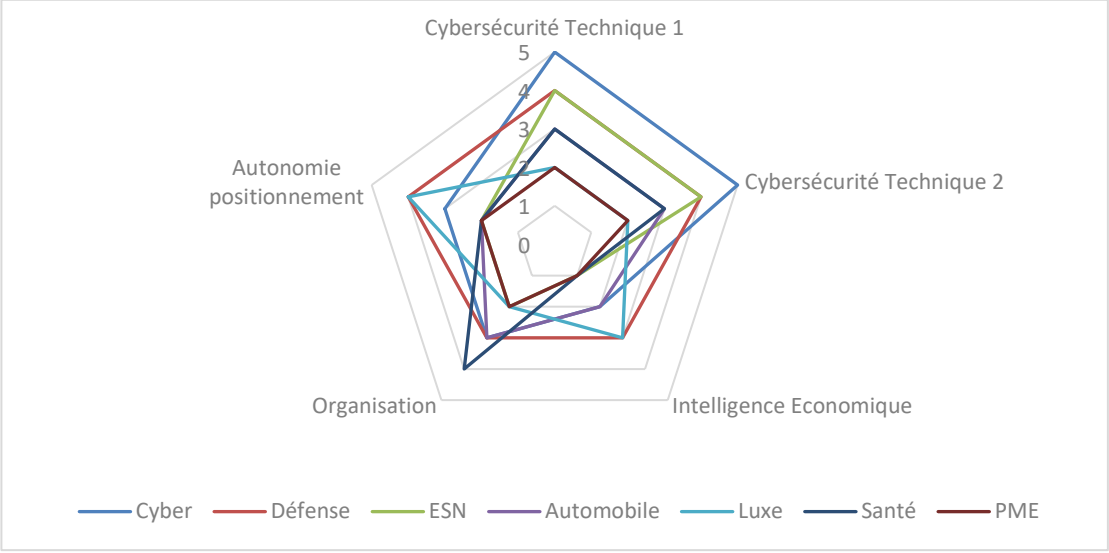
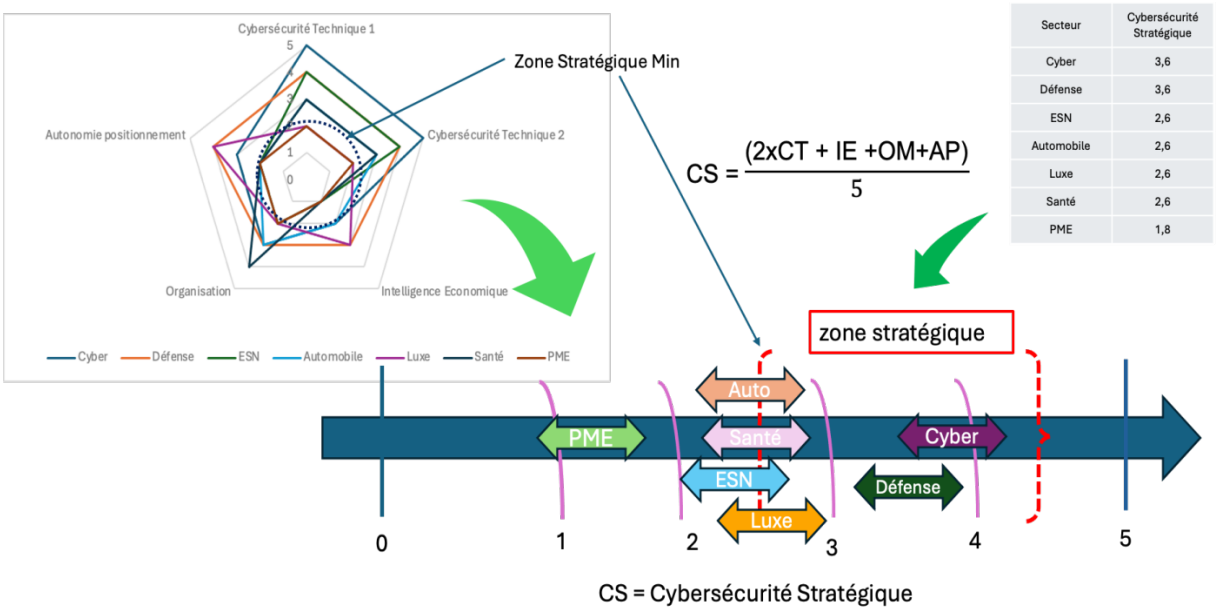


Figure 20 - Radar de cybersécurité stratégique du panel

V.2.3 Synthèse des évaluations du panel en Cybersécurité Stratégique



Secteur	Cybersécurité Stratégique
Cyber	3,6
Défense	3,6
ESN	2,6
Automobile	2,6
Luxe	2,6
Santé	2,6
PME	1,8

Figure 21 - Synthèse cybersécurité stratégique

Le niveau 3, la **Cybersécurité Stratégique Apprenante**, est déjà un niveau intéressant puisqu'il s'agit de la résultante de 4 variables clés, on peut considérer qu'il s'agit du début de la zone stratégique.

Dans notre exemple, la **PME** affiche un niveau **Emergent** mais elle a tout à fait les moyens de monter en maturité elle aussi.

Tableau 11 : Libellé Cybersécurité Stratégique

Intervalle du Cyber Score Stratégique	Libellé de la plage de Cybersécurité Stratégique
1 < CS 1,5	CS **Embryonnaire**
1,5 < CS < 2,3	Cybersécurité Stratégique **Émergente**
2,3 < CS < 3,2	Cybersécurité Stratégique **Apprenante**
3,2 < CS < 4	Cybersécurité Stratégique **Globale**
CS ≥ 4	**Cyber Puissance Stratégique**

V.3 Les modèles, des leviers pour transformer l'entreprise

Bien évidemment, le modèle de maturité proposé a pour ambition première de donner **une photo à un instant T** du **Cyber Score Stratégique** d'une entreprise en particulier.

Néanmoins, à travers un programme de transformation transverse, ces modèles de maturité constituent un excellent moyen pour permettre aux entreprises de **monter en maturité**.

Prenons le cas d'une entreprise de notre panel, par exemple l'**Entreprise de Service Numérique**. Notre calcul indique une valeur de 2,6 en Cybersécurité Stratégique, c'est-à-dire une Cybersécurité **apprenante**.

Il s'agit déjà d'un niveau intéressant mais l'entreprise pourrait tout à fait être désireuse de monter en maturité afin d'être plus performante. Naturellement elle dispose de plusieurs approches différentes et complémentaires pour ce faire. Ainsi, elle peut décider de passer de :

- 4 à 5 en **Cybersécurité Technique**
- 1 à 2 en **Intelligence Économique**
- 2 à 3 en **Positionnement**
- 2 à 3 en **Organisation & Moyens**

Maintenant, l'effort pour passer d'un niveau **1-Initial** à un niveau **2-Géré** ou d'un niveau **3-Défini** à un niveau **4-Mesuré** ou encore pour passer d'un niveau **4-Mesuré** à un niveau **5-Optimisé** n'est pas le même.

Il parait moins coûteux de gravir les premiers échelons même si l'**effort politique** pour démarrer n'est pas à sous-estimer.

Ainsi, passer de **3** à **4** ou **4** à **5** coûtera sans doute plus cher que de passer de **1** à **2** mais en même temps les décideurs seront plus à l'écoute si l'entreprise est déjà à un niveau **3-Défini** par exemple.

Pour résumer, il existe plusieurs pistes à emprunter pour faire grimper la **Cybersécurité Stratégique** de l'entreprise en décidant d'investir sur telle ou telle variable.

Naturellement cela demandera des efforts **opérationnels** ou bien le lancement de **projets spécifiques** en fonction des pistes choisies.

V.4 Plan de montée en maturité à travers des projets et des opérations

La montée en maturité pourra se faire très naturellement à travers un certain nombre de projets qu'on rassemblera au sein d'un **Programme de Transformation**.

Reprenons notre **Entreprise de Service Numérique** avec une maturité en **Cybersécurité Stratégique** de **2,6** soit le niveau **Apprenante**. Voilà le détail de son évaluation :

Tableau 12 : Evaluation initiale de l'ESN

	Cybersécurité Technique 1	Cybersécurité Technique 2	Intelligence Economique	Positionnement	Organisation	Cybersécurité Stratégique
ESN	4	4	1	2	2	2,6

V.4.1 Plan de montée en maturité autour de la Cybersécurité Technique

L'**ESN** décide de viser l'excellence en **Cybersécurité Technique** et passer de **4** à **5**.

Tableau 13 : La Cybersécurité Technique de l'ESN passe de 4 à 5

N	Cybersécurité Technique	Description
4	Se défendre **Cyber Défense**	La cyber défense répond à la nécessité d'orienter la détection des incidents numériques afin d'**anticiper** et **optimiser** la réponse d'une organisation. Il s'agit de concevoir et formaliser une capacité de supervision de la sécurité (**SOC**) qui s'intégrer avec un dispositif de **CSIRT/CERT** pour structurer la chaine de réponse aux incidents de sécurité, de la détection à la remédiation. Ex : Tableaux de Bord de sécurité, métriques de conformité, tests réguliers etc.
5	Se relever plus fort **Cyber Résilience**	Ce volet concerne la **continuité** d'activité avec un niveau de dégradation tolérable en cas de **crise**, puis la reprise nominale progressive pour minimiser les impacts stratégiques et métiers. La culture de la cybersécurité irrigue l'entreprise et s'intègre dans chaque projet et décision. L'organisation utilise des indicateurs de mesure de l'efficacité de sa cybersécurité, afin anticiper les risques et les menaces, améliorer continuellement ses pratiques et devenir encore **plus résiliente**. Ex : détection de menaces, incidents et crises : Rapport **BIA**, **CTI**, **PCA** et **PRA**. Optimisation du SMSI, programme de certification ISO 27001, EBIOS RM etc.

L'**ESN** a clairement une maturité élevée en Cybersécurité avec un score de **4**. Ainsi un premier SMSI est en place mais l'optimisation régulière n'est pas encore finalisée. C'est sans doute un projet à lancer pour passer au niveau **5**.

De même, EBIOS RM n'est pas utilisé dans l'entreprise et elle envisage également de former des collaborateurs clé dont le RSSI. C'est potentiellement une nouvelle offre qu'elle pourrait à terme proposer à ses clients.

Nous résumons ainsi les projets ou opérations envisagées :

- Projet d'optimisation du SMSI ;
- Projet de formation des équipe cybersécurité : formation ISO 27001 afin de mieux gérer le SMSI et formation/certification EBIOS RM ;
- Projets annexes.

V.4.2 Plan de montée en maturité en Intelligence économique

L'**ESN** désire passer de **1** à **2** voire **3** en **Intelligence Économique**.

Tableau 14 : l'Intelligence Economique de l'ESN passe de 1 à 2

N	Intelligence Économique	Description
1	**IE Réactive** et non structurée	L'IE est inexistante et pas organisée, certaines personnes font de l'IE sans le savoir. **Veille** uniquement **opportuniste** et peu structurée.
2	**IE Émergente** « intuitu personae »	**Veille** grâce à **l'IE ponctuelle** et **localisée** à un petit département, en réponse à des besoins immédiats, souvent par intuition ou par opportunisme. C'est globalement le fait d'individualités qui commencent à structurer une démarche et **conçoivent les premiers processus** d'intelligence économique pour le besoin spécifique du département. Prise de **conscience de l'état de guerre économique** par ces individualités.
3	**IE Informative** et structurée	Les processus d'IE se formalisent et se généralisent au niveau d'une BU au minimum. Cela suppose une compréhension plus générale du besoin et des apports globaux de l'intelligence économique afin d'**informer** et **dévoiler** le contexte réel de l'entreprise Les différentes activités d'Intelligence Economique se structurent au sein de l'entreprise.

