LIVRE BLEU

TABLE DES MATIERES

Nous avons accepté de préfacer le « Livre Bleu » du GINUM car nos missions de défense, de sécurité et de délivrance de service vitaux traitent quotidiennement de la maitrise des outils numériques que nous mettons en œuvre. La démarche, partant des besoins métiers pour identifier les dépendances et proposer une action globale visant à faire émerger des solutions souveraines nationales ou européennes, est vitale. La crise du COVID et, plus récemment, la situation dramatique en Ukraine démontrent, s'il en était besoin, l'impérieuse nécessité de maitriser notre autonomie dans ce domaine stratégique du numérique.

Général de Corps d'Armée **Frédéric Aubanel**, Chef du Service des Technologies et des Systèmes d'Information de la Sécurité intérieure (ST(SI)²), Ministère de l'Intérieur

La souveraineté est un des moyens de garantir une liberté d'action permettant le fonctionnement et la continuité de l'Etat en particulier dans les situations de crise. Pour les forces de sécurité, il s'agit d'être en tout temps en mesure d'assurer la protection de la population et des institutions. Le numérique étant de plus en plus central dans l'exécution des missions, la question de la maitrise de ces technologies, y compris en situation de crise de haute intensité, est majeure. Aussi, en tant que chef du ST(SI)², je me dois de rechercher des solutions techniques et de mettre en place des équipes en mesure de les maitriser en toutes circonstances. La démarche originale du GIMUM peut contribuer à faire émerger des solutions techniques souveraines correspondant à nos besoins. Les premières orientations proposées par le Livre Bleu vont dans ce sens et peuvent contribuer à développer une dynamique d'intérêts communs entre les acteurs publics et privés.

Ingénieur Général de l'Armement de première classe **Dominique Luzeaux**, Directeur de l'agence numérique de la défense (AND), Ministère des Armées

Affirmer notre souveraineté numérique pour exercer notre autonomie stratégique suppose d'avoir le choix entre différentes solutions technologiques viables industriellement et économiquement. En tant que Directeur de l'Agence du numérique de la défense, je suis chargé de la mise en œuvre de la politique industrielle dans le domaine des technologies numériques des systèmes d'information. La démarche du GINUM basée sur une approche métier, m'apparait très intéressante. Elle apporte une dynamique sectorielle en créant une synergie entre les intervenants de toute taille et en proposant de la valeur à la politique industrielle nationale. Le Livre Bleu, en fixant des axes de réflexions très concrets et en couvrant des thématiques vastes, lance une approche originale que je vais suivre avec intérêt.

Vincent Niebel, Directeur des Systèmes d'Information, Groupe EDF

La souveraineté du numérique doit adopter une approche de bout en bout pour s'assurer de la prise en compte de l'ensemble des éléments de l'écosystème. Pour ce faire, trois capacités sont au centre de la résilience et de la continuité du service : les infrastructures, la pile logicielle et les données. Les acteurs d'importance vitale œuvrant dans des secteurs fortement concurrentiels doivent garantir un équilibre toujours délicat entre la performance technique et commerciale, indispensable pour rester compétitif, et les investissements nécessaires pour conserver dans le temps la maitrise stratégique de notre périmètre. Le Livre Bleu du GINUM apporte une contribution intéressante à la définition d'une stratégie intégrée en prenant en compte les particularités de chacun des intervenants de ces secteurs et, souhaitons-le, nous permettre de disposer à terme de solutions techniques souveraines alliant performance technique et efficacité économique.

LE MOT DE LA PRÉSIDENTE

Avec la parution de la première édition de son Livre Bleu, le GINUM, Groupement des Intervenants du Numérique pour la défense, la sécurité et les enjeux d'importance vitale, franchit une étape importante de sa jeune existence que nous sommes fiers de partager avec vous.

Ce Livre Bleu est le reflet du **travail collectif** réalisé par nos adhérents et d'entretiens auprès d'acteurs étatiques, académiques, industriels. Il est construit autour d'une approche des enjeux de souveraineté numérique par les besoins métier (Défense, sécurité et enjeux d'importance vitale) et propose une méthodologie permettant de définir, pour chacun de ces métiers, les degrés de liberté d'action nécessaires en regard des besoins opérationnels et du niveau de souveraineté requis.

Sur ces bases, il présente **19 axes de réflexion** autour de quatre sujets essentiels en matière de numérique souverain et responsable : la mise en œuvre effective d'une stratégie industrielle, un numérique innovant et respectueux de nos valeurs en matière environnementale et éthique, la sécurisation des approvisionnements de bout en bout et la gestion des compétences.

C'est volontairement que le GINUM a choisi d'utiliser le terme « axe de réflexion » et non « proposition » pour bien marquer qu'avec cette première édition, nous ne sommes qu'au début d'un chemin. Nous invitons tous les acteurs intéressés (étatiques, représentants des OIV, futurs adhérents, académiques, syndicats) à se joindre à nos travaux futurs pour **construire ensemble** un numérique souverain et responsable au profit de la Défense, de la Sécurité et des enjeux d'importance vitale.

Dans ce cadre, le GINUM va lancer prochainement plusieurs groupes de travail thématiques (autour des métiers et des quatre sujets évoqués ci-dessus). Nous serons ravis de vous y retrouver afin que nous puissions élaborer ensemble des propositions concrètes qui viendront constituer une deuxième édition du Livre Bleu qui sera publiée dans le courant de l'année 2022.

Enfin, le GINUM a l'ambition de porter très rapidement nos réflexions au niveau européen car, comme le confirme la crise majeure que nous traversons actuellement, l'affirmation d'un modèle de numérique souverain et responsable, différenciant et pleinement assumé, est incontournable pour construire une Europe du numérique.

Bonne lecture !

Nadine Foulon-Belkacémi
Présidente du GINUM
Directrice Executive Grands Clients – Orange Business Services

INTRODUCTION

La numérisation croissante de la société révolutionne le besoin d'accès, la disponibilité et l'utilisation de produits et services technologiques vitaux pour la Nation. Cette révolution numérique constitue, certes, une nouvelle opportunité de performance mais est également un multiplicateur des menaces d'aujourd'hui et de demain, où les préoccupations liées au secteur marchand rejoignent souvent l'intérêt général.

Le GINUM souhaite fédérer les acteurs du numérique qui œuvrent pour la défense, la sécurité et les enjeux d'importance vitale autour d'une ambition souveraine et responsable. L'effet majeur de la souveraineté pour le GINUM consiste à atteindre l'autonomie stratégique, c'est-à-dire la capacité à choisir nos dépendances, au niveau national et européen, dans ces domaines critiques. Sur le plan opérationnel, cette capacité conditionne la liberté d'action des décideurs politiques et industriels, et des forces de défense et de sécurité.

Le GINUM, dans une approche globale, vise à renforcer la résilience et la performance de l'ensemble des composantes du numérique (approvisionnement, distribution, accès et utilisation).

Ainsi, dans un premier temps (chapitre 1), le GINUM expose sa vision des enjeux de souveraineté liés au numérique sur ces sujets critiques. Partant des objectifs métier, il propose une cartographie des libertés d'action et de décision à préserver dans le temps, et une méthode d'analyse destinée à prioriser les objectifs en termes de solutions souveraines.

Dans un second temps (Chapitres 2 à 5), il présente des premiers axes de réflexion, organisés autour de quatre thématiques, pour atteindre progressivement cette autonomie stratégique.

CHAPITRE 1 : CARTOGRAPHIE DE LA LIBERTÉ D'ACTION DU NUMÉRIQUE

La pandémie du COVID-19 a rappelé les risques intrinsèques d'une interdépendance toujours plus forte entre les acteurs d'une économie mondialisée. En parallèle, l'incertitude pesant sur la scène internationale, de la crise ukrainienne aux tensions taiwanaises, amène à questionner la capacité nationale et européenne à relever de manière autonome les défis de demain pour conserver la **liberté d'action**.
[1]

> *"Souvenez-vous de vous méfier et même de l'évidence, elle passe son temps à changer1."*
>
> **Jean d'Ormesson**

L'autonomie stratégique de la France demeure un objectif prioritaire de sa politique de défense et de sécurité nationale, car elle conditionne l'exercice de sa souveraineté et de sa liberté d'action.

Toutefois, les ressources fondant cette liberté d'action s'érodent, notamment sous l'effet de la vulgarisation de technologies disruptives. Celles-ci permettent à certains acteurs de menacer des secteurs critiques pour la résilience de l'Etat, avec des moyens jusqu'alors réservés aux grandes puissances.

Face à cette menace, chaque organisation, étatique ou non étatique, aspire donc à se doter des moyens pour imposer, ou tout du moins conserver, sa liberté de choix et d'action.

A) Approche par métier de la liberté d'action vis-à-vis du numérique

La liberté d'action, au sens d'autonomie d'action et de décision, diffère en fonction des métiers car les enjeux, les objectifs, les contraintes et les risques sont bien évidemment distincts. A l'aube du XXI^{e} siècle, le numérique et les technologies disruptives sont présents dans l'ensemble des activités humaines et constituent un facteur multiplicateur de risques. Les menaces traditionnelles (terrorisme, délinquance, désinformation, etc.) utilisent le numérique comme un nouveau vecteur avec un fort effet d'amplification pour atteindre leur finalité.
Le GINUM propose donc de présenter, pour chacun des domaines, sa perception des libertés de décision et d'action indispensables à l'exercice de leurs missions.

[1] Jean d'Ormesson, C'était bien, Gallimard, 2003

Le domaine de la défense

La compréhension par le GINUM des besoins de souveraineté du numérique pour le domaine de la défense se fonde sur la revue stratégique de défense et de sécurité nationale[2] (2017), la revue stratégique cyberdéfense[3] (2018), la vision stratégique du chef d'état-major des armées[4] (2021) et les rapports législatifs décrivant l'environnement dans lequel évoluent les forces armées. Ces documents structurent les orientations pour un modèle d'armée équilibré et complet. Les forces armées doivent disposer des capacités pour répondre à des engagements dans un contexte de compétition, de contestation, voire d'affrontement direct, incluant le combat de haute intensité et de continuum entre défense et sécurité.

Les forces doivent donc pouvoir participer à la résilience de l'État. Elles doivent agir simultanément et de manière coordonnée dans les cinq milieux et les deux champs définis : terre, air, mer, espace exo-atmosphérique, cyberespace, champs informationnel et électromagnétique. Elles contribuent aux facteurs de supériorité opérationnelle que sont, en particulier, la performance du commandement, la compréhension, l'agilité et l'influence.

Le domaine de la sécurité intérieure

La compréhension par le GINUM des besoins de souveraineté dans le domaine du numérique du ministère de l'Intérieur se fonde, tout d'abord, sur le livre blanc de la sécurité intérieure[5] (2021), lequel définit un pacte de protection et de sécurité des Français au regard des enjeux du XXIe siècle. Elle a, de plus, été complétée par des entretiens, avec des intervenants en charge de la stratégie numérique du ministère et des systèmes d'information et de communication de la Police et de la Gendarmerie.

Le domaine des activités d'importance vitale

Les opérateurs d'importance vitale (OIV) contribuent à la production et à la distribution de biens et services indispensables au fonctionnement de l'État. Exploitant des installations vitales à la résilience de la Nation, ces organismes se doivent de garantir un niveau de protection adéquat pour répondre aux menaces et assurer leur résilience en cas de crise. La continuité de ces services vitaux impose donc une maîtrise des infrastructures et des technologies. Tous ces éléments sont définis dans le cadre de la loi de programmation militaire (LPM 2019)[6].

---

[2] Ministère de la défense, *Revue stratégique de défense et de sécurité nationale,* La Documentation Française, 2017.
[3] Secrétariat général de la défense et de la sécurité nationale (SGDSN), *Revue stratégique de cyberdéfense,* 2018.
[4] Ministère des armées, La vision stratégique du chef d'état-major des armées, 2021.
[5] Ministère de l'intérieur, Livre *blanc de la sécurité intérieure,* 2020.
[6] LOI no 2018-607 du 13 juillet 2018 relative la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense.

Le numérique est au cœur de toutes les missions de ces trois domaines (Armées, Intérieur et OIV) et impacte fortement ces dernières. Dans la suite de ce chapitre, le GINUM s'attache à identifier les enjeux de ces domaines en matière de numérique pour conserver leur liberté d'action et ce au regard de **plusieurs axes métiers** : le lien de confiance avec la population, la gestion de crise, la protection de la population et l'efficacité de l'action des acteurs de défense et de sécurité.

Renouvellement du lien de confiance avec la population

L'omniprésence du numérique et, notamment, des réseaux sociaux dans la vie quotidienne des citoyens, a totalement modifié le rapport entre l'individu et l'Etat et particulièrement les forces de sécurité. L'espace numérique, lieu de confrontation d'idées, est devenu un outil de communication majeur qui tend à supplanter les médias traditionnels. Il est donc impératif que cet outil reste, en toute circonstance, libre d'accès. Il est aussi un des lieux privilégiés de remise en cause de l'Etat et de délitement du lien de confiance des citoyens à son égard. Les institutions doivent pouvoir faire face aux déstabilisations qui proviendraient notamment de pays étrangers.

Le renouvellement de la confiance avec le citoyen passe également par une capacité à protéger les données sensibles, à en garantir la validité et la non-usurpation. Ceci concerne autant l'identité numérique de nos concitoyens que les nombreuses données sensibles et stratégiques de l'Etat et des OIV : leur protection et la transparence de leur gestion sont des enjeux majeurs pour garantir la confiance de la population. L'emploi dans ce cadre de solutions techniques pleinement maîtrisées est donc indispensable.

Gestion des crises

Dans tout type de crise, les **capacités à communiquer** entre les acteurs, à fiabiliser les informations nécessaires à la prise de décision et à diffuser les ordres, sont centrales. L'ensemble de ces actions ne peut se concevoir sans des outils numériques fiables et maitrisés.

La dimension polymorphe des crises susceptibles d'être prises en compte (catastrophes naturelles, mouvements sociaux, attentats, crises sanitaires, etc.) multiplie le nombre d'acteurs. L'interaction entre ceux-ci passe donc par des solutions numériques interopérables, sécurisées et maitrisées.

L'espace numérique est également, dans ces circonstances, un vecteur de communication opérationnel majeur vers la population dont la disponibilité ne saurait être entravée et l'intégrité des informations institutionnelles mise à mal. Là encore, la libre disposition et la maîtrise de ces outils sont majeures.

Protection de la population

L'espace numérique doit être considéré comme un **nouveau territoire** où nos concitoyens réclament un équilibre toujours délicat entre la liberté d'action, la demande de sécurité et de protection.

La criminalité a pleinement investi ce moyen d'action qui est souvent un **amplificateur** de leurs méfaits : c'est en particulier le cas de la cyber délinquance avec ses formes multiples (rançongiciels, cyber escroqueries, trafics d'armes et de stupéfiants, etc.).

Dans un autre registre, les organisations terroristes utilisent pleinement l'espace numérique qui est devenu un lieu de diffusion de leur idéologie, de recrutement de leurs membres et de communication envers le public et les autorités.

Pour combattre ces auteurs d'actions illicites, l'Etat et les OIV doivent, chacun dans leur domaine, déployer des moyens numériques appropriés, fiables, maitrisés sur le plan technique, et répondant aux exigences de légalité, mises en place par nos institutions démocratiques. Ces moyens garantissent un équilibre entre la protection des libertés individuelles et l'efficacité opérationnelle.

Garantir l'efficacité de l'action des acteurs de la sécurité intérieure

La possession et la mise en œuvre de moyens techniques avancés ont longtemps été le monopole de l'Etat et de ses forces de sécurité intérieure. Face à la démocratisation des technologies, ces moyens sont devenus pleinement accessibles à leurs adversaires (communications chiffrées, moyens d'observation comme les drones par exemple, etc.). De plus, l'évolution des technologies disponibles est de moins en moins portée par des décisions et des investissements étatiques mais par le marché auquel elles s'adressent.

Ainsi, l'enquête pénale et les preuves associées se fondent de plus en plus sur des données recueillies au travers des outils numériques utilisés par les délinquants ou générant des informations utiles. Le maintien dans le temps de cette capacité essentielle ne peut se concevoir sans une maîtrise minimale des réseaux 5G, et demain 6G, le tout dans un cadre légal correspondant à nos normes de droit et à la liberté d'action des forces.

La libre circulation des personnes et des biens au sein de l'Union européenne et le développement toujours plus important des échanges internationaux nécessitent une coopération renforcée avec nos partenaires, au premier lieu desquels les membres de l'espace Schengen.

Cette coopération se fonde notamment sur des outils communs favorisant l'échange d'informations d'identification et de traçabilité. La maîtrise de ces outils apparait donc comme un levier majeur d'efficacité.

Enfin, tout comme pour la gestion de crise, l'efficacité des forces de sécurité passe par leur capacité à interagir sur le terrain avec des partenaires toujours plus variés : les services de secours, les OIV, les polices municipales, les entreprises de sécurité privée, les polices des pays frontaliers, etc. Cette coordination opérationnelle passe essentiellement par des moyens de communication s'appuyant sur une **cohérence capacitaire** entre les acteurs. Là encore, la liberté d'action des forces dans la période de crise impose la maîtrise de ces technologies et des réseaux associés pour l'ensemble des intervenants.

Garantir l'efficacité de l'action des acteurs en opération militaire

La remise en cause du cadre international, accompagnée d'une compétition stratégique entre états et des "risques de la faiblesse[7]", favorise l'émergence de **modes d'actions hybrides** menaçant la sécurité internationale. L'engagement des forces militaires projetées en dehors du territoire national contribue à protéger les concitoyens français, défendre les intérêts stratégiques de la France et exercer nos responsabilités internationales.

Le brouillard de la guerre est dissipé par la supériorité décisionnelle sur les théâtres d'opérations. La connaissance situationnelle nécessite un renforcement de la disponibilité des systèmes d'information et de communication pour recueillir, analyser, décider et pour communiquer des informations, depuis les théâtres vers les centres de décision jusqu'au plus haut niveau.