La première étape est donc de faire suivre à une partie des cadres de l'entreprise une formation de découverte de l'**intelligence économique** ou mieux, de leur faire suivre un programme plus ambitieux autour de l'**IE**.

Ainsi un leader formé à l'**intelligence économique** pourrait prendre la direction du futur pôle d'**IE** et commencer à concevoir les **premiers processus** dans un premier temps pour son domaine d'activité. Cela permettrait sans doute faire passer le niveau d'**IE** de **1** à **2** dans un premier temps.

La montée au niveau **3** sera liée à la **généralisation** et standardisation des processus d'intelligence économique à toute l'entreprise.

Résumons ainsi les projets ou les opérations envisagées :

- Sélection des candidats, formation en intelligence économique ;
- Conception des processus d'intelligence économique
- Activités annexes.

V.4.3 Plan de montée en maturité en Autonomie & Positionnement

L'entreprise désire passer de **2** à **3** voire **4** en **Positionnement.**

Tableau 15 : L'Autonomie de l'ESN passe de 2 à 3

N	Positionnement	Description
2	Entreprise **Lucide et Éveillée**	Prise de conscience de la **guerre économique** et des impacts de l'environnement. L'entreprise s'éveille et prend **conscience** qu'il faut surveiller et tenir compte de son l'écosystème, même si la veille est souvent réduite à un petit département.
3	**Consciente des rapports de force**	L'entreprise interagit de façon régulière et structurée avec son écosystème, elle prend en compte les influences et **interdépendances géopolitiques** dans ses décision stratégique. Elle s'affirme comme un acteur de son **écosystème**. Le **juridique** au sein de l'entreprise devient **clé** en particulier pour comprendre l'écosystème cyber et, entre autres, les règles d'extra-territorialité et les **rapports de force**.
4	**Marge de Manœuvre** En recherche de liberté d'action	L'entreprise établit des **partenariats stratégiques** solides et collabore avec son écosystème, facilitant une liberté d'action accrue et maîtrisée Le **Comex** recherche une autonomie, des **marges de manœuvre**, permettant d'atteindre une liberté d'action stratégique pour l'entreprise. Ainsi il demande **explicitement** à la cybersécurité de faire ce qu'il faut pour s'affranchir des contraintes externes (techniques, juridiques etc.).

Afin de pouvoir monter au niveau **3** et devenir une **entreprise consciente des rapports de force**, l'ESN devra se rapprocher d'autres entreprises par exemple en intégrant des associations professionnelles. Le Rotary Club, le **Clusif**, le **PMI** ou encore **Numeum**, le syndicat des ESN… Ces pistes devraient sans doute lui permettre de mieux se connecter à son écosystème et ainsi atteindre le niveau **3**.

Pour le Niveau **4**, il sera nécessaire à la fois de nouer des partenariats stratégiques en particulier au niveau *business* mais également se rapprocher de la cybersécurité pour qu'elle puisse s'affranchir des contraintes externes (Cloud US, lois d'extra territorialité, matériel douteux etc.)

Résumons ainsi les projets et les opérations envisagées :

- Décision et communication de la stratégie du Comex aux collaborateurs ;
- Budget spécifique et « sensibilisation » des *leaders* pour « sortir de l'entreprise » et aller d'une entreprise **éveillée** vers une entreprise **connectée** et **autonome**.

V.4.4 Plan de montée en maturité en Organisations & Moyens

L'ESN désire passer de **2** à **3** voire **4** en **Organisations & Moyens.**

Tableau 16 : L'Organisation de l'ESN passe de 2 à 3

N	Organisation & Moyens	Description
2	O & M **externalisée**, en compréhension du sujet	Compréhension que l'organisation n'est pas suffisamment structurée malgré une bonne volonté évidente. Prise de conscience qu'il faut se faire aider. **Externalisation** partielle.
3	Organisation **internalisée**, adaptée et standardisée	Une nouvelle organisation apparait, le Comex fait évoluer la gouvernance et reprend le *lead* sur la cybersécurité. Création d'une direction de la **sécurité** qui centralise la cybersécurité au niveau de l'entreprise. Les processus décisionnels sont établis et les responsabilités sont clairement attribuées au sein de l'organisation.
4	Organisation **pilotée**	L'efficacité de l'organisation est mesurée et pilotée à travers des indicateurs précis. Le Comex valorise les travaux de l'IE et lui donne son organisation propre et **un responsable IE.**

A priori, l'ESN étant au niveau **2** en Organisation, une partie de sa cybersécurité est **sous-traitée**. Pour passer au niveau **3**, elle pourrait décider de créer une direction de la sécurité intégrant la **Cybersécurité** réellement distincte de la DSI.

La personne à la tête de ce département ou direction de la cybersécurité, en plus d'une expérience pertinente, pourrait avantageusement suivre une formation longue en gouvernance de la **Cybersécurité**. Le rôle de cette direction serait, bien sûr, de centraliser, standardiser et généraliser la démarche.

Cela est indéniablement un projet d'Organisation et de RH qui structurera la société afin de lui permettre d'atteindre le niveau **3**.

Pour atteindre le niveau **4**, le leader formé à l'**IE** pourrait prendre la tête d'une direction de l'**Intelligence Économique**.

Résumons ainsi les projets ou les opérations envisagées :

- Création et structuration d'une direction de la **cybersécurité** **distincte** de la DSI ;
- Sélection du **leader** amené à diriger cette structures et formations adéquates ;
- Création et structuration d'un pôle ou direction d'intelligence économique et choix du **leader**.

V.4.5 Démarche d'Amélioration Continue de la Cybersécurité Stratégique

La démarche globale comporte les étapes suivantes :

V.4.5.1 Évaluation initiale de la Cybersécurité Stratégique de l'entreprise à l'instant T

1. Etat des lieux et démarrage (Présentation de la démarche, constitution des équipes).
2. Évaluation de chacun des 4 axes individuellement.
3. Calcul du **Cyber Score Stratégique Initial.**
4. Discussion du résultat avec le COMEX pour le contextualiser et décision ou non de faire monter la maturité en CS et selon quels délais.

V.4.5.2 Plan de montée en maturité de la Cybersécurité Stratégique

1. Analyse du **Cyber Score Stratégique Initial** et proposition d'un **Cyber Score Stratégique Objectif** (à atteindre collectivement par les équipes).
2. Identification des **différentes pistes** permettant la montée en maturité sur les différents axes.
3. Passage des **pistes** vers des **projets** « réalistes » ou des **opérations** au sein d'un **Programme de Transformation de montée en maturité.**
4. Confirmation du **Cyber Score Stratégique Objectif** à atteindre.
5. Décision du Comex : Cadrage et Lancement d'un Programme Transverse.

V.4.5.3 Lancement opérationnel du programme de Transformation

1. Démarrage du programme : planification, constitution des équipes.
2. Lancement et suivi individuel des projets et des opérations.

V.4.5.4 Nouvelle évaluation de la Cybersécurité Stratégique

Chaque année une nouvelle évaluation du **Cyber Score Stratégique** devra être effectuée.

Cette démarche est synthétisée dans le schéma suivant :

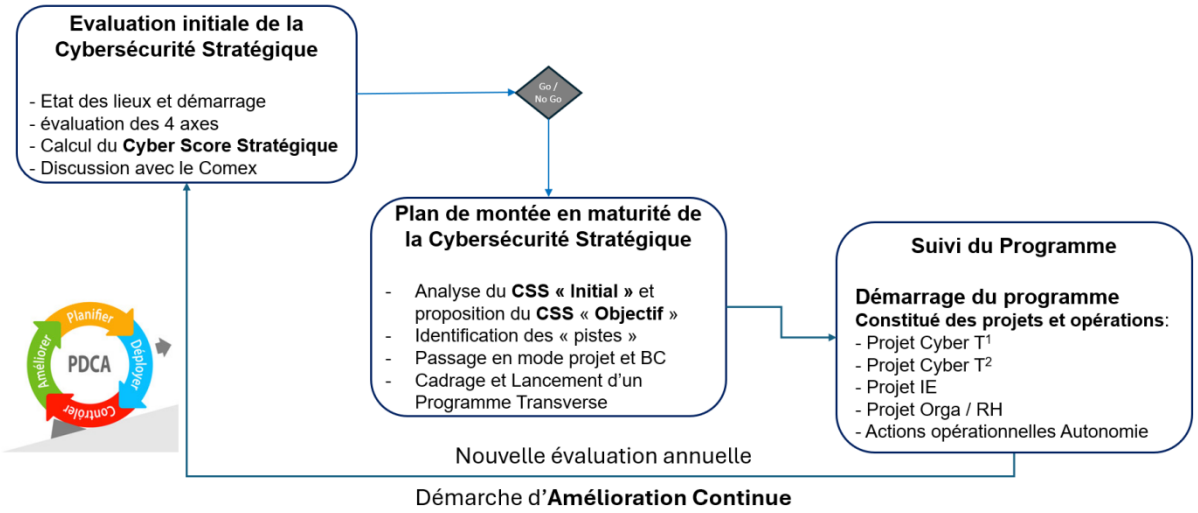


Figure 22 - Schéma de montée en maturité de la CS

V.5 Une démarche qui s'intègre dans le cadre de gouvernance projet de l'entreprise

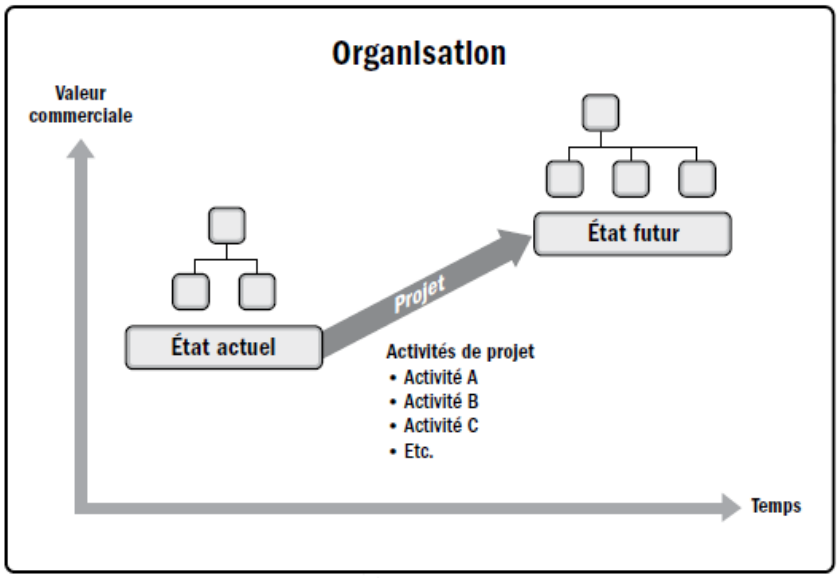


Figure 23 - Transition des états organisationnels via un projet

Source : https://www.pmi.org/standards/pmbok

Comme nous l'avons vu, les modèles de maturités permettent de donner une **photo** à un moment **T** de la maturité de l'entreprise.

Il est, en revanche, nécessaire de s'appuyer sur des transformations d'entreprises, c'est-à-dire en général des **projets** afin de la faire **changer d'état** - état actuel vers l'état futur - et ainsi la faire progresser. Dans notre cas, les projets permettront de faire monter en maturité la Cybersécurité Stratégique de l'entreprise.

En revanche, les projets permettant de faire monter en maturité la Cybersécurité Stratégique de l'entreprise, comme **tous les projets** doivent s'intégrer dans le cadre de gouvernance de cybersécurité et des transformations. Ce point sera détaillé dans le chapitre suivant.

VI. Instanciation d'une gouvernance « cybersécurité et transformations »

VI.1 Intégration de la sécurité dans les projets et programmes de l'entreprise

Nous venons de voir dans le chapitre **V** que la montée en maturité de l'entreprise en matière de **Cybersécurité Stratégique** se fera pour partie à travers des **projets spécifiques** dont des projets de cybersécurité comme la mise en place d'un SMSI, par exemple.