Garantir l'efficacité de l'action dans l'espace numérique

Le numérique est devenu depuis plusieurs décennies un terrain d'affrontements et de contestations dont les vulnérabilités permettent à des acteurs étatiques et privés d'en exploiter les failles.

L'espace numérique est donc devenu un enjeu de souveraineté majeur dont la matière première, la donnée, véritable actif stratégique, constitue le cœur.

[7] Ministère de la Défense, *Livre blanc sur la défense et la sécurité nationale*, 2013, p39.

B) Méthodologie de travail proposée par le GINUM

Les moyens numériques utilisés pour répondre aux besoins des domaines de la défense, de la sécurité et des OIV reposent, pour bon nombre d'entre eux, sur des outils d'origines extra-européennes. Au regard de ce constat largement partagé par les intervenants du numérique, le GINUM propose une méthode de travail visant à se fixer des priorités. La finalité est la mise à disposition progressive de solutions technologiques souveraines destinées à garantir, dans le temps, la liberté d'action dans les secteurs essentiels à la résilience de la Nation.

Dans un premier temps, il convient de définir, par cercles concentriques, le niveau de sensibilité des missions et des moyens associés à ces dernières :

- **Impératif** : si le service n'est pas rendu, l'Etat et ses partenaires ne sont plus en mesure d'assurer la mission essentielle à la vie et à la continuité de la Nation, y compris de manière dégradée ;
- **Nécessaire** : la mission est sensible et la délivrance du service permet sa mise en œuvre dans de bonnes conditions. En revanche, si ce service est déficient, la continuité des services vitaux peut tout de même être assurée de manière dégradée en situation de crise ;
- **Souhaitable** : cela correspond aux services non indispensables en situation de crise, mais permettant un fonctionnement nominal.

Dans un second temps, une déclinaison plus technique des moyens à maîtriser pour permettre la fourniture de ces différents services de manière souveraine est à mener selon trois axes qui doivent intégrer, par construction, les enjeux de la cybersécurité :

- **Les infrastructures** sous toutes leurs formes : transport (réseaux fixes et mobiles (4G/5G), satellites, câbles sous-marins, etc.), stockage de données (data centers, clouds, etc.), objets connectés et capteurs divers,
- **Les applications** garantissant le fonctionnement des systèmes de commandement, les outils d'aide à la décision et de pilotage des infrastructures vitales**,**
- **Les données**, en se concentrant sur les données sensibles, classifiées ou non, sur les données d'intérêt stratégique et sur tout moyen contribuant à leur intégrité, à leur accessibilité et à leur traçabilité.

Cette double analyse permettra de définir un ensemble d'axes de travail destinés à construire les conditions d'une garantie de la liberté de décision et d'action pour les domaines de la défense, de la sécurité et des OIV, en particulier en situation de crise.

Pour illustrer la démarche d'analyse des missions selon l'approche des cercles concentriques, prenons le cas du ministère de l'Intérieur qui, dans son livre blanc, a fixé comme impératif opérationnel la capacité de fonctionnement des forces de sécurité intérieure et de sécurité civile dans le cadre de crises multiformes[8].

Cet impératif opérationnel se décline selon les axes techniques choisis comme suit :

- **Infrastructure** :
  Maîtrise des systèmes de communication de bout en bout à savoir les terminaux, le système central et les infrastructures de transport,
  Maîtrise du stockage des données sur un data center interne ou un cloud souverain,
- **Applicatif :**
  Maîtrise des applicatifs permettant le fonctionnement des salles de commandement,
- **Données :**
  Maîtrise de l'accès et de la traçabilité des données.

La **stratégie de préservation** de la liberté d'action répond à une logique proche de celle mise en œuvre à l'occasion de l'homologation des systèmes. En l'absence de solution technologique souveraine, des solutions de sécurisation de son emploi doivent être mises en œuvre.

Ces solutions de sécurisation reposent sur une combinaison de mesures à déterminer au cas par cas :

- Chiffrement, en prenant dès aujourd'hui en compte la problématique post-quantique (par exemple : le chiffrement homomorphe),
- Transparence des codes imposée aux fournisseurs,
- Durcissement des cadres règlementaires pour accéder à certains marchés concernant tant la défense que la sécurité et les OIV.

[8] Ministère de l'intérieur, Livre *blanc de la sécurité intérieure,* 2020, p119.

Le déploiement de ces solutions requiert que les organismes en charge de leur mise en œuvre disposent des **compétences internes** spécifiques, aujourd'hui encore trop rares. Ces organismes devront également être en mesure d'analyser les conséquences métier des technologies disruptives (cloud, intelligence artificielle, quantique, 5G SA, les réalités virtuelles et augmentées, le métavers, etc.).

De plus, les **politiques de soutien** des systèmes opérationnels apparaissent essentielles pour assurer leur durabilité dans des conditions de sécurité adaptées aux enjeux.

L'émergence de solutions souveraines impose donc le développement d'une **stratégie globale** exploitant l'ensemble des leviers, **tant au niveau national qu'européen**.

La stratégie doit se définir au regard de l'effet majeur recherché. Pour le GINUM, l'objectif est de garantir la liberté d'action au travers d'une maîtrise des outils numériques nécessaires à l'exécution des missions critiques, y compris dans l'espace numérique.

Pour la défense, la sécurité et les OIV, ancrés dans les obligations régaliennes, la « main invisible » du marché, pour reprendre le concept d'Adam Smith, ne suffit pas à assurer la liberté d'action. L'expérience montre, en effet, dans le secteur marchand, combien cette « main » contrarie notre souveraineté en France et en Europe.

La **stratégie industrielle** doit donc faciliter l'émergence d'une offre et de leviers nationaux et européens, garantissant la liberté d'action.

A) Les conditions d'émergence d'une offre industrielle

Le marché du numérique se compose d'une multitude d'acteurs de tailles très différentes ayant chacun un ensemble de compétences dans leurs spécialités respectives. Les domaines de la défense, de la sécurité et des OIV ne font pas exception à cette règle.

L'environnement technologique évolue très rapidement, imposant une **cadence des cycles** courts de conception, de réalisation et d'industrialisation, ce qui favorise l'émergence de petites structures par leur réactivité aux besoins immédiats. Ce foisonnement d'acteurs apparait comme une réelle richesse en matière d'innovation. Cependant, cette dispersion des acteurs peut handicaper l'émergence d'acteurs de niveau européen, aptes à rivaliser avec la concurrence mondiale.

Le GINUM souhaite donc créer une **synergie** entre ces acteurs pour favoriser l'émergence d'offres souveraines et responsables, françaises et européennes. Le regroupement d'acteurs autour d'objectifs de coopération sur le moyen terme, répondant à des critères nationaux, est un préalable pour affronter la concurrence existante.

Les moyens alloués à la **recherche et au développement** par les grands acteurs extra-européens sont conséquents. Si la France et l'Union européenne souhaitent être en mesure de concurrencer ces acteurs, il convient de créer les conditions favorisant la recherche et le développement ainsi que le transfert industriel.

Le soutien public en est un des éléments essentiels. Le crédit d'impôt recherche correspond à un coût budgétaire de près de 6 milliards d'euros par an, soit près de 60 % de l'ensemble des soutiens publics à l'innovation en France[9].

Ce dispositif d'octroi de subventions ou avances remboursables comporte des effets positifs comme la hausse de la probabilité de 5% de déposer un brevet[10]. Néanmoins, l'impact réel de ce dispositif est encore difficilement perceptible en matière d'innovation et d'activité économique[11].

Aux États-Unis, le dispositif de subventions est moins généralisé qu'en France ou en Europe. Les administrations commandent des produits ou systèmes opérationnels matures mais également des produits en cours de conception. Le modèle américain repose sur la passation de contrats qui apprécient la performance du produit[12]. Ce retour sur investissement impose aux entreprises de délivrer rapidement un **produit de qualité**.

Le dispositif des études amont de la défense peut se rapprocher de cette méthodologie américaine. Pour autant, le processus décisionnel et la durée des cycles français subissent la très forte évolutivité du numérique.

Ce constat amène le GINUM à proposer les deux axes de réflexion suivants.

Axe de réflexion 1 : de manière adaptée, prévoir des budgets et un processus d'études prospectives correspondant aux besoins numériques des acteurs de la sécurité et des OIV sur le modèle de ce qui existe au ministère des Armées.

Axe de réflexion 2 : privilégier une logique de commande avec obligation de performance à une logique de subvention.

B) Les Leviers pour la mise en œuvre d'une stratégie industrielle souveraine

1) Les leviers nationaux

Un premier levier est la **régulation des exportations**.

Le Service de l'information stratégique et de la sécurité économiques (SISSE), dépendant de la Direction générale des entreprises (DGE), protège les technologies, les entreprises et les filières stratégiques de l'économie française. Cette autorité permet une **intervention étatique** lors de la vente d'entreprises critiques.