Néanmoins, il est indispensable pour toutes les transformations de bien **intégrer la sécurité** et ce dès le lancement du projet et tout au long du cycle de vie du projet. Elles doivent donc s'inscrire dans une instanciation d'un **cadre de gouvernance de la cybersécurité et des transformations**.

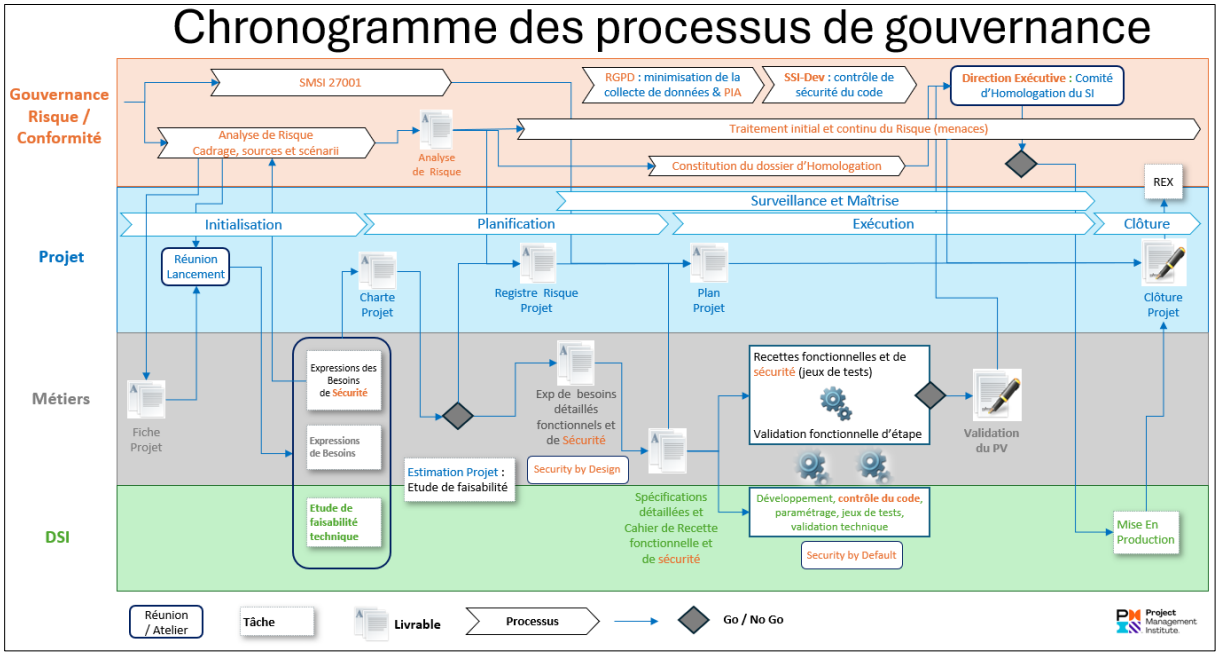


Figure 24 - les différents niveaux impliqués dans la Gouvernance

Source : Livre blanc du PMI France : Projets & Cybersécurité – Ecosystème et Gouvernance de la SI

Ce schéma (consultable en annexe 4 dans un format plus lisible) propose une représentation systémique des processus de gouvernance impliqués dans l'intégration de la cybersécurité au sein des projets. Son objectif est d'offrir une compréhension globale des interactions entre différents niveaux organisationnels et des responsabilités associées à chaque acteur clé dans la conduite sécurisée des projets.

Ce cadre de gouvernance intègre des processus d'une **maturité élevée** tant dans le domaine **Gouvernance Risque Conformité** que celui du **Pilotage de projet**. Il dérive des travaux détaillés dans le chapitre V.

VI.2 Quatre niveaux d'organisation qui coopèrent

Le dispositif de gouvernance est structuré autour de **quatre niveaux distincts**, chacun ayant son rôle spécifique :

Gouvernance, Risque et Conformité (GRC) :

Le niveau **GRC** englobe le Responsable de la Sécurité des Systèmes d'Information (RSSI) ou le directeur de la sécurité. Ce dernier agit en concertation avec la Direction Générale (ou le Comité exécutif) afin d'assurer la validation des jalons majeurs du projet, notamment ceux relatifs à l'**homologation** du système d'information. Ce niveau garantit ainsi la conformité des démarches aux exigences réglementaires et stratégiques de l'organisation.

Projet :

Ce niveau réunit le chef de projet, le directeur de projet ou de programme, dont la mission est d'assurer le pilotage opérationnel de la transformation. Il leur incombe de coordonner l'ensemble des acteurs, de planifier les actions et de superviser le bon déroulement du projet en conformité avec les objectifs impartis.

Métier :

Le responsable métier est à l'origine de la demande et des exigences du projet. En conséquence, il occupe un rôle central. Il porte la voix des utilisateurs finaux et est garant de la conformité du livrable avec les besoins fonctionnels. Sa contribution s'avère essentielle lors des arbitrages financiers, de la co-construction des solutions, ainsi que lors des phases de validation (recette).

Direction des Systèmes d'Information (DSI) :

Chargée de la mise en œuvre technique, la DSI assure que le produit livré respecte les contraintes d'architecture, les impératifs budgétaires et les standards de sécurité fixés. Un dialogue constant avec les autres échelons s'avère fondamental pour garantir l'adéquation de la solution avec le contexte organisationnel.

VI.3 Importance de la coordination entre ces différents niveaux

Le succès d'un projet dépend de la capacité des différents acteurs à interagir de manière fluide et constructive :

- Le chef de projet doit posséder une vision claire des rôles et responsabilités de chaque échelon, afin de concilier les intérêts et exigences parfois divergents.
- La réussite du projet repose sur l'engagement de chaque acteur dans son rôle propre. Le métier doit être force de proposition, particulièrement en matière de besoins et de sécurité. Il doit participer activement aux choix techniques, aux arbitrages budgétaires et à la validation finale des livrables.
- La DSI doit se montrer attentive aux attentes exprimées et s'adapter aux contraintes, tout en veillant au respect du cadre technique et financier.
- Le niveau de gouvernance, souvent sous-estimé, joue un rôle structurant. Il assure l'alignement du projet avec la stratégie totale et veille à l'implication de la Direction Générale, facteur clé pour le portage des sujets de sécurité.

L'intégration efficace de la sécurité dans les projets nécessite une gouvernance structurée, impliquant l'ensemble des parties prenantes autour de processus clairement définis. La compréhension fine et le respect des rôles par chacun des échelons sont les

garants d'une démarche cohérente, conforme aux exigences réglementaires et en phase avec les besoins métiers.

VI.4 Les acteurs des transformations

La mise en œuvre de ces bouleversements au sein d'une organisation ne s'improvise. Notamment, pour donner les meilleures chances de réussite possible à ce chantier stratégique, il faut choisir les bonnes personnes, les bons process. Cette sous-partie met en exergue le rôle des responsables de la sécurité de l'information et des responsables de projet. En outre, un bref rappel de l'intérêt d'une matrice de suivi de projet, telle que RACI, est effectué.

VI.4.1 Les différents rôles du RSSI et/ou du CISO

Une question se pose de manière récurrente au sujet du Responsable de la Sécurité du Système d'information, le fameux RSSI. La dénomination anglo-saxonne de CISO - Chief Information Security Officer - représente-t-elle la même chose que la dénomination française de RSSI ?

Le CISO fait partie des CxO et il est idéalement rattaché au COMEX. En France le RSSI a plutôt un rôle opérationnel. La partie stratégique du rôle est, généralement, confié à un directeur conformité (et risque). Donc globalement CISO et RSSI recouvrent des rôles légèrement différents. Même aux Etats-Unis, le CISO n'est pas toujours au même niveau que les autres "C-levels", et peu sont directement rattachés au COMEX. Néanmoins, dans bien des cas le CISO est rattaché à un membre du Comex.

Néanmoins, une solution existe pour résoudre cette situation. Il suffit de séparer les domaines d'intervention du RSSI en deux :

- **RSSI Gouvernance Risque Conformité** (RSSI GRC) : au cœur des organisations stratégiques, un conseiller du Comex définit la politique de sécurité à haut niveau et travaille étroitement avec le RSSI opérationnel. Il peut être rattaché à un directeur de la conformité par exemple.
- **RSSI Opérationnel** : il a pour mission de maintenir la sécurité des SI. En tant qu'assistance à maîtrise d'œuvre, il apporte son expertise et propose des mesures de sécurité en termes d'architectures, de produits et de paramétrages. L'objectif est de se conformer aux bonnes pratiques, à la PSSI de l'organisation et aux mesures arbitrées lors des analyses de risque. Ainsi la direction et son RSSI GRC bénéficient de la sécurité des éléments techniques du système d'informations de l'organisation.

VI.4.2 Le rôle du Chef de Projet et/ou du Responsable de Programme

Le Chef de projet aura naturellement la charge du pilotage du Projet et responsable des différents processus de management de projet suivants :

1. **Initialisation :** cadrage du projet, en lien avec le cadrage et socle de sécurité de l'analyse de Risque ;
2. **Planification** : Dès les premières phases, il est crucial d'intégrer la gestion des risques cyber. Cela comprend l'identification des actifs critiques, l'analyse des menaces potentielles et la définition des exigences de sécurité ;
3. **Exécution** : Pendant la mise en œuvre du projet, des mesures de sécurité doivent être appliquées pour protéger les systèmes et les données. Des audits réguliers et des tests de vulnérabilité permettent de s'assurer de l'efficacité des contrôles de sécurité ;
4. **Surveillance et Maîtrise** : Une fois le projet opérationnel, la surveillance continue des systèmes et la détection des incidents de sécurité sont essentielles. Des plans de réponse aux incidents doivent être mis en place pour gérer efficacement les situations critiques ;
5. **Clôture** : À la fin du projet, il est important de prendre des mesures pour assurer la sécurité des données et des systèmes, même après la fin de leur utilisation. Cela peut inclure la suppression sécurisée des données, la désactivation des systèmes et la mise à jour des politiques de sécurité.

Il sera également en charge des livrables de management de Projet. Pour mémoire, citons les principaux livrables :

- La charte de projet ;
- Le Registre des risques ;
- Le Plan de management de Projet ;
- La clôture de projet.

VI.5 La matrice RACI, un outil synthétique

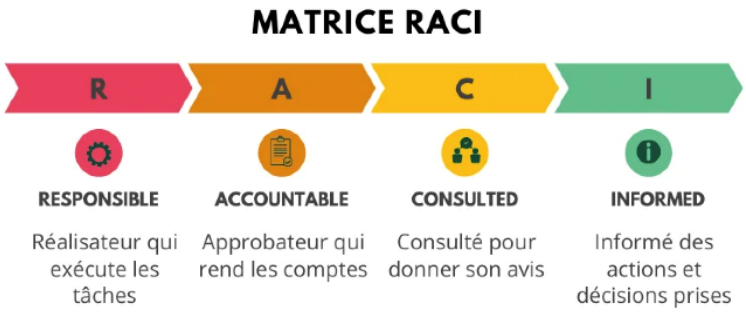


Figure 25 - La matrice RACI

Source : https://blog-gestion-de-projet.com/quest-ce-que-la-matrice-raci/

La matrice RACI (**Responsable, Accountable, Consulted, Informed**) est un outil de gestion de projet qui permet de clarifier et de formaliser la répartition des rôles et responsabilités entre les différents acteurs impliqués. Ce modèle structurel est particulièrement pertinent pour **articuler l'interaction** entre la **gouvernance** (pilotage stratégique, conformité, sécurité) et le **pilotage opérationnel des projets**, notamment dans des organisations complexes ou multisites comme les Entreprises de Services Numériques (ESN)[134].