---

[9] France stratégie, Commission nationale d'évaluation des politiques d'innovation, *L'impact du crédit d'impôt recherche*, mars 2019, p7.
[10] France stratégie, Commission nationale d'évaluation des politiques d'innovation, *L'impact du crédit d'impôt recherche*, mars 2019, p55.
[11] INSEE, *Évaluation du crédit d'impôt innovation : dynamique des bénéficiaires depuis son introduction*, 2019, p 81.
[12] Taylor & Francis Group, *The Economics of the Global Defence Industry*, 2019, p24.

Les Américains disposent d'une réglementation extraterritoriale comme les Export Administration Regulations (EAR) et l'International Traffic in Arms Regulation (ITAR) protégeant efficacement leurs technologies stratégiques, allant du composant aux systèmes complexes[13].

Axe de réflexion 3 : étudier la faisabilité de mise en place de règles type ITAR/EAR aux niveaux national et européen.

Un deuxième levier consiste en la définition d'une **politique publique de l'open source** alliant autonomie stratégique et maîtrise des coûts d'acquisition.

En novembre 2021, le gouvernement a lancé un plan d'action « logiciels libres » pour la transformation numérique du service public[14]. Le logiciel libre n'est pas forcément une réelle voie de souveraineté. De nombreux outils libres sont, en effet, sous le contrôle d'acteurs extra-européens majeurs comme PostgreSQL, développé par Oracle, ou Linux par IBM/Redhat. De plus, certaines fonctionnalités sont payantes et uniquement accessibles via des relations contractuelles avec des acteurs extra-européens. Par ailleurs, les codes ne sont pas publics. A contrario, l'open source, porté par des communautés, peut être maîtrisé à condition d'y investir les compétences suffisantes[15]. Dans un contexte de contrainte budgétaire, si l'effort en matière de ressources humaines est réalisé, l'open source permet une maîtrise des coûts récurrents et autorise une indépendance accrue vis-à-vis des acteurs commerciaux extra-européens.

Axe de réflexion 4 : définir une politique open source plus volontariste au profit des besoins de la défense, de la sécurité et des OIV.

Un troisième levier correspond à la **commande publique.** Les choix nationaux d'acquisitions sont de réels instruments en vue de soutenir des orientations géopolitiques, technologiques et économiques pour conserver la liberté d'action. Pour la défense, la sécurité et les OIV, une très grande partie des contrats relève de la commande publique ou parapublique. Le dispositif de la commande publique laisse aux acheteurs une réelle capacité de définition de leurs besoins et des clauses contractuelles qui en découlent[16].

Du contrat simple à prix ferme aux contrats à remboursement de coûts, l'approvisionnement doit se traduire par une **performance** en matière de respect des coûts, de réalisation des objectifs visés et de maîtrise du calendrier, alliée à une stratégie industrielle.

---

[13] Jared Mondschein, Jonathan W. Welburn, Daniel Gonzales, « Securing the Microelectronics Supply Chain: Four Policy Issues for the U.S. Department of Defense to Consider», *Santa Monica*, 2022.
[14] https://www.numerique.gouv.fr/publications/plan-action-logiciels-libres-communs-numeriques/
[15] Cigref, *L'open source, une alternative aux grands fournisseurs,* 2018, p9.
[16] Renaut Bellais, Martial Foucault, Jean-Michel Oudot, *Économie de la défense*, 2014.

Ainsi, le développement d'une **ingénierie contractuelle** pour atteindre le niveau de performance sur le plan technique, économique, industriel, pourrait intégrer des notions de souveraineté dans les processus d'acquisition.

Ce mécanisme consiste à utiliser tous les leviers du code des marchés publics pour s'assurer, dans le temps, de la préservation de la liberté d'action au travers d'un processus de type « souveraineté par construction ». Un autre mécanisme visant à favoriser la maîtrise des outils acquis au travers de la commande publique consisterait à imposer la **transparence des codes** et leur dépôt chez un tiers de confiance (par exemple l'ANSSI).

Axe de réflexion 5 : étudier les modalités d'intégration de notions liées à la souveraineté et incluant des aspects économiques et industriels dans les intérêts essentiels de l'Etat, au sein des processus d'acquisition dans les domaines de la défense, de la sécurité et des enjeux d'importance vitale.

2) Les leviers européens

La force des grands acteurs américains du numérique est de bénéficier d'un marché intérieur dont la taille garantit des **volumes de commandes** importants. En comparaison, la taille du marché européen constitue une masse critique suffisante pour développer une politique comparable à celle des États-Unis. Pour autant, une **harmonisation normative** en Europe est une prémisse pour offrir un marché du numérique pour la défense, la sécurité et les OIV.

L'Europe doit développer des certifications correspondant à ses exigences en matière de sécurité, de protection des libertés individuelles et de souveraineté. Or, on constate une multiplication des certifications nationales et européenne qui complexifie l'accès aux marchés et limite les effets de levier au niveau des marchés européens. L'impact est aussi ressenti sur les capacités à assurer la **sécurité d'approvisionnement** et d'**interopérabilité** entre pays européens.

Axe de réflexion 6 : Harmoniser les certifications à l'échelle européenne et française.

Pour aller plus loin dans la mise en œuvre effective, les règlementations de l'Union européenne sont un instrument clé pour favoriser un marché du numérique **équitable** et **inclusif** entre les acteurs.

Négociés actuellement au sein de l'Union européenne, les règlements Digital Services Act (DSA) et Digital Markets Act (DMA) ont pour objectif de réguler l'espace numérique.
D'une part, le DSA vise à s'assurer du respect de la libre concurrence des contrôleurs d'accès[17].

[17] https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

D'autre part, le DMA a pour finalité de freiner la propagation de contenus et de produits illicites[18]. Ces deux textes régulant l'espace numérique européen assurent le respect des droits fondamentaux en ligne et limitent la distorsion de la concurrence.

Afin de renforcer la compétitivité des petites et moyennes entreprises, l'Europe s'est dotée en juin 2008 d'un Small Business Act (SBA). Ce dispositif non contraignant énonce des principes destinés à favoriser l'émergence de ces structures au travers notamment de financements[19].

Cependant, contrairement au SBA américain, le SBA européen n'impose pas de **quota des marchés publics** des pays membres en faveur des PME, ce qui le rend peu efficace[20]. Cette différence majeure entre les deux textes repose sur le refus de l'Union Européenne de transgresser l'accord sur les marchés publics de l'OMC[21]. Les États-Unis ont négocié une **dérogation** pour pallier cette incompatibilité règlementaire.

Axe de réflexion 7 : demander une dérogation auprès de l'OMC pour permettre aux États membres de mettre en place, sur les sujets de souveraineté numérique dans les domaines de la défense, de la sécurité et des OIV, un quota de marchés publics en faveur des TPE et PME.

[18] https://ec.europa.eu/competition-policy/sectors/ict/dma_fr
[19] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52008DC0394&from=EN
[20] Assemblée nationale, Rapport d'information sur la politique industrielle européenne, 2007.
[21] https://www.senat.fr/rap/r06-347-1/r06-347-1119.html

Face à la démultiplication des objets connectés et à la masse exponentielle des données, l'enjeu de la **gouvernance du cycle de la donnée** de manière transparente, démocratique et éthique devient saillant pour la souveraineté française et européenne.

Actuellement, l'Europe est confrontée à la dominance de **deux modèles** de gouvernance de la donnée, l'un américain et l'autre chinois. D'une part, le **modèle américain**, construit autour d'une puissance financière et technologique, laisse à ses entreprises une grande liberté d'utiliser les données qu'elles détiennent et de proposer leurs services sur l'ensemble du globe. D'autre part, le **modèle chinois** dote Pékin du pouvoir nécessaire pour contrôler et surveiller ses citoyens et leurs données. Dans les deux cas, la Chine et les États-Unis réglementent leurs entreprises du numérique en dehors de leurs frontières au travers de cadres légaux extraterritoriaux (Cloud Act, CISPA, Cyber Security Law, etc.), indépendamment de la localisation des données. Du point de vue du GINUM, ces deux modèles entravent l'implémentation d'une gouvernance souveraine, transparente et démocratique des données.

Une telle gouvernance apparait nécessaire et peut certainement être proposée par l'Union européenne. L'adoption en 2016 du règlement général relatif à la protection des données personnelles (RGPD) a permis tant une **harmonisation juridique** entre les États membres pour favoriser en son sein l'intégration économique et sociale qu'une régulation des flux des données personnelles des Européens vers des pays tiers. Le RGPD a donc dynamisé les travaux vers un potentiel **standard mondial** pour les droits à la protection des droits de la personne[22]. Conscients du souhait de leurs citoyens d'être rassurés sur la protection de leurs données, Américains et Chinois se sont eux-mêmes dotés de leurs propres législations locales, par exemple le California Consumer Privacy Act (2020) et le Personal Information Protection Law (2021) chinois.

Les valeurs européennes, décrites dans la charte des droits fondamentaux (2000), offrent un socle pour établir un modèle numérique européen démocratique et éthique. Parmi ces principes, la transparence est essentielle à l'établissement d'un **cadre de confiance,** tel un véritable « contrat social »[23], entre les différents acteurs. Elle permet aux citoyens de recouvrer un contrôle sur leurs données et d'en garantir l'intégrité.