La responsabilité principale du pilotage des projets incombe aux acteurs opérationnels, notamment les **directeurs et chefs de projet**, qui assurent la conduite pratique et la réussite des initiatives. Toutefois, la gestion de la sécurité s'appuie sur un dispositif articulant à la fois une présence au niveau du terrain et un accompagnement institutionnel.

Dans le contexte d'une Entreprise de Services Numériques (ESN), la structuration des projets s'organise autour de Centres de Services, placés sous la supervision de directeurs et chefs de projet, sans intervention directe de la DSI dans cet exemple. Ainsi, les équipes projets prennent en charge l'intégralité du développement logiciel, chaque projet intégrant un chargé de sécurité opérationnelle dédié.

La coordination globale de la sécurité au sein de l'entreprise est confiée à une équipe centrale de sécurité, pilotée par un **Responsable de la Sécurité des Systèmes d'Information** (RSSI) rattaché à la direction de la conformité, elle-même représentée au sein du comité exécutif (COMEX). Cette équipe se compose de divers professionnels : experts en veille sécuritaire, gestionnaires d'incidents et auditeurs internes.

L'équipe centrale de sécurité exerce un rôle d'accompagnement transversal auprès des projets, notamment au travers de la réalisation d'analyses de risques, de conduites d'études spécialisées, d'audits, de conseils relatifs au suivi des vulnérabilités et d'actions de sensibilisation. Par ce biais, le **RSSI** et son équipe assurent la gouvernance sécurité et fédèrent la communauté des acteurs sécurité impliqués dans les différents métiers et projets de l'organisation.

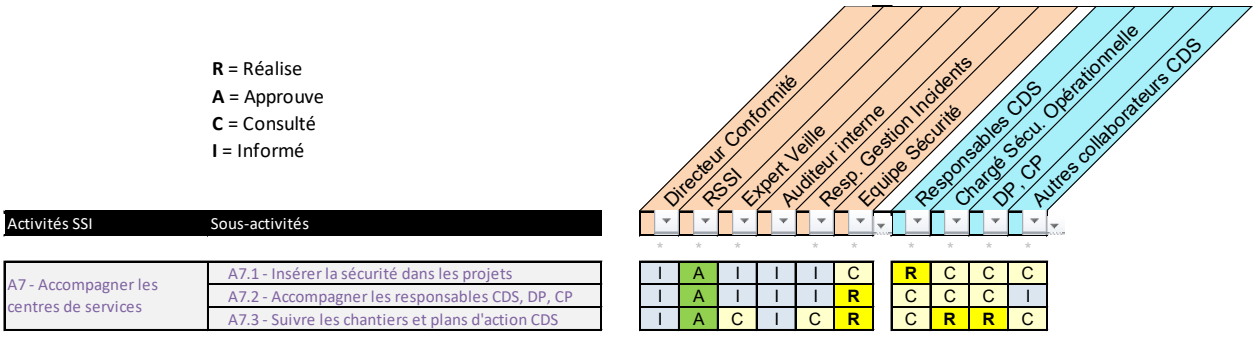


Figure 26 - Répartition des rôles et la Gouvernance et le Management de Projet

Comme le présente l'exemple de RACI ci-dessus, l'affectation varie en fonction du projet et du contexte de l'entreprise.

[134] : Laurent Grancer. « Matrice RACI », 15 juillet 2025. https://www.manager-go.com/gestion-de-projet/dossiers-methodes/matrice-raci. GO, « Matrice RACI », 15 juillet 25.

Conclusion

Arrivé au terme de cette réflexion sur les interactions possibles entre l'intelligence économique et la cybersécurité, le constat est sans appel : s'il est tout à fait possible d'instaurer un état de cybersécurité dans une entreprise sans recours à l'intelligence économique, il est beaucoup plus incertain de réussir à aligner la stratégie de cybersécurité sur la stratégie totale de l'entreprise sans le recours à l'intelligence économique. Et d'ailleurs, comment aurait-il pu en être autrement dans la mesure où l'intelligence économique c'est la « *maîtrise de l'information stratégique* »[135], alors que la cybersécurité, c'est l'activité de protection de cette l'information ?! L'acquérir par l'IE, puis la protéger par la cybersécurité pour empêcher ces concurrents de l'acquérir à leur tour, constituent les deux faces d'une même pièce. L'approche « technico-financière » de l'état de cybersécurité n'est donc pas sans valeur, sans efficacité, mais elle s'avère coûteuse et surtout révélatrice d'une approche en vase clos de la cybersécurité. En effet, son étude révèle les dépendances et les limites dont elle est porteuse, les risques qu'elle fait peser sur la capacité de l'entreprise à conduire souverainement sa stratégie totale.

Or cette prise de conscience sans le recours à l'intelligence économique aurait été extrêmement compliqué puisque c'est elle qui dévoile le contexte de guerre économique dans lequel s'exerce l'activité des entreprises : compétition féroce où tous les coups sont permis, où les Etats mettent leurs pouvoirs régaliens et leurs administrations au service de la vitalité économique de leurs acteurs nationaux. Le cyberespace, de par sa pénétration dans l'ensemble des autres territoires, est également devenu un lieu d'affrontements… à fleurets mouchetés ? Pas certain, car si la guerre économique n'est pas sanglante, elle n'est pas non plus sans violence symbolique. Son bilan se mesure à l'aune d'emplois précaires ou perdus, d'usines abandonnées, de villes dépérissant, de manifestations sociales… d'émeutes. Et dans le cyberespace : brevets volés, rançons exorbitantes, experts débauchés, machines vérolées voire modifiées, téléphones espionnés, entreprises ruinées, réputations détruites…

Pour bien comprendre l'importance de la cybersécurité au sein d'une entreprise, il faut comprendre leur relation. L'école française de pensée stratégique a mis en exergue la nécessité d'instaurer une stratégie totale coordonnant l'ensemble des stratégies subordonnées, distinctes et interdépendantes, afin d'arriver au but désiré. Ainsi, la stratégie de cybersécurité constitue une stratégie subordonnée distincte et interdépendante au service de la stratégie totale de l'entreprise. Toutefois, la stratégie de cybersécurité tient un rôle particulier puisque, toujours selon les réflexions des stratèges français, « *la lutte pour la liberté d'action est en effet l'essence de la stratégie. Il en résulte que la protection de sa propre liberté d'action (la sûreté) et l'aptitude à priver l'adversaire de sa liberté d'action (par la surprise et par l'initiative) constituent les bases du jeu stratégique.* »[136] Ainsi, parce que la cybersécurité a pour objet la « *protection de sa propre liberté d'action* » de l'entreprise, elle se situe à la base du jeu stratégique, elle constitue une condition certes non suffisante, mais nécessaire, de ce jeu.

C'est donc à la lumière de cette dimension qu'il faut juger du grand intérêt de l'intelligence économique au service de la performance de la stratégie de cybersécurité. Parce que l'intelligence économique n'éclaire pas seulement les problèmes, elle informe également

[135] Alain Juillet. « Qu'est-ce que l'intelligence économique ? », Document de travail (Sécrétariat général de la Défense nationale, 2004).
[136] Beaufre, *Introduction à la stratégie*, p.184.

sur les solutions ! Parmi celles-ci, comme cela a été étudié dans ce document, la recherche de la souveraineté numérique dans une stratégie de cybersécurité constitue une solution éminente. Réduisant les dépendances et les incertitudes, elle réduit la possibilité de concurrents de porter directement ou indirectement atteinte à la liberté d'action. Il convient d'ajouter que la liberté d'action n'est jamais un jeu à somme nulle : lorsque la sienne augmente, celle des concurrents diminue (gagnant-perdant), et celle des partenaires augmente (gagnant-gagnant). On peut également citer l'apport de l'intelligence économique, au sein de cette stratégie de cybersécurité, pour la gestion des ressources humaines, la gestion des risques, la communication…

Ce mémoire a été rédigé dans l'idée d'aller progressivement du général au particulier, de l'abstrait au concret. Après la définition du cadre conceptuel (stratégie cyber protégeant la liberté d'action de la stratégie totale), après la mise en exergue de la guerre économique dans le cyberespace grâce à l'intelligence économique, après la proposition de corrections et de mesures correctives telles que la souveraineté numérique, il fallait se mettre au niveau de chaque entreprise, proposer une clé d'accompagnement précise, parfaitement adaptée à sa situation, ses besoins, son ambition… sa stratégie totale. Un modèle de maturité, selon le modèle matriciel CMMI, s'est imposé comme une évidence. Ce modèle de maturité est la matérialisation des réflexions menées dans les premières parties du mémoire et il a pour ambition de modéliser l'organisation pour mieux la comprendre. Il s'appuie sur quatre axes complémentaires : la cybersécurité technique, l'intelligence économique, l'organisation et les moyens alloués ainsi que l'autonomie et le positionnement de l'entreprise. Ensemble, ces quatre variables définissent la **cybersécurité stratégique,** c'est-à-dire que cela permet d'évaluer si l'entreprise a correctement pris conscience de l'importance de la cybersécurité dans le « jeu stratégique ». Simple sans être simpliste, il permet aux différentes organisations de s'évaluer aisément afin de calculer leur Cyber Score Stratégique. Par la suite, cette évaluation initiale permet d'identifier des chemins de montée en maturité et donc en performance de l'entreprise, en particulier à travers des projets.

Parce que les projets s'incarnent nécessairement dans une gouvernance, parce qu'il faut des personnes pour mettre en œuvre la roue de Déming (planifier, déployer, contrôler, améliorer – auquel nous rajoutons en amont le verbe « penser »), ce travail s'est conclu par des conseils sur cette gouvernance et le rôle de ces personnes.

En introduisant ce travail il y a plusieurs mois, l'élection de Donald Trump était considérée comme une opportunité d'enfin prendre conscience de cette conflictualité des relations géoéconomiques en vue d'un réarmement tout d'abord intellectuel et moral. Au moment d'écrire ces lignes, le même président vient de remporter une immense victoire économique contre l'Union Européenne par l'établissement de droits de douane, mais également de promesses de 600 milliards de dollars d'investissement dans l'économie américaine. Par l'absurde, cet évènement démontre la nécessité de ce réarmement. Pour avoir négligé la leçon de Xénophon, pour avoir oublié que ce sont les mêmes vérités fondamentales déjà énoncées depuis des millénaires qui ne font que se présenter de nouveau avec un habit neuf, que reste-t-il de la liberté d'action des entreprises françaises ? Dans un mode de stratégie indirecte où la stratégie économique constitue le principal effet de levier de l'accroissement de puissance, que reste-t-il des ambitions de souveraineté numérique clamées par les plus hauts dirigeants français et européens ? Il n'est peut-être pas encore minuit, mais assurément, il est minuit moins le quart…

Références bibliographiques

Intro

Le Monde Informatique. « Telex : Le compte Microsoft du procureur de la CPI suspendu, Vincent Villette nommé secrétaire général de la Cnil ». 19 mai 2025. https://www.lemondeinformatique.fr/actualites/lire-telex-le-compte-microsoft-du-procureur-de-la-cpi-suspendu-vincent-villette-nomme-secretaire-general-de-la-cnil-un-datacenter-pour-chauffer-l-eau-de-brassage-d-une-biere-96874.html.

Owen Sayers. « Microsoft coupe les mails de la Cour Pénale Internationale, un avertissement pour tous les Européens ». LeMagIT, 27 mai 2025. https://www.lemagit.fr/actualites/366624982/Microsoft-coupe-les-mails-de-la-Cour-Penale-Internationale-un-avertissement-pour-tous-les-Europeens.

Partie 1

André Beaufre. Introduction à La Stratégie. Hachette, 1998.

ANSSI. Construire la gouvernance de sécurité numérique adaptée à son organisation. 23 mai 2024. https://cyber.gouv.fr/construire-la-gouvernance-de-securite-numerique-adaptee-son-organisation.

Aurélie Tavernier. L'importance d'instaurer une culture de la sécurité au sein de votre entreprise. 15 juillet 2025. https://immersivefactory.com/fr/actualites/268-Limportance-dinstaurer-une-culture-de-la-s%C3%A9curit%C3%A9-au-sein-de-votre-entreprise.

Beaufre, André, et François Géré. La stratégie de l'action. Nouv. éd. Monde en cours. Éd. de l'Aube, 1997.

Bruce Schneier. « The Process of Security ». Schneier on Security, 2000. https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html.

Corinne Laurta. Le rôle essentiel de la gouvernance dans la cybersécurité. Affairesinternationales Édition. 10 juillet 25. Affairesinternationales Édition. https://www.affairesinternationales.fr/le-role-essentiel-de-la-gouvernance-dans-la-cybersecurite/.

CSM. « Création d'un système de management de la sécurité de l'information (SMSI) conforme à la norme ISO 27001 ». s. d. https://cybersecurite-management.fr/creation-dun-systeme-de-management-de-la-securite-de-linformation-smsi-conforme-a-liso-27001/.

Ferdinand Foch. Des principes de la guerre. Deuxième édition. Berger-Levrault & Cie, 1906.

Gouvernance en cybersécurité : principes essentiels pour les entreprises modernes. 16 juillet 2025. https://ami-gestion.fr/gouvernance-cybersecurite/.

IBM et Palo Alto Networks. How unified cybersecurity platforms add business value. 2025. https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/unified-cybersecurity-platform.

Ingrid Vergara. « Cybersécurité : les entreprises de plus en plus ciblées par les « hacktivistes » ». Tech & Web. Le Figaro, 5 décembre 2024. https://www.lefigaro.fr/secteur/high-tech/cybersecurite-les-entreprises-de-plus-en-plus-ciblees-par-les-hacktivistes-20241205.

Julien VERCHÈRE. « Cybersécurité : quel est l'état de la menace en France ? » Société. mesinfos, 11 mars 2025. https://mesinfos.fr/cybersecurite-quel-est-l-etat-de-la-menace-en-france-218061.html.

« Le CyberDico | ANSSI ». https://cyber.gouv.fr/le-cyberdico.

Steve McDowell. Why AT&T's Suing Broadcom Over Forced VMware License Charges. Cloud. 6 septembre 2024. https://www.forbes.com/sites/stevemcdowell/2024/09/06/why-atts-suing-broadcom-over-forced-vmware-license-changes/.

Steve Morgan. « Top 10 Cybersecurity Predictions and Statistics For 2024 ». Cybercrime Magazine, 8 janvier 2021. https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/.

The CISO Report 2025. Splunk / CISCO, 2025. https://www.splunk.com/en_us/pdfs/gated/ebooks/ciso-report-2025.pdf.

Vincent Desportes. « Stratégie et liberté d'action ». Politique étrangère, nº 1 (mars 2018): 133-42. https://doi.org/10.3917/pe.181.0133.

Partie 2

Alexander Martin. « Spain Awards Huawei Contracts to Manage Intelligence Agency Wiretaps ». The Record, 11 juillet 2025. https://therecord.media/spain-awards-contracts-huawei-intelligence-agency-wiretaps.

Ali Laïdi. « Histoire mondiale de la guerre économique ». Hors collection, Vuibert, 2023, 104-104.

Ali Laïdi. Histoire mondiale de la guerre économique. Perrin, 2016.

Amandine Jonniaux. « Finalement, WeTransfer fait marche arrière sur l'utilisation de vos données ». Intelligence Artificielle. Journal du Geek, 17 juillet 2025. https://www.journaldugeek.com/2025/07/17/finalement-wetransfer-fait-marche-arriere-sur-lutilisation-de-vos-donnees/.

Andy Greenberg. « How China Demands Tech Firms Reveal Hackable Flaws in Their Products ». Tags. Wired, 6 septembre 2023. https://www.wired.com/story/china-vulnerability-disclosure-law/.

Anne de Guigné. « «L'entreprise sans usines» : Serge Tchuruk ou le symbole de la désindustrialisation ». Conjoncture. Le Figaro, 14 août 2024. https://www.lefigaro.fr/conjoncture/l-entreprise-sans-usines-serge-tchuruk-ou-le-symbole-de-la-desindustrialisation-20240813.

Bertrand Warusfel. Intelligence économique et droit. 1995.

Bruno Amable, Elvire Guillaud, et Stefano Palombarini. L'économie politique du néolibéralisme: le cas de la France et de l'Italie. Collection du CEPREMAP 26. Éd. Rue d'Ulm, 2012.

Carine Guillemet. « Quentin Adam invité de Micode dans l'émission Underscore_ ». Clever Cloud, 27 mars 2025. https://www.clever-cloud.com/fr/blog/entreprise/2025/03/27/quentin-adam-invite-de-micode-dans-lemission-underscore_/.

Del Rosso Kristin et Dakota Cary. Sleight of Hand: How China Weaponizes Software Vulnerabilities. Atlantic council, 2023. https://www.atlanticcouncil.org/in-depth-research-reports/report/sleight-of-hand-how-china-weaponizes-software-vulnerability/.

Emilia Samuelsson. European Parliament approves watered-down Euro 7 rules | Air Pollution & Climate Secretariat. 2024. https://www.airclim.org/acidnews/european-parliament-approves-watered-down-euro-7-rules.

European Parliament. « Revision of CO2 Emission Performance Standards for Cars and Vans, as Part of the European Green Deal | Legislative Train Schedule ». 2022. https://www.europarl.europa.eu/legislative-train/package-fit-for-55/file-co2-emission-standards-for-cars-and-vans-post-euro6vi-emission-standards.

Geoffroy Ondet. « Microsoft va augmenter le prix de son abonnement Microsoft 365 ». Applis & Logiciels. 01net, 17 janvier 2025. https://www.01net.com/actualites/microsoft-augmente-prix-abonnement-microsoft-365.html.

Gilles Servient. Les pertes de souveraineté industrielle : cas d'école à la française. 12 décembre 2022. https://www.ege.fr/infoguerre/les-pertes-de-souverainete-industrielle-cas-decole-la-francaise.

Henri Martre. Rapport du Groupe « Intelligence économique et stratégie des entreprises ». Commissariat Général du Plan, 1994.

Jacqueline Sala. « Entretien. Bernard Besson analyse les apports du Rapport Martre. "Intelligence économique et stratégie des entreprises" ». www.veillemag.com, s. d. https://www.veillemag.com/Entretien-Bernard-Besson-analyse-les-apports-du-Rapport-Martre-Intelligence-economique-et-strategie-des-entreprises_a4748.html.

Jules BOITEAU. « Info ou intox - Le Rafale victime d'une campagne de dénigrement dans la sinosphère ». Asie-Pacifique. France 24, 2 juillet 2025. https://www.france24.com/fr/%C3%A9missions/info-ou-intox/20250702-l-avion-fran%C3%A7ais-rafale-victime-d-une-campagne-de-d%C3%A9nigrement-de-la-sinosph%C3%A8re.

Keren Lentschner. « Guerre commerciale : les Gafam au cœur du bras de fer transatlantique ». Conjoncture. Le Figaro, 2 avril 2025. https://www.lefigaro.fr/conjoncture/guerre-commerciale-les-gafam-au-coeur-du-bras-de-fer-transatlantique-20250402.

Laurie Clarke. « Mike Lynch yacht disaster: Missing tycoon's ties to UK spy chiefs ». Politico, 20 août 2024. https://www.politico.eu/article/missing-tech-tycoon-mike-lynchs-ties-to-uk-spy-chiefs/.

Lucas Mediavilla. « Les législations européennes sur le numérique «ne feront pas l'objet d'un marchandage» avec Trump, assure Bercy ». Tech & Web. Le Figaro, 10 avril 2025. https://www.lefigaro.fr/secteur/high-tech/le-dsa-et-le-dma-ne-feront-pas-l-objet-d-un-marchandage-avec-donald-trump-assure-bercy-20250410.

Manifeste souveraineté technologique l'autonomie stratégique. Innovator Makers Alliance, 2025. https://www.illuin.tech/wp-content/uploads/2025/03/Manifeste_Souverainete-Technologique-lAutonomie-Strategique_Innovation-Makers-Alliance_2025.pdf.

Marie-Noëlle Lienemann et Jean-Baptiste Lemoyne. Rapport d'information fait au nom de la commission des affaires économiques sur l'intelligence économique,. Sénat, 2023. https://www.senat.fr/rap/r22-872/r22-8721.pdf.

Michel Canévet. CS Cybersécurité : compte rendu de la semaine du 10 février 2025. 2025. https://www.senat.fr/compte-rendu-commissions/20250210/cs_cyber.html.

Michel Canévet, Patrick Chaize, et Hugues Saury. au nom de la commission spéciale sur le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité (procédure accélérée),. Sénat, 2025. https://www.senat.fr/rap/l24-393/l24-3931.pdf.

Nicolas Moinet. « Le nouveau paradigme stratégique : compétition-contestation-affrontement ». IH2EF, 30 juin 2025. https://www.ih2ef.gouv.fr/le-nouveau-paradigme-strategique-competition-contestation-affrontement.

Nicolas Moinet. « L'intelligence économique, une culture du renseignement appliquée à l'entreprise ». Conflits : Revue de Géopolitique, 16 mars 2020. https://www.revueconflits.com/entreprise-renseignement-guerre-economique-abonne-nicolas-moinet/.

Nicole Buyse. « Le rêve américain contrarié de la jeune pousse lilloise Vade Secure ». Tech - Médias. Les Echos, 26 août 2021. https://www.lesechos.fr/tech-medias/hightech/le-reve-americain-contrarie-de-la-jeune-pousse-lilloise-vade-secure-1341199.

Panorama de la cybermenace 2024. ANSSI, 2025.

Patrick, Juignet. Néolibéralisme - De l'idéologie néolibérale à la pratique du gouvernement. 2020. https://philosciences.com/ideologie-neoliberale.

Philip Blenkinsop. « EU Brings Forward Review of 2035 Zero Emission Vehicles Target ». Climate & Energy. Reuters, 12 septembre 2025. https://www.reuters.com/sustainability/climate-energy/eu-brings-forward-review-2035-zero-emission-vehicles-target-2025-09-12/.

Philip Blenkinsop. « EU Gives Automakers "breathing Space" on CO2 Emission Targets ». Autos & Transportation. Reuters, 3 mars 2025. https://www.reuters.com/business/autos-transportation/eu-propose-giving-automakers-three-years-meet-co2-emission-targets-2025-03-03/.

Pierre Dardot, et Christian Laval. La nouvelle raison du monde. Essai sur la société néolibérale. La Découverte, 2010. https://doi.org/10.3917/dec.dardo.2010.01.

Pierre Sauveton. La guerre de l'ombre contre l'industrie de défense française. 16 mai 2025. https://fr.linkedin.com/pulse/5-la-guerre-de-lombre-contre-lindustrie-d%C3%A9fense-pierre-sauveton-rkbpe.

RISKINTEL MEDIA, réal. Cyberguerre d'état : entre discours et réalité. Riskintel média, 2023. 45:19. https://www.youtube.com/watch?v=_SbbrPQfSw0.

Stefano Valentino, Lorenzo Di Stasi, et James Jackson. « Comment le lobby automobile a enfumé l'Europe sur les normes anti-pollution des voitures ». Environnement. Libération, 7 novembre 2023. https://www.liberation.fr/environnement/comment-le-lobby-automobile-a-enfume-leurope-sur-les-normes-anti-pollution-des-voitures-20231107_VROAW4FKQFEJHKGAZRBO4NRR6I/.

WEF Global Cybersecurity Outlook 2025. WEF, 2025. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf.

Yannick Pech. « Intelligence cyber : intégrer les hackers dans une stratégie de sécurité numérique globale. Le modèle de l'intelligence économique ». Université de Poitiers, 2023. https://hal.science/tel-04563954.