[22] Jeanne Saliou, *1970-2021 : la protection des données essaime le monde,* Laboratoire d'innovation numérique de la CNIL, 2021.
[23] Jean-Jacques Rousseau, *Du contrat social,* Flammarion, 2011.

Aujourd'hui en situation de forte dépendance numérique, l'Union européenne, face à la Chinamérique[24], doit s'emparer de la **puissance normative** octroyée par le RGPD et l'associer à ses **valeurs fondamentales** afin de proposer une véritable alternative aux modèles américains et chinois.

Dès lors, la construction d'une **troisième voie européenne**, respectueuse de nos valeurs démocratiques et éthiques, et garante des données de ses citoyens, entreprises et États membres, est primordiale. Dans ce contexte, le GINUM aspire à participer à l'élaboration d'un modèle européen régissant **le cycle de la donnée** pour les secteurs de la défense, de la sécurité et des OIV. Ses travaux s'attachent ainsi à détailler des enjeux et propositions concrètes pour faciliter et structurer cette construction qui se doit de concilier transparence, réglementation et innovation pour un numérique de confiance.

A) Une innovation par la donnée au ralenti

Carburant de la transformation numérique, la maîtrise du traitement des données est essentielle pour intégrer efficacement les ruptures technologiques et en retirer des gains de productivité. Par exemple, dans le cadre d'une intervention extérieure, l'information captée par des systèmes d'information renforce la capacité des acteurs régaliens à conserver leur supériorité décisionnelle. Cependant, le **déluge informationnel** doit être maîtrisé, requérant une gouvernance articulée autour d'une donnée transversale et de qualité.

Les **cloisonnements historiques**, liés aux modes de fonctionnement des domaines critiques de la défense de la sécurité et des OIV, dus en partie aux contraintes de sécurité et au besoin d'en connaître, constituent un frein à la circulation de l'information. Cette culture de silos induit une absence d'homogénéité et de transversalité entre les systèmes d'information. Une ouverture maîtrisée de la donnée contribuera à accroître la performance opérationnelle tout en garantissant un contrôle d'accès aux données sensibles.

Les activités des acteurs de la défense, de la sécurité et des OIV sont soumises à une multitude de réglementations qui encadrent l'utilisation et la sécurisation des systèmes d'information opérant des données sensibles. Ces dernières années, les **obligations légales se sont complexifiées** et leurs champs d'application se sont confondus dans certains domaines. Par exemple, certaines banques doivent appliquer le RGPD (2016) et la Directive sur les services de paiements II (2015). Alors que le règlement requiert une conservation des données « a minima », la directive oblige la conservation des informations sur un paiement pendant au moins 20 ans.

[24] Jean-Louis Chambon, *La Chinamérique, un couple contre-nature ?*, 2010.

La mise en place d'un cadre juridique, orienté sur le cycle de la donnée et regroupant l'ensemble des exigences règlementaires, facilitera leurs mises en œuvre tout en garantissant le respect des libertés fondamentales.

La publication d'un **Code du Numérique** s'appliquant aux domaines de la défense, de la sécurité et aux OIV est de nature à favoriser la compréhension des différents cadres réglementaires par l'ensemble de ces acteurs.

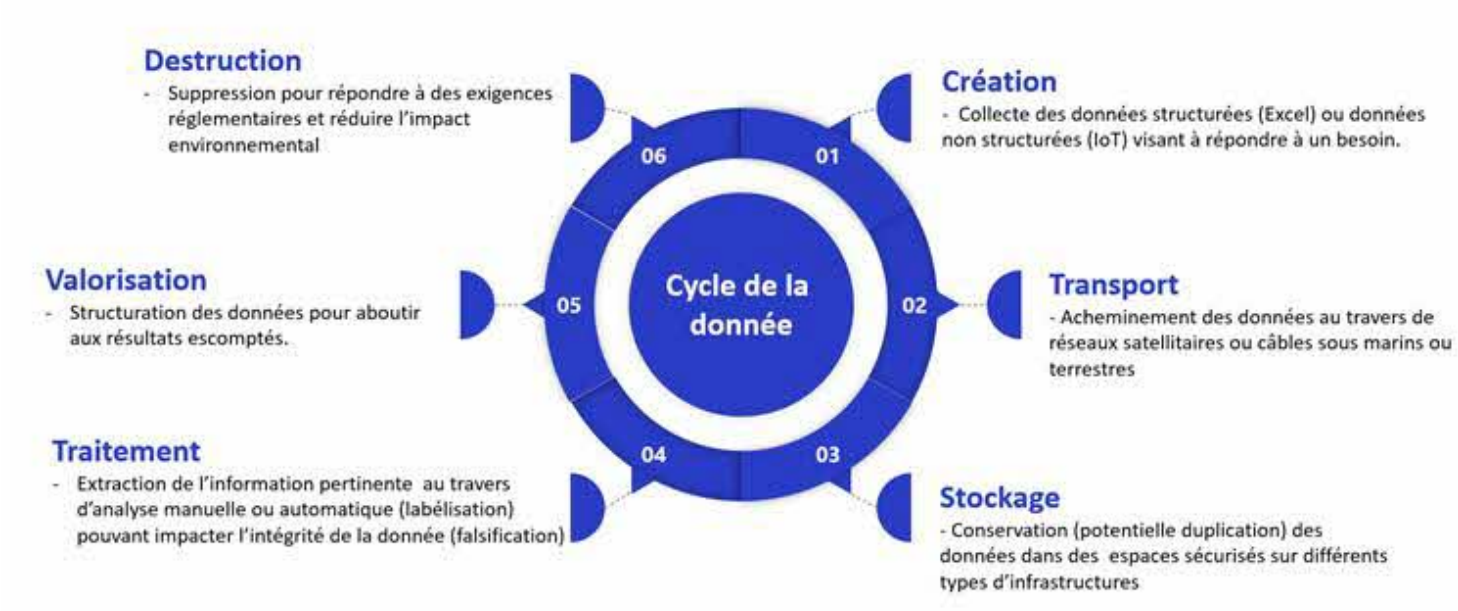
Basé sur le cycle de la donnée, ce Code du Numérique regroupera :

- l'ensemble des règlementations, des jurisprudences afin d'assurer une cohérence globale des différents textes dans leurs champs d'applications,
- des synthèses, comme la CNIL a commencé à le faire dans domaines sous le nom de « référentiels », pour préciser les bonnes pratiques relatives à certaines données (durée de conservation légale par exemple),
- des exemples pour anonymiser, pseudonymiser et flouter des données pour des utilisations statistiques par exemple.

Axe de réflexion 8 : créer un Code du Numérique pour renforcer la cohérence et l'applicabilité des textes règlementaires.

B) L'importance de considérer la donnée dans l'intégralité de son cycle de vie

Appréhender la donnée au travers de son cycle de vie permet de s'assurer de la **cohérence des procédures et règlementations**, avec cette finalité de garantir la disponibilité, la traçabilité, l'intégrité et la confidentialité de cette donnée.



Seul ce changement de paradigme permet d'assurer une **transparence** dans la gouvernance de la donnée, tout au long de son cycle. Cette vision facilite également la gestion des risques de falsification et de **destruction** de la donnée sur les réseaux physiques.

Dans la continuité de l'applicabilité des textes, la mise en place d'un **outil unique pour l'analyse d'impact** regroupant l'ensemble des exigences réglementaires facilitera la mise en œuvre de ces dispositions.

En amont de la mise en production d'un système d'information ou d'une application, les équipes projet doivent, en effet, réaliser différentes analyses d'impact et de risques pour s'assurer de leurs mises en conformité à l'ensemble des textes. Ces différentes actions, requises pour confirmer le respect du niveau d'exigences d'une homologation, sont chronophages et onéreuses pour les acteurs étatiques et privés. La mise en œuvre d'un outil unique pour apprécier le **niveau de conformité** règlementaire et sécuritaire contribuerait donc à accélérer le développement et la mise à disposition de produits et services innovants.

Axe de réflexion 9 : fournir aux équipes projet un outil d'analyse d'impact unique afin de faciliter la mise en conformité.

C) L'intelligence artificielle dans le cycle de la donnée

L'utilisation croissante du machine learning et la prise de décision plus ou moins automatique par une machine, au travers de l'intelligence artificielle, soulèvent des enjeux clefs dans la manière d'exploiter les données. L'utilisation de cette technologie s'insère dans le cycle de vie de la donnée et nécessite d'expliciter certaines spécificités.

Qu'il s'agisse de traitement d'images, d'analyse de comportements suspicieux, de système de contrôle-commande, voire de système d'armes létales autonomes, l'intelligence artificielle permet a priori d'amplifier les performances des systèmes. Son application implique une robustesse sans faille du système pour permettre à la chaîne de commandement de se fier aux recommandations faites en vue de la prise de décision[25]. Cependant, la maturité et la pertinence d'une intelligence artificielle restent actuellement difficiles à mesurer, en raison de l'opacité de son fonctionnement dit « effet boite noire ».

[25] Assemblée nationale, *Rapport d'information en conclusion des travaux d'une mission d'information sur les systèmes d'armes létaux autonomes,* 2020, p32.

L'intelligence artificielle, objet de nombreux travaux actuels, repose avant tout sur l'apprentissage, censé améliorer ses performances avec l'expérience et acquérir ainsi de nouvelles compétences en vue d'exécuter des tâches prédéfinies[26].

La proposition de règlement de la Commission européenne (2021) est un premier levier juridique pour imposer des obligations dans l'usage de l'intelligence artificielle au sein du marché européen, en fonction du niveau de risque porté par cette technologie[27]. La mise en place d'outils techniques pour auditer, expliquer et qualifier les intervalles de confiance et les biais dans un système constituent autant de fondations nécessaires pour le développement d'une intelligence artificielle de confiance. Toutefois, les équipes projet se retrouvent souvent confrontées à une multiplication des outils et à une augmentation des réglementations. Avant une mise en production, la nécessité de passer par un processus d'homologation, puis de réaliser une analyse d'impact des données personnelles, voire de la robustesse d'une intelligence artificielle, peut s'avérer complexe et constituer potentiellement une entrave à l'innovation. Il est donc nécessaire de définir une méthode standardisée relative à la cohérence et la conformité de l'ensemble de ces réglementations, afin de faciliter la mise en œuvre de ces systèmes potentiellement disruptifs.

L'autre difficulté concerne l'expérimentation et le passage à l'échelle, c'est-à-dire la transformation d'une innovation en un projet industriel viable. Les industriels doivent pouvoir expérimenter leurs offres dans un cadre réglementaire adapté à cette phase amont. Ainsi, le GINUM propose de fédérer les acteurs publics et privés des domaines de la défense, de la sécurité et des OIV autour de **« Expérience-IA »** : ce bac à sable sécurisé en environnement fermé aura pour objectif de permettre des expérimentations à haut risque dans les secteurs concernés.

« Expérience-IA » fournira un cadre légal et expérimental qui servira à :

- garantir l'intégrité de la donnée manipulée,
- constituer une « zone franche » dans laquelle la règlementation serait adaptée pour expérimenter des sujets dits sensibles comme la reconnaissance faciale,
- protéger la propriété intellectuelle des industriels en se prémunissant de l'application de tout cadre légal extracommunautaire ou de subtilisation par acte malveillant.

Par la suite, un passage à l'échelle de l'innovation provenant du bac à sable reposera sur :

- de bonnes garanties concernant le respect plein et entier de la règlementation,

[26] Yann Le Cun, *Quand la machine apprend : La révolution des neurones artificiels et de l'apprentissage profond,* Odile Jacob, 2019.
[27] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52021PC0206

- une transition vers un projet viable réduisant le risque de décrochage technologique.

Cette proposition sera de nature à faciliter l'émergence d'offres innovantes françaises et européennes en phase avec les valeurs démocratiques et éthiques, et protégées d'actions malveillantes ou de soumission à des cadres légaux extraterritoriaux.

La mise en œuvre de « Expérience-IA » nécessitera de :

- définir un cadre précis de mise en place et d'utilisation de ce bac à sable et se doter des moyens de contrôle associés – techniques, sectoriels ou réglementaires,
- proposer aux entreprises membres un environnement complet (de type cloud souverain avec des conditions spécifiques), offrant à la fois les moyens d'expérimentation en bac à sable puis de passage à l'échelle en minimisant le risque de rupture technologique,
- mettre en place une technologie (blockchain privée, chiffrement etc.) pour garantir la confidentialité et l'intégrité de la donnée lors de l'expérimentation.

Axe de réflexion 10 : lancer le bac à sable « Expérience-IA » pour mener des expérimentations sensibles.

La sécurisation de la chaine d'approvisionnement du numérique est une condition essentielle à la conservation de la liberté d'action. En effet, la prise en compte de l'ensemble des biens et des services est indispensable à la souveraineté opérationnelle du numérique. Depuis 2019, la chaine d'approvisionnement a été ébranlée par deux facteurs majeurs. D'une part, l'interruption de la production causée par la pandémie COVID-19 et la logique de flux tendus ont contribué à la rareté des stocks. D'autre part, la guerre économique entre les grandes puissances a illustré la volonté de certains États d'utiliser les ressources stratégiques dont ils disposent comme leviers de leur politique.

Notre dépendance en matière d'approvisionnement en métaux rares et en composants électroniques, influe sur la capacité nationale à produire dans le respect de sa « culture stratégique [28]». Ainsi, l'enjeu de la chaine d'approvisionnement illustre le besoin d'une politique industrielle intégrée pour garantir la liberté d'action.

A) Les matières premières

Du panneau solaire à la production du dernier smartphone, la révolution technologique a démultiplié les besoins en approvisionnement en métaux rares comme le cobalt, le germanium ou le prométhéum[29]. Dans les années 80, le Premier Ministre chinois Deng Xiaoping a voulu diminuer la dépendance technologique extérieure. Pour ce faire, Pékin a mis en place une stratégie destinée à acquérir les compétences humaines et technologiques pour maîtriser la chaine d'extraction et de traitement des métaux rares. Quarante ans plus tard, la Chine se positionne en quasi-monopole avec 80 % de la production de ces métaux sur son sol ou ceux de ses « états satellites » comme la Mongolie[30]. La conquête chinoise de minerais stratégiques se traduit également par des investissements et l'acquisition de compagnies étrangères comme l'entreprise australienne Arafura Ressources ou l'américaine Magnetench pour contrôler l'offre sur les marchés de métaux rares[31]. À la suite d'une prise de conscience, le gouvernement américain en 2019 a officialisé une feuille de route pour sécuriser les approvisionnements des minéraux critiques nécessaires à l'industrie américaine[32]. En France, la publication du rapport Varin, en janvier 2022, souligne l'intérêt français de développer son autonomie stratégique en développant les filières d'avenir et en réduisant la dépendance aux fournisseurs extra-européens[33].

---

[28] Basil Henry Liddell Hart, *Stratégie,* Perrin, 2015.
[29] Guillaume Pitron, *La guerre des métaux rares*, Les liens qui libèrent, 2019.
[30] https://www.lefigaro.fr/conjoncture/les-terres-rares-ultime-moyen-de-pression-de-la-chine-20190522
[31] Christophe-Alexandre Paillard, Les Nouvelles guerres économiques, Ophrys, 2011, p234.
[32] https://www.commerce.gov/sites/default/files/2020-01/Critical_Minerals_Strategy_Final.pdf
[33] https://www.ecologie.gouv.fr/investir-dans-france-2030-remise-au-gouvernement-du-rapport-varin-sur-securisation

Filières industrielles stratégiques, les secteurs de la défense, de la sécurité et des OIV sont des consommateurs importants de ces métaux rares. Une stratégie intégrée de réindustrialisation doit adopter l'approvisionnement en minerai de la chaine de production des composants.

Axe de réflexion 11 : intégrer l'approvisionnement des métaux rares dans nos partenariats stratégiques européens et internationaux et renforcer notre capacité à exploiter nos ressources.

B) Les composants électroniques

Au cœur de la guerre commerciale entre la Chine et les États-Unis les composants électroniques sont devenus une monnaie stratégique à fort enjeu. Depuis 1990, la production complexe de semi-conducteurs basée à Taiwan dans les usines de la Taiwan Semi-conducteur Manufacturing Company est essentielle à l'échelle internationale (TSMC)[34].

La diminution de la disponibilité des semi-conducteurs durant les confinements a impacté les capacités de production des domaines de la défense, de la sécurité et des OIV. En parallèle, les sanctions américaines à l'encontre d'entreprises chinoises ont été renforcées en 2020 en y ajoutant les fabricants de puces. La production actuelle de puces électroniques en Europe s'élève à 10% de la production mondiale.

Soucieuse de maîtriser sa chaine de production, la Commission Européenne a publié le Chips Act visant principalement à produire des puces à moins de 10 nanomètres au travers d'un partenariat public-privé subventionné par une enveloppe de 45 milliards d'euros[35]. Malgré cette annonce, des problématiques environnementales et économiques persistent pour conserver la liberté d'action sur la production de ces composants. D'une part, la production de composants électroniques nécessite un marché local et la prise en compte de l'ensemble de la chaine de valeur de production comme les circuits électroniques de pointes ou les outils logiciels de conception de circuits[36]. D'autre part, l'énergie nécessaire, en eau et électricité, pour produire ces composants électroniques constitue un défi environnemental[37]. Le recyclage doit être une voie à suivre.

Axe de réflexion 12 : structurer des filières de fabrication et de recyclage des composants électroniques, dans un modèle visant à minimiser les empreintes environnementale et énergétique.