Yoann Bourgin. « L'antivirus russe Kaspersky désormais banni des agences gouvernementales australiennes ». usine digitale, www.usine-digitale.fr, 24 février 2025. https://www.usine-digitale.fr/article/l-antivirus-russe-kaspersky-desormais-banni-des-agences-gouvernementales-australiennes.

Partie 3

Alain Juillet. « Commande publique : audition d'Alain Juillet ». 8 avril 2025. Sénat. https://videos.senat.fr/video.5274762_67f579d885772.commande-publique--audition-dalain-juillet.

Aurélie Lebelle. « « Un marché multiplié par deux en trois ans » : les câbles sous-marins, un business fructueux pour la France ». /Economie/Business/. Le parisien, 18 janvier 2025. https://www.leparisien.fr/economie/business/un-marche-multiplie-par-deux-en-trois-ans-les-cables-sous-marins-un-business-fructueux-pour-la-france-18-01-2025-QY7LYRL5KBEOZGTOJSAX7W2PCQ.php.

Bertrand Lemaire. « La France veut renforcer son leadership numérique ». DÉCIDEURS IT. Républik IT Le Média, 26 mars 2024. https://www.republik-it.fr/decideurs-it/gouvernance/la-france-veut-renforcer-son-leadership-numerique.html.

Camille Auchère. « Marseille, plaque tournante du trafic Internet entre l'Afrique et le reste du monde ». Futura, 17 mai 2024. https://www.futura-sciences.com/tech/actualites/internet-marseille-plaque-tournante-trafic-internet-afrique-reste-monde-113484/.

Carine Guillemet. « Quentin Adam invité de Micode dans l'émission Underscore_ ». Clever Cloud, 27 mars 2025. https://www.clever-cloud.com/fr/blog/entreprise/2025/03/27/quentin-adam-invite-de-micode-dans-lemission-underscore_/.

Clara Chappaz. « Cybersécurité : audition de Clara Chappaz ». 2025. Sénat. https://videos.senat.fr/video.4986271_679762adce8d6.cybersecurite--audition-de-clara-chappaz.

« Cybersécurité : la Cour des comptes alerte sur la vulnérabilité persistante des systèmes civils en France ». Breizh-info, 18 juin 2025. https://www.breizh-info.com/2025/06/18/248198/cybersecurite-la-cour-des-comptes-alerte-sur-la-vulnerabilite-persistante-des-systemes-civils-en-france/.

Etude Asteres La dépendance technologique aux services de cloud et logiciels americains. Asterès, 2025. https://www.cigref.fr/wp/wp-content/uploads/2025/04/Etude-Asteres-La-dependance-technologique-aux-services-de-cloud-et-logiciels-americains-avril-2025.pdf.

Fabrice Deblock. « Cybersécurité : l'image de la France sur la scène internationale monte en puissance ». INCYBER NEWS, 30 novembre 2022. https://incyber.org/article/cybersecurite-limage-de-la-france-sur-la-scene-internationale-monte-en-puissance/.

Jean-Marc Joannès. « Alerte rouge sur les achats publics de solutions numériques ». achatpublic.info, 9 mai 2025. https://www.achatpublic.info/actualites/editos/2025/05/01/alerte-achats-publics-solutions-numeriques-souverainete-commande-publique-36140.

Jérôme Valat. « La Commission européenne continue de clouer le cercueil de l'innovation numérique ». Le monde, 7 mai 2024. https://www.lemonde.fr/idees/article/2024/05/07/la-commission-europeenne-continue-de-clouer-le-cercueil-de-l-innovation-numerique_6232047_3232.html.

Julia Voo, Irfan Hemani, et Daniel Cassidy. « National Cyber Power Index 2022 ». Belfer Center, 2022. https://www.belfercenter.org/publication/national-cyber-power-index-2022.

Juliette Françaix. « France 2030 : un nouvel appel à projet et 12 lauréats pour renforcer l'offre industrielle en matière de cybersécurité ». Presse - Ministère des Finances, 22

novembre 2024. https://presse.economie.gouv.fr/france-2030-un-nouvel-appel-a-projet-et-12-laureats-pour-renforcer-loffre-industrielle-en-matiere-de-cybersecurite/.

Keren Lentschner. « IA, cybersécurité, agroalimentaire… Comment la tech israélienne résiste à l'épreuve de la guerre ». Entreprises. Le Figaro, 16 février 2025. https://www.lefigaro.fr/societes/ia-cybersecurite-agroalimentaire-comment-la-tech-israelienne-resiste-a-l-epreuve-de-la-guerre-20250216.

L, Kenza. « GAFAM en Europe : la souveraineté numérique européenne en péril ». Portail de l'IE, 5 décembre 2024. https://www.portail-ie.fr/univers/2024/gafam-en-europe-la-souverainete-numerique-europeenne-en-peril/.

« La France, leader européen dans la préparation à l'IA selon Oxford Insights (A. Hié, Excelia) ». News Tank Éducation & Recherche, s. d. Consulté le 1 novembre 2025. https://education.newstank.fr/article/view/383496/france-leader-europeen-preparation-ia-selon-oxford-insights-hie-excelia.html.

« La guerre informationnelle des GAFAM pour conserver leur hégémonie numérique en Europe ». Ecole de Guerre Economique, 19 mai 2025. https://www.ege.fr/infoguerre/la-guerre-informationnelle-des-gafam-pour-conserver-leur-hegemonie-numerique-en-europe.

« L'aménagement numérique des territoires ». Arcep, s. d. Consulté le 1 novembre 2025. https://www.arcep.fr/nos-sujets/lamenagement-numerique-des-territoires.html.

Laurent Lagneau. « Otan : La France remporte l'édition 2019 de l'exercice de cyberdéfense Locked Shields ». Zone Militaire, 13 avril 2019. https://www.opex360.com/2019/04/13/otan-la-france-remporte-ledition-2019-de-lexercice-de-cyberdefense-locked-shields/.

Le pilotage transformation numerique-Etat par direction interministerielle du numérique. Cour des comptes, 2024. https://www.ccomptes.fr/sites/default/files/2024-07/20240710-S-2024-0754-Pilotage-transformation-numerique-Etat-par-direction-interministerielle-du-numerique.pdf.

« Le soutien à la transition numérique en France - Représentation en France ». Consulté le 1 novembre 2025. https://france.representation.ec.europa.eu/strategie-et-priorites/les-politiques-cles-pour-la-france/le-soutien-la-transition-numerique-en-france_fr.

« L'équipe franco-estonienne sur le podium de l'exercice international Locked Shields | Ministère des Armées ». 29 avril 2024. http://www.defense.gouv.fr/comcyber/actualites/lequipe-franco-estonienne-podium-lexercice-international-locked-shields.

Liste des recommandations de la commission d'enquête sur les coûts et les modalités de la commande publique. Sénat, 2025. https://www.senat.fr/fileadmin/cru-1750816532/Structures_temporaires/commissions_d_enquete/CE_Commande_publique/Liste_recommandations_CE_CP.pdf.

« Locked Shields – La France, première nation au classement de l'exercice de Cyberdéfense organisé par l'Otan | ANSSI ». 12 mai 2025. https://cyber.gouv.fr/actualites/locked-shields-la-france-premiere-nation-au-classement-de-lexercice-de-cyberdefense.

« Locked Shields 2025 : l'équipe franco-polonaise remporte la 2ème place | Ministère des Armées ». 12 mai 2025. http://www.defense.gouv.fr/comcyber/actualites/locked-shields-2025-lequipe-franco-polonaise-remporte-2eme-place.

Lucas Mediavilla. « Investissements massifs, sites sécurisés... En France, les projets de construction de data centers IA battent leur plein ». Tech & Web. Le Figaro, 29 octobre 2025. https://www.lefigaro.fr/secteur/high-tech/investissements-massifs-sites-securises-en-france-les-projets-de-construction-de-data-centers-ia-battent-leur-plein-20251029.

Manifeste souveraineté technologique l'autonomie stratégique. Innovator Makers Alliance, 2025. https://www.illuin.tech/wp-content/uploads/2025/03/Manifeste_Souverainete-Technologique-lAutonomie-Strategique_Innovation-Makers-Alliance_2025.pdf.

Margaux Vulliet. « Comment les Français sont devenus les rois de l'IA... dans la Silicon Valley ». BFMTV, 16 avril 2023. https://www.bfmtv.com/tech/intelligence-artificielle/comment-les-francais-sont-devenus-les-rois-de-l-ia-dans-la-silicon-valley_AV-202304160025.html.

Margaux Vulliet. « Quel avenir pour le cloud souverain européen ? » Tech - Numérique. Challenges, 11 janvier 2025. https://www.challenges.fr/entreprise/tech-numerique/quel-avenir-pour-le-cloud-souverain-europeen_595864.

Michaël Barthellemy, Catherine Morin-Desailly, et Olivier Bonnet de Paillerets. « Cyberdéfense : Airbus, Orange et Thales ». 11 février 2025. Sénat. https://videos.senat.fr/video.5040919_67ab8dadc65cb.cyberdefense--airbus-orange-et-thales.

Olivier Devillers. « Bonne élève de l'UE sur les infrastructures numériques, la France invitée à accélérer sur la formation et les entreprises ». Banquedesterritoires.fr. banque des territoire, 2 juillet 2024. https://www.banquedesterritoires.fr/bonne-eleve-de-lue-sur-les-infrastructures-numeriques-la-france-invitee-accelerer-sur-la-formation.

Philippe Leroy. « Luc Julia : « Les français sont les meilleurs du monde dans l'IA » ». Silicon, 7 février 2025. https://www.silicon.fr/Thematique/data-ia-1372/Breves/luc-julia-francais-meilleurs-monde-l-ia-467477.htm.

Qualité du droit : la surtransposition des directives européennes. 26 mars 2019. https://www.vie-publique.fr/en-bref/19813-qualite-du-droit-la-surtransposition-des-directives-europeennes.

rapport annuel cybercriminalite. COMCYBER-MI, 2025. https://www.interieur.gouv.fr//sites/minint/files/medias/documents/2025-07/rapport_annuel_cybercriminalite_2025-COMCyber_MI.pdf.

Résolution EUROPÉENNE visant à lutter contre les addictions numériques chez les enfants. Sénat, 2024. https://www.assemblee-nationale.fr/dyn/opendata/RIONANR5L17BTA0019.html.

Roger Romani. au nom de la commission des Affaires étrangères, de la défense et des forces armées sur la cyberdéfense. Sénat, 2025. https://www.senat.fr/rap/r07-449/r07-4491.pdf.

Simon Uzenat et Dany Wattebled. Les coûts et les modalités effectifs de la commande publique et la mesure de leur effet d'entraînement sur l'économie française,. Sénat, 2025.

« Souveraineté numérique de l'État : sortir de la dépendance technologique ». Antemeta, 25 juin 2025. https://www.antemeta.fr/souverainete-numerique-de-letat-sortir-de-la-dependance-technologique/.

Souveraineté numérique UE 2025 : l'Europe cherche à reprendre le contrôle face aux géants du numérique - L'Europe à Contre-Courant. REVUE DE PRESSE. 19 juillet 2025. https://europeacontrecourant.eu/europe-souverainete-numerique-ue-2025/.

« Souveraineté technologique : la France renforce ses ambitions européennes ». A2 Consulting, s. d. Consulté le 1 novembre 2025. https://a2consulting.fr/actualites/souverainete-technologique-la-france-renforce-ses-ambitions-europeennes/.

Stéphane Blanc, Jean-Noël Galzain, Dorothée Decrop, et Jérôme Lecat. « Commande publique : audition d'Hexatrust ». 30 avril 2025. Sénat. https://videos.senat.fr/video.5325612_681113606a372.commande-publique--audition-dhexatrust.

Thomas Fauré. Après Facebook, rebâtir. Nouvelles Editions De Passy, 2022.