---

[34] https://www.lepoint.fr/monde/guerre-des-puces-les-lecons-des-maitres-taiwanais-15-05-2021-2426530_24.php
[35] https://ec.europa.eu/commission/presscorner/detail/fr/STATEMENT_22_891
[36] https://www.lesechos.fr/tech-medias/hightech/chips-act-un-plan-necessaire-mais-pas-suffisant-selon-les-acteurs-francais-des-semi-conducteurs-1385495
[37] https://ecoinfo.cnrs.fr/2010/10/20/le-silicium-les-impacts-environnementaux-lies-a-la-production/

C) Les besoins énergétiques

La sécurisation de l'approvisionnement énergétique est en pleine mutation. La demande croissante en énergie des infrastructures numériques nécessite une offre alignée à cette consommation en hausse. Selon la Commission Européenne en 2020, la consommation énergétique des data centers atteindra 98,5 TWh/an, soit 3.2% de la demande en électricité mondiale [38]. En effet, les data centers ont besoin d'une disponibilité électrique constante et d'un système de refroidissement pour assurer leur fonctionnement.

Afin de lutter contre le réchauffement climatique et de pérenniser sa souveraineté énergétique, la France poursuit la diversification des sources énergétiques[39]. Les énergies renouvelables, comme l'éolienne, ont besoin d'aimants permanents qui sont produits à partir de terres rares et de métaux critiques dans les batteries lithium-ion[40]. L'énergie nucléaire représente un intérêt par sa faible émission de dioxyde carbone et restreint les dépendances aux hydrocarbures.

Par ailleurs, la plupart des grandes puissances intègrent l'accès à l'énergie dans leurs stratégies de défense et de sécurité, sous l'angle soit défensif, soit offensif, par exemple au travers d'embargos ou d'attaques cyber.

Axe de réflexion 13 : élaborer une stratégie intégrée prenant en compte les besoins énergétiques visant à sécuriser la chaine d'approvisionnement du numérique dans les domaines de la défense, de la sécurité et des OIV.

[38] Commission européene, Directorate-General for Communications Networks, *Energy-efficient cloud computing technologies and policies for an eco-friendly cloud market: final study report*, 2020.
[39] https://www.ecologie.gouv.fr/sites/default/files/PPE_2020_en%204%20pages.pdf
[40] Gilles Lepesant, *La transition énergétique face au défi des métaux critiques*, IFRI, 2018.

Le GINUM partage le constat qu'il existe aujourd'hui un déficit très important de compétences. En 2019, l'Union européenne comptait 7,8 millions de professionnels dans le secteur numérique dont 18% de femmes[41]. Sur ce sujet spécifique, les domaines de la défense et de la sécurité se caractérisent de manière générique par une sous-représentation marquée des femmes qui représentent environ 20 % des effectifs[42]. Une réflexion spécifique afin d'attirer davantage de femmes dans les métiers numériques de la défense et de la sécurité apparait donc indispensable. Dans ce cadre, des travaux avec des associations comme « Femmes@numérique » pourraient être particulièrement utiles.

Par ailleurs, près de trois quarts des entreprises ne trouvent pas, à l'heure actuelle, les professionnels dont elles ont besoin[43]. A l'horizon 2030, ces besoins sont estimés à près de 20 millions de professionnels[44].

Les domaines de la défense, de la sécurité et des OIV n'échappent pas à ce constat global de déficit de compétences et d'inclusion insuffisante. La pénurie de ressources est aggravée par l'exigence, pour les acteurs du numérique œuvrant dans ces domaines, de pouvoir intervenir sur des sujets à forte sensibilité, avec des ressources humaines pouvant être habilitées, ce qui constitue une réelle contrainte.

Cette spécificité impacte le volume du vivier potentiel de compétences à toutes les étapes du parcours professionnel : formation initiale, recrutement des talents à leur sortie de formation et rétention tout au long de leur carrière.

A) Renforcer la formation initiale

La France doit concentrer ses efforts de formation sur des secteurs à haut potentiel : cybersécurité, intelligence artificielle et blockchain [45].
En outre, à l'horizon 2030, l'Europe estime que trois entreprises sur quatre auront adopté des services tels que le cloud, le big data et l'intelligence artificielle.

[41] https://www.vie-publique.fr/eclairage/282033-leurope-numerique-une-transition-tournee-vers-lhumain
[42] Ministère des Armées, Le plan mixité du ministère des armées, 2019.
[43] https://www.vie-publique.fr/eclairage/282033-leurope-numerique-une-transition-tournee-vers-lhumain
[44] Ibid
[45] Assemblée nationale, *Bâtir et promouvoir une souveraineté numérique nationale et européenne*, Juin 2021.

Pour faire face à cette demande et pour s'assurer que **l'offre de formation soit adaptée aux besoins,** le GINUM considère qu'il est indispensable de rapprocher les structures de formation et les acteurs économiques (entreprises, organisations professionnelles, etc.)

Le GINUM encourage donc le **développement de partenariat** entre les filières d'enseignement et les industriels français ou européens développant des offres souveraines. Le contact approfondi avec ces outils lors des phases de formation fera naturellement de ces étudiants les futurs ambassadeurs de ces solutions souveraines. On peut citer en exemple, la démarche mise en place entre l'école Hexagone et l'industriel Stormshield, spécialiste du domaine du chiffrement[46].

De ces partenariats pourraient émerger des référentiels de compétence, par secteur technologique au sein des entreprises et au niveau national, sur lesquelles les structures d'enseignement pourront s'appuyer pour définir leur ingénierie de formation

Des principes similaires peuvent et doivent être mis en œuvre pour la **formation continue**. Ainsi, les organismes de formation professionnelle pourraient également travailler en collaboration avec les fournisseurs de solutions souveraines dans une optique d'harmonisation entre l'enseignement initial et la formation continue.

Dans ce contexte global, le GINUM propose trois axes de réflexion, afin de répondre aux enjeux spécifiques des domaines de la défense, de la sécurité et des OIV.

Il est tout d'abord indispensable que les filières de formation prennent en compte les spécificités mentionnées précédemment. A cet effet, le GINUM propose donc de créer un label « **Souveraineté Numérique** » qui pourrait s'adapter à toutes les formations initiales et continues quels que soient le sujet et le niveau visés.

Cette approche pourrait, par exemple, s'inspirer des pratiques de l'université de Laval qui propose des formations allant de niveau Bac +2 (BTS et IUT) jusqu'à des niveaux BAC + 5 dont certaines sont labélisées par l'ANSSI (SECNUMEDU) et qui proposent toutes un fonctionnement par alternance.

Axe de réflexion n°14 : développer un label "Souveraineté Numérique" pour les formations initiales et continues et construire ces formations avec les industriels proposant des solutions souveraines.

[46] https://www.ecole-hexagone.com/fr/cursus/cyberdefense

Au nom des **valeurs de responsabilité** qu'il défend, le GINUM estime qu'il est souhaitable et possible d'attirer vers le numérique souverain des **profils éloignés de l'emploi** (personnes handicapées, personnes en reconversion, etc.) en leur apportant, notamment via des acteurs spécialisés de l'économie sociale et solidaire, une formation et un encadrement adaptés.

Ces personnels pourraient notamment venir renforcer les entreprises fournissant ou désireuses de fournir des solutions et technologies souveraines et constituer, pour certains profils, une alternative à la délocalisation.

Le recours à de telles structures est déjà prévu dans de nombreux marchés publics. Il pourrait, dans le cas du numérique souverain, être systématisé pour tous les marchés de l'Etat et étendu à l'ensemble des achats réalisés par les OIV.

De même, le développement de partenariat avec des structures de formation adaptées à des profils type « Geek », ne s'épanouissant pas pleinement dans le système académique traditionnel, est une piste de travail. A cet effet, l'exemple de la coopération déjà menée entre l'École 42 et la Gendarmerie Nationale mérite d'être étudié.

Axe de réflexion n°15 : Renforcer les filières favorisant la formation et le recrutement de profils éloignés de l'emploi dans le secteur du numérique souverain et favoriser leur employabilité via les marchés publics.

L'objectif de la formation ne doit pas se limiter aux spécialistes du numérique mais concerner également les acteurs métier des domaines de la défense, de la sécurité et des OIV et notamment leurs cadres dirigeants. Une **diversification des profils recrutés** pourrait être recherchée afin de disposer de davantage de dirigeants disposant d'une formation scientifique ou technique utile à une meilleure compréhension des enjeux stratégiques du numérique.

Le GINUM partage également le constat affiché par le rapport « Bâtir et promouvoir une souveraineté numérique nationale et européenne, » relevant qu'il est indispensable que les salariés et les dirigeants d'une entreprise maîtrisent **les codes du cyberespace** afin d'être suffisamment vigilants face aux risques[47].

[47] Assemblée nationale, *Bâtir et promouvoir une souveraineté numérique nationale et européenne*, Juin 2021.

Plus une entreprise monte en puissance sur cette maîtrise du numérique, plus elle sera souveraine sur la maîtrise de ses choix, en disposant de la capacité d'identifier les technologies adaptées à ses besoins métier et de piloter les fournisseurs de solutions.

Axe de réflexion n°16 : assurer dans toutes les écoles de formation de la fonction publique et, en particulier, dans le nouvel Institut du Service Public, un parcours numérique prenant en compte les notions de souveraineté et de responsabilité.

B) Attirer les talents du numérique

Même s'il reste bien entendu des axes d'amélioration, la France dispose d'un vivier conséquent d'ingénieurs et de chercheurs, formés par les plus prestigieuses écoles scientifiques.