Thomas Morel. « Comment l'État snobe les entreprises numériques françaises ». Valeurs actuelles, 18 juin 2025. https://www.valeursactuelles.com/clubvaleurs/economie/120-millions-pour-reinventer-la-roue-comment-letat-snobe-les-entreprises-numeriques-francaises.

Yoann Bourgin. « La France devient championne européenne des levées de fonds en cybersécurité ». Usine digitale, www.usine-digitale.fr, 7 mars 2025. https://www.usine-digitale.fr/article/la-france-devient-championne-europeenne-des-levees-de-fonds-en-cybersecurite.N2228586.

Partie 4

Chaste, Jonathan. « L'Intelligence économique au cœur des ressources humaines : une approche offensive ». Portail de l'IE, 22 juillet 2024. https://www.portail-ie.fr/univers/business-development-innovation-et-start-up/2024/lintelligence-economique-au-coeur-des-ressources-humaines-une-approche-offensive/.

Cyber Espionage. ENISA, 2020. https://www.enisa.europa.eu/sites/default/files/all_files/ETL2020%20-%20Cyber%20Espionage%20A4.pdf.

Fernandez, Alain. « Qu'est-ce que CMMI ? Le modèle de maturité pour la gouvernance du SI Capability Maturity Model Integration ». Management. Management et Performance, piloter.org, 22 septembre 2017. https://www.piloter.org/gouvernance/CMMI_gouvernance_SI.htm.

Girollet, Albane. « Protection du patrimoine informationnel : regard sur le cyber-espionnage ». Almond, 13 décembre 2022. https://almond.eu/cybersecurity-insights/protection-du-patrimoine-informationnel-regard-sur-le-cyber-espionnage/.

Les instantanés 2022. CESIN, 2022. https://cesin.fr/document.php?d=64a586188565c.

Maze, Taylor. « Qualitative vs. Quantitative Analysis for Cyber Risk: What's the Difference? » FAIR Institute, 29 octobre 2018. https://www.fairinstitute.org/blog/qualitative-vs.-quantitative-analysis-for-cyber-risk-whats-the-difference.

WEF Global Cybersecurity Outlook 2025. WEF, 2025. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf.

Partie 5

Partie 6

Grancer, Laurent. Matrice RACI. 15 juillet 2025. https://www.manager-go.com/gestion-de-projet/dossiers-methodes/matrice-raci.

Conclusion

Alain Juillet. Qu'est-ce que l'intelligence économique ? Document de travail. Sécrétariat général de la Défense nationale, 2004.

Beaufre, André. Introduction à La Stratégie. Hachette, 1998.

Annexes

Annexe 1. Recommandations de la Commission d'enquête sénatoriale sur la commande publique

Suite au cycle d'auditions menées par la commission d'enquête sénatoriale sur les coûts et les modalités de la commande publique au premier semestre de l'année 2025, un document contenant une liste de 67 recommandations a été publié. Sont présentées ci-dessous celles qui traitent de la souveraineté numérique en général, et la commande publique en particulier :

- **Recommandation n° 16**. – Transférer dans les meilleurs délais l'hébergement de la plateforme des données de santé, dite *Health Data Hub*, sur une solution souveraine, immune aux législations extraterritoriales, conformément à l'article 31 de la loi Sren ;
- **Recommandation n° 19**. – Instaurer, dans le cadre de la révision des directives européennes sur la commande publique, un principe général de préférence européenne dans les achats des personnes publiques ;
- **Recommandation n° 20**. – Instituer, à l'occasion de la révision des directives européennes sur la commande publique, un *Small Business Act* européen réservant aux PME une part d'au moins 30 %, en valeur, des marchés publics passés par l'ensemble des pouvoirs adjudicateurs ;
- **Recommandation n° 21**. – Dans le cadre du *Small Business Ac*t européen, réserver aux TPE et PME les marchés publics d'un montant inférieur au seuil des procédures formalisées pour les fournitures et les services et à 100 000 euros HT pour les travaux ;
- **Recommandation n° 22**. – Publier au plus vite le décret d'application de l'article 31 de la loi Sren qui respecte la volonté du législateur et en assurer la mise en œuvre effective ;
- **Recommandation n° 23**. – Élargir le périmètre des données considérées comme sensibles à l'ensemble des données produites ou détenues par des personnes publiques ;
- **Recommandation n° 24**. – Rendre obligatoire l'insertion d'une clause de non-soumission aux lois extraterritoriales étrangères dans tous les marchés publics comportant des prestations d'hébergement et de traitement de données publiques en cloud ;
- **Recommandation n° 25**. – Faire respecter le recours obligatoire à des offres disposant de la qualification **SecNumCloud** pour l'hébergement des données publiques d'une sensibilité particulière ;
- **Recommandation n° 26**. – Parmi les solutions qualifiées SecNumCloud, privilégier le recours à celles qui reposent sur des technologies **intégralement** souveraines ;
- **Recommandation n° 29**. – Rationaliser le pilotage de la politique numérique de l'État en réaffirmant le rôle de pilote de la direction interministérielle du numérique, sous l'autorité du Premier ministre, et en rappelant aux administrations de l'État le caractère obligatoire de la doctrine « cloud au centre » ;
- **Recommandation n° 59**. – Créer un parcours de formation certifiant sur l'achat et la souveraineté numériques.

Annexe 2. Textes à valeur juridique en lien avec la cybersécurité

Annexe 2.1. Textes d'origine française

	Nom du texte en lien avec la cybersécurité	Référence	Objet
1	Instruction interministérielle nº 2100 (1975)	II n° 2100/SGDN/SSD	Empêcher la compromission d'informations classifiées dématérialisées de l'OTAN traitées ou échangées via des systèmes d'information.
2	Loi sur la liberté de communication en ligne (LCEN)	Loi 2004-575 Décret 2007-663	Définir les modalités de contrôle domestique des moyens de cryptologie.
3	Référentiel général de sécurité	Ordonnance nº 2005-1516	Limiter la fraude liée à l'usage des services numériques de l'Administration.
4	Instruction générale interministérielle n° 2102 (2011)	IGI nº 2102/SGDSN/PSE/PSD	Empêcher la compromission d'informations classifiées dématérialisées de l'UE traitées ou échangées via des systèmes d'information.
5	Protection du potentiel scientifique et technique de la Nation (PPST)	Décret nº 2011-1425	Limiter la captation d'informations dans le domaine scientifique et technique pouvant affecter les intérêts de la Nation.
6	Instruction interministérielle nº 901 (2015)	II nº 901/SGDSN/ANSSI	Limiter la divulgation d'informations sensibles dématérialisées traitées ou échangées via des systèmes d'information.
7	Loi de Programmation militaire 2014-2019	Loi n° 2013-1168	Créer les exigences du code de la défense relatives au renforcement de la sécurité des systèmes d'information d'importance vitale (SIIV) mis en œuvre par les opérateurs d'importance vitale (OIV).
8	Loi de Programmation militaire 2019-2025	Loi n°2018-607	Imposer des obligations strictes aux OIV et OSE pour protéger les infrastructures critiques et moderniser les capacités numériques.
9	Instruction générale interministérielle n° 1300	Décret n° 2019-1271	Définir les exigences applicables aux informations et supports soumis au secret de la défense nationale (classifiés).
10	Instruction interministérielle nº 910	II nº 910/SGDSN/ANSSI	Définir les exigences relatives à la mise en œuvre et à la gestion des articles contrôlés de la sécurité des systèmes d'information.
11	Instruction interministérielle n° 300	II n° 300/SGDSN/ANSSI	Définir les exigences relatives à la protection contre les signaux compromettants.
12	Homologation de sécurité des SI de l'état	Décret n° 2022-513	Définir le cadre de gouvernance de la sécurité numérique des administrations et établissements publics d'État.

Annexe 2.2. Textes d'origine européenne

	Nom du texte en lien avec la cybersécurité	Type	Date d'entrée en vigueur
1	Règlement *Electronic Identification, Authentication and Trust Services* (eIDAS) (UE 2014/910)	Règlement	23 juillet 2014
2	Règlement général sur la protection des données (RGPD) (UE 2016/679)	Règlement	24 mai 2016
3	Directive sur la sécurité des réseaux et des systèmes d'information (NIS1) (UE 2016/1148)	Directive	8 août 2016
4	Règlement sur la cybersécurité (Cybersecurity Act) (UE 2019/881)	Règlement	27 juin 2019
5	Règlement sur la gouvernance des données (Data Governance Act) (UE 2022/868)	Règlement	23 juin 2022
6	Règlement sur les services numériques (Digital Services Act) (UE 2022/2065)	Règlement	16 novembre 2022
7	Directive sur la résilience des entités critiques (REC) (UE 2022/2557)	Directive	16 janvier 2023
8	Règlement sur la résilience opérationnelle numérique du secteur financier (DORA) (UE 2022/2554)	Règlement	16 janvier 2023
9	Directive sur des mesures destinées à assurer un niveau élevé commun en cybersécurité (NIS2) (UE 2022/2555)	Directive	16 janvier 2023
10	Directive sur la résilience opérationnelle numérique du secteur financier (DORA) (UE 2022/2556)	Directive	16 janvier 2023
11	Règlement « *e-evidence* » (UE 2023/1543)	Règlement	17 août 2023
12	Règlement sur les données (Data Act) (UE 2023/2854)	Règlement	7 janvier 2024
13	Règlement établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union (UE/Euratom 2023/2841)	Règlement	11 janvier 2024
14	Règlement Electronic Identification, Authentification and Trust Services 2 (eIDAS 2) (UE 2024/1183)	Règlement	20 mai 2024
15	Règlement sur l'intelligence artificielle (AI Act) (UE 2024/1689)	Règlement	11 juillet 2024
16	Règlement sur la responsabilité du fait des produits défectueux (UE 2024/2853)	Règlement	9 décembre 2024
17	Règlement sur la cyber-résilience (Cyber Résilience Act, CRA) (UE 2024/2847)	Règlement	10 décembre 2024
18	Règlement sur la solidarité en matière de cybersécurité (Cyber Solidarity Act, CSA)	Règlement	4 février 2025

Annexe 3. Liste des acronymes et abréviations (par ordre alphabétique)

ACPR : Autorité de contrôle prudentiel et de résolution

ANSSI : Agence nationale de la sécurité des systèmes d'information

APT : Advanced persistant threat

BIA : Business impact analysis ou Analyse d'impact sur les Entreprise

CA : Conseil d'administration

CERT : Computer emergency response team

CIGREF : Club informatique des grandes entreprises françaises

CISO : Chief information security officer

CMDB : Configuration management database

COMCYBER-MI : Commandement du ministère de l'Intérieur dans le cyberespace

COMEX : Comité exécutif

CRA : Cyber Resilience Act

CSO : Chief security officer (directeur de la sécurité)

CTI : Cyber threat intelligence (renseignement d'intérêt cyber)

CTO : Chief technical officer (directeur technique)

DAF : Direction des affaires financières

DINUM : Direction interministérielle du numérique

DoD : Department of defense (département de la défense)

DORA : Digital operational resilience act

ESN : Entreprise de services numériques

ETI : Entreprise de taille intermédiaire

GCHQ : Governement communications headquarters

IE : Intelligence économique

JUNALCO : Juridiction nationale de lutte contre la cybercriminalité

KPI : Key point indicator

LPM : Loi de programmation militaire

MI5 : Military intelligence, section 5

NSA : National security agency

NIS : Network and information system security

OFAC : Office français anti-cybercriminalité

OIV : Opérateur d'importance vitale

PCA : Plan de continuité d'activité

PDCA : Plan-do-check-act (planifier-faire-contrôler-améliorer)

PRA : Plan de reprise d'activité

RGPD : Règlement général sur la protection des données

RSSI : Responsable de la sécurité des systèmes d'information

SEI : Software engineering institute

SGDSN : Secrétariat général de la défense et de la sécurité nationale

SIGINT : Signal intelligence (intelligence d'origine électromagnétique)

SISSE : Service de l'information stratégique et de la sécurité économiques

SLA : Service level agreement

SMQ : Système de management de la qualité

SMSI : Système de management de la sécurité de l'information

SOC : Security operation center

Tiering : Le modèle de Tiering de l'ANSSI

UNC : Unité nationale cyber

VUCA : Volatility, uncertainty, complexity and ambiguity (Volatilité, incertitude, complexité et ambiguïté)

WEF : World economic forum

Annexe 4. Les auteurs de ce mémoire

Ce mémoire a été rédigé au cours de l'Exécutif MBA en **Management de la Cybersécurité et Gouvernance des Systèmes d'Informations** de l'**Ecole de Guerre Economique**. Les auteurs font partie de la promotion MaCyb07, d'octobre 2024 à septembre 2025.

François Delignette, Manager de transformation au sein de Musubi Consulting

François Delignette, certifié PMP® depuis 2005 et PMI-ACP® depuis 2016, est diplômé de Polytech Nancy (Ex ESSTIN) en 1991 et diplômé de l'Exécutive MBA des Ponts et Chaussées en 2010.

Après un VSNE au Portugal et d'autres expériences à l'international, il devient, en 1995, consultant indépendant pendant 17 ans à Paris.

Par la suite, il rejoint le cabinet Daylight de 2012 à 2023. Daylight Consulting est un cabinet de conseil spécialisé en Projet, Programme, Portefeuille et Agilité. Daylight Consulting a rejoint le groupe Blue Soft en 2018 pour devenir ultérieurement Blue Soft Consulting.

Courant 2023, il crée son propre cabinet de conseil, Musubi Consulting dédié aux projets de transformations des entreprises.

Il démarre fin 2024 son Exécutive MBA en Management de la Cybersécurité à l'EGE. Il est certifié ISO 27001 LI et EBIOS Risk Manager.

Cuneyt KAYA, Bid & Engineering Project Manager, Thales

Fort de plus de 13 ans d'expérience en ingénierie système et gestion stratégique de projets technologiques complexes, il intervient sur des programmes d'envergure mêlant innovation, transformation et performance organisationnelle.

Ses domaines d'intervention couvrent notamment la gestion de projets critiques, la cybersécurité, le cloud, l'ingénierie système, le pilotage budgétaire et la maîtrise des risques. Il accompagne les organisations dans la conception, la sécurisation et l'optimisation de solutions complexes, tout en alignant enjeux business et stratégies technologiques. Il poursuit actuellement le programme Exécutive « Strategic Management » à HEC Paris.

Il est certifié PMP®, AWS® Cloud, PECB® ISO/IEC 27001 Lead Implementer et ANSSI® EBIOS Risk Manager.

Matthieu Rousseau, Gendarmerie Nationale

Officier Saint-cyrien diplômé de l'Enseignement Supérieur du second degré, titulaire de deux MBA (Security Management ; Cybersecurity Management) et des certifications ISO/IEC 27001 LI ANSSI® EBIOS Risk Manager, il a successivement exercé, pendant 13 années, des fonctions de commandement au sein de la Légion Étrangère et de la gendarmerie nationale. Après cinq années dans la Légion étrangère, notamment marquées par deux années en Guyane (lutte contre l'orpaillage illégal et protection du Centre spatial), il a commandé pendant quatre années un escadron de gendarmerie mobile au cours desquelles il a été engagé dans les principaux troubles à l'ordre public (Nouvelle-Calédonie, Notre-Dame des Landes, Gilets Jaunes…). A l'été 2020, il a pris le commandement de la compagnie de gendarmerie départementale de Chartres où il a de nouveau été confronté à des troubles à l'ordre public et des enquêtes judiciaires complexes (criminalité organisée, homicides…).

Conscient des enjeux liés à la cybercriminalité, il aide depuis 2024 les services publics, les collectivités territoriales ainsi que les TPE/PME à bâtir leur cyber-résilience, en développant notamment leurs capacités de gestion de crises d'origine cyber. Un enjeu majeur dans un monde où l'attaque numérique n'est plus une hypothèse, mais une certitude...

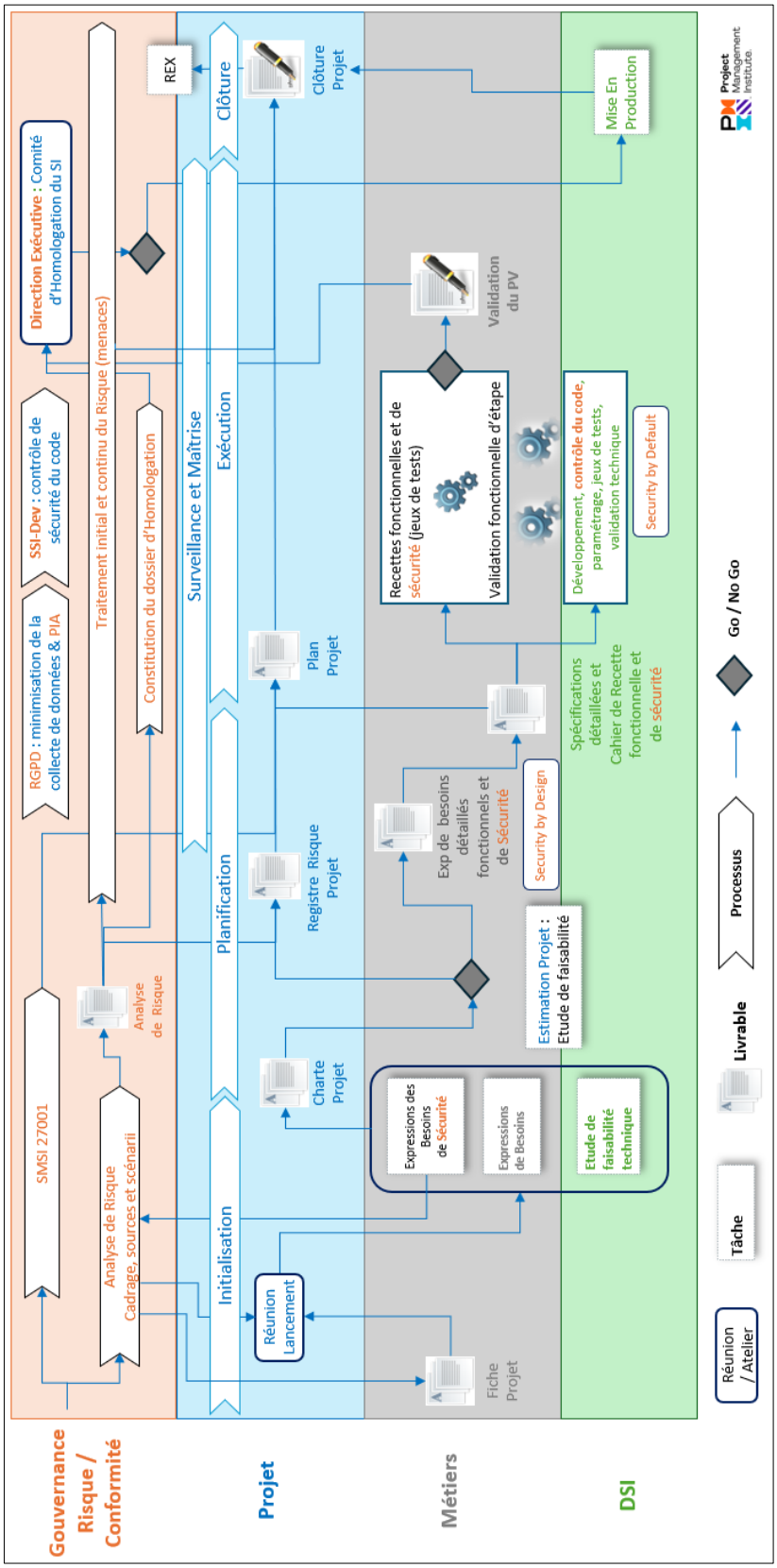
Guillaume Turlan, Armée de l'Air et de l'Espace

Athlète de classe internationale, il a construit une carrière sportive marquée par deux participations aux Jeux Olympiques (2020, 2024) couronnée par une 8-ème place au Jeux de Paris 2024. Multimédaillé sur la scène internationale, son parcours se distingue par une exigence constante, une discipline exemplaire et une capacité durable à performer au plus haut niveau.

En parallèle de cette trajectoire sportive d'exception, il a développé une carrière dans le domaine du DevOps au sein de l'Armée de l'Air et de l'Espace. Cette expérience lui a permis d'acquérir une expertise opérationnelle solide dans des environnements techniques complexes et critiques. Soucieux d'élargir ses compétences dans le champ de la cybersécurité, il a poursuivi une spécialisation en analyse de risques cyber, est titulaire d'un MBA en Cybersecurity Management, et détient les certifications ANSSI® EBIOS Risk Manager ainsi que ISO/IEC 27001 Lead Implementer.

Ce double parcours, à la croisée du sport de haut niveau et de l'ingénierie informatique, illustre sa capacité à évoluer dans des univers exigeants, à conjuguer performance, précision et résilience, et à mobiliser une expertise plurielle pour répondre à des enjeux stratégiques tant physiques que numériques, au service de la France.

Annexe 5. Chronogramme des processus de gouvernance



L’Intelligence économique comme facteur de performance de la cybersécurité

La pensée stratégique occidentale du vingtième siècle a accouché de la « stratégie totale » : un modèle où toutes les forces d’une nation ont un rôle à jouer, le principe de sûreté permettant d’empêcher l’adversaire de restreindre la liberté d’action. Transposé au contexte de l’économie contemporaine, la stratégie de cybersécurité contribue à la sûreté de l’entreprise et crée de la liberté d’action. Toutefois, la méthodologie de l’intelligence économique révèle un état de guerre économique et démontre que l’approche prévalente en cybersécurité, dite « technico-financière », crée des dépendances restreignant *in fine* cette liberté d’action. L’intelligence économique renseigne également sur les solutions possibles pour que la cybersécurité contribue toujours mieux à la liberté d’action de l’entreprise, dont la recherche d’une souveraineté numérique au premier chef. Afin de guider les entreprises dans cette démarche d’intégration de l’intelligence économique à leur stratégie de cybersécurité, ce document propose une échelle de maturité cyber rénovée particulièrement novatrice. En effet, en s’appuyant sur quatre axes complémentaires (cybersécurité, intelligence économique, organisation, positionnement de l’entreprise), elle calcule le cyber score stratégique de l’entreprise et pourrait amener également à améliorer de cadre de gouvernance de cybersécurité et des transformations de l’entreprise.

Mots-clés : Intelligence économique, entreprise, cybersécurité, stratégie totale, stratégie, gouvernance, guerre économique, souveraineté numérique, modèle de maturité, cyber score stratégique, cadre de gouvernance.

Competitive intelligence as a cybersecurity performance factor

Western strategic thinking in the twentieth century gave rise to the concept of ‘total strategy’: a model in which all of a nation's forces have a role to play, with the principle of security preventing the adversary from restricting freedom of action. Transposed to the context of the contemporary economy, cybersecurity strategy contributes to corporate security and creates freedom of action. However, competitive intelligence methodology reveals a state of economic warfare and demonstrates that the prevailing ‘technical-financial’ approach to cybersecurity creates dependencies that ultimately restrict this freedom of action. Competitive intelligence also provides information on possible solutions to ensure that cybersecurity contributes ever more effectively to the company's freedom of action, including the pursuit of digital sovereignty in the first instance. In order to guide companies in this process of integrating competitive intelligence into their cybersecurity strategy, this document proposes a particularly innovative, updated cyber maturity scale. Based on four complementary axes (cybersecurity, economic intelligence, organization, and company positioning), it calculates the company's strategic cyber score and could also lead to improvements in cybersecurity governance frameworks and company transformations.

Keywords : Competitive intelligence, company, cybersecurity, total strategy, strategy, governance, economic warfare, digital sovereignty, maturity model, strategic cyber score, governance framework.