Ce constat posé, l'enjeu est de retenir ces talents à leur sortie de formation en leur proposant des emplois et des parcours attractifs. A cet effet, le GINUM a identifié cinq critères de choix :

- n°1 : le salaire,
- n°2 : les conditions de travail (matériel et humain),
- n°3 : le sens et les perspectives de l'activité proposée,
- n°4 : la contribution au bien commun,
- n°5 : les engagements RSE.

Les domaines de la défense, de la sécurité et des OIV rivalisent difficilement sur certains de ces critères : par exemple, sur le critère n°1 avec les GAFAM qui peuvent proposer des rémunérations « hors échelles » ou sur le critère n°2 avec certaines start-ups qui proposent des modèles de travail totalement disruptifs.

Il semble donc indispensable d'avoir **une approche globale** sur les cinq critères proposés pour valoriser l'attractivité de ces domaines. Cela pourrait passer par la création d'un label « Filière Souveraineté » permettant pour certains métiers du numérique de valoriser l'emploi occupé au sein d'un parcours professionnel et d'y associer un certain nombre d'avantages : droits à la formation continue, encouragement de l'innovation ou de l'entreprenariat.

Il sera important de définir des **profils prioritaires** pouvant bénéficier de ce label sur la base des compétences critiques pour les domaines concernés. Il semble également nécessaire de prévoir un encadrement adapté pour ces profils, sur le modèle de ce qui existe déjà dans de nombreuses entreprises en matière de gestion des talents.

Axe de réflexion n° 17 : créer une « Filière Souveraineté » en matière de numérique et proposer une gestion des compétences et des parcours au sein de ce label.

C) Conserver les compétences

Ces solutions constituent une approche nécessaire pour attirer des compétences critiques au sein des domaines de la défense, de la sécurité et des OIV. Elles devront toutefois être accompagnées d'autres propositions, sur toute la **durée du parcours professionnel**, pour conserver ces profils.

Comme cela est évoqué dans la théorie des 3P d'Alain Meignant, il existe trois manières d'appréhender le développement des compétences tout au long de sa carrière : le perfectionnement, la reconversion et la diversification[48].

Les grandes entreprises ont la capacité de répondre à ces besoins soit en interne, soit en s'appuyant sur des organismes de formation professionnelle. De plus elles peuvent permettre à certains salariés de développer des projets personnels, en dehors de l'entreprise, tout en leur laissant la possibilité d'y revenir une fois cette nouvelle expérience acquise.

Les PME rencontrent plus de difficultés pour mettre en œuvre ce genre de mécanismes et se limitent bien souvent à des tutorats pour permettre une transmission des savoirs.

L'Etat, pour sa part, rencontre des difficultés à proposer à ces profils des parcours professionnels **variés et enrichissants**, y compris ceux intégrant des passages vers le secteur privé. Force est de constater qu'actuellement ces parcours se font principalement dans un sens, de l'Etat vers le secteur privé, une fois acquise une expérience valorisable sur le marché. Face à cette pénurie de compétences, et sans même parler d'externalisation, l'Etat est contraint de **déléguer** de plus en plus de sujets au secteur privé, risquant ainsi de perdre progressivement la capacité à réaliser des choix et à les adapter dans la durée, y compris sur des sujets critiques pour la résilience et la souveraineté du pays.

A la lumière de ce constat, le GINUM considère que seule une **approche coordonnée** entre tous les acteurs de la souveraineté numérique permettra de prendre en compte toute l'ampleur et la complexité de cet enjeu et suggère donc deux axes de réflexions pour y apporter des réponses.

[48] Alain Meignant, « Dossier 12. La formation », dans : Charles-Henri Besseyre des Horts éd., *RH au quotidien. 100 fiches.* Paris, Dunod, « Pratiques en Or », 2015, p. 350-427.

Dans une optique de gestion d'un écosystème intégrant les grands groupes, les ETI et les PME, les grandes entreprises pourraient faire bénéficier les PME de leur propres formations internes en échange, par exemple, de formations sur les produits et services proposés par ces PME.

Cet **échange de formations** pourrait par ailleurs se traduire par du prêt de compétence entre ces grandes entreprises et ces PME, permettant de proposer des parcours encore plus attractifs pour les salariés concernés.

Axe de réflexion n° 18 : faciliter une démarche de « parcours de talents » entre les intervenants au sein de la « Filière Souveraineté ».

Au niveau des acteurs étatiques, d'autres solutions doivent être imaginées pour assurer la rétention des compétences critiques. Pour tenter de remédier à ce problème, nous proposons un nouveau **modèle de coopération** entre l'Etat et les industriels proposant des solutions souveraines dans le domaine du numérique, modèle basé sur une **logique de coexploitation.**

Sur un sujet donné, l'objectif de ce modèle est de construire un modèle de coopération entre Etat et industriels reposant sur les principes suivants :

1) Les équipes « mixtes » sont situées sur un même lieu et partagent leurs expertises et leur savoir-faire en matière de conception, mise en œuvre et exploitation ;
2) Les personnels de l'Etat peuvent bénéficier d'opportunités professionnelles chez le partenaire de co-exploitation pour enrichir leurs compétences et leurs expériences avant de revenir ensuite au service de l'Etat,
3) En cas de crise majeure, l'Etat peut reprendre seul la main sur la solution souveraine coexploitée.

Axe de réflexion n° 19 : définir un cadre juridique et contractuel permettant la mise en place de modèles de coexploitation entre Etat et industriels.

LES 19 AXES DE REFLEXION DU LIVRE BLEU DU GINUM

Thématique 1 : établir une stratégie industrielle, levier de la liberté d'action

Axe de réflexion 1 : de manière adaptée, prévoir des budgets et un processus d'études prospectives correspondant aux besoins numériques des acteurs de la sécurité et des OIV sur le modèle de ce qui existe au ministère des Armées.

Axe de réflexion 2 : privilégier une logique de commande avec obligation de performance à une logique de subvention.

Axe de réflexion 3 : étudier la faisabilité de mise en place des règles type ITAR/EAR aux niveaux national et européen.

Axe de réflexion 4 : définir une politique open source plus volontariste au profit des besoins de la défense, de la sécurité et des OIV.

Axe de réflexion 5 : étudier les modalités d'intégration de notions liées à la souveraineté et incluant des aspects économiques et industriels dans les intérêts essentiels de l'Etat, au sein des processus d'acquisition dans les domaines de la défense, de la sécurité et des enjeux d'importance vitale.

Axe de réflexion 6 : harmoniser les certifications à l'échelle française et européenne.

Axe de réflexion 7 : demander une dérogation auprès de l'OMC pour permettre aux États membres de mettre en place, sur les sujets de souveraineté numérique dans les domaines de la défense, de la sécurité et des OIV, un quota de marchés publics en faveur des TPE et PME.

Thématique 2 : un numérique conciliant innovation et respect des libertés fondamentales

Axe de réflexion 8 : créer un Code du Numérique pour renforcer la cohérence et l'applicabilité des textes règlementaires.

Axe de réflexion 9 : fournir aux équipes projet un outil d'analyse d'impact unique afin de faciliter la mise en conformité.

Axe de réflexion 10 : lancer le bac à sable « Expérience-IA » pour mener des expérimentations sensibles.

Thématique 3 : la sécurisation de la chaîne d'approvisionnement du numérique

Axe de réflexion 11 : intégrer l'approvisionnement des métaux rares dans nos partenariats stratégiques européens et internationaux et renforcer notre capacité à exploiter nos ressources.

Axe de réflexion 12 : structurer des filières de fabrication et de recyclage des composants électroniques, dans un modèle visant à minimiser les empreintes environnementale et énergétique.

Axe de Réflexion 13 : élaborer une stratégie intégrée prenant en compte les besoins énergétiques visant à sécuriser la chaine d'approvisionnement du numérique dans les domaines de la défense, de la sécurité et des OIV.

Thématique 4 : former, attirer et conserver les compétences essentielles à notre souveraineté numérique

Axe de réflexion n°14 : développer un label "Souveraineté numérique" pour les formations initiales et continues et construire ces formations avec les industriels proposant des solutions souveraines.

Axe de réflexion n°15 : renforcer les filières favorisant la formation et le recrutement de profils « éloignés de l'emploi » dans le secteur du numérique souverain et favoriser leur employabilité via les marchés publics.

Axe de réflexion n°16 : assurer dans toutes les écoles de formation de la fonction publique et, en particulier, dans le nouvel Institut du Service Public, un parcours numérique prenant en compte les notions de souveraineté et de responsabilité.

Axe de réflexion n° 17 : créer une « Filière Souveraineté » en matière de numérique et proposer une gestion des compétences et des parcours au sein de ce label.

Axe de réflexion n° 18 : faciliter une démarche de « parcours de talents » entre les intervenants au sein de la « Filière Souveraineté ».

Axe de réflexion n° 19 : définir un cadre juridique et contractuel permettant la mise en place de modèles de coexploitation entre Etat et industriels.

Pour en savoir plus : www.ginum.fr
Pour nous contacter : contact@ginum.fr