Newsletter n°61 - 16 juin 2023

□□ Éditorial

Assis sur les levées

Nous nous asseyons sur les levées. Pas un jour sans que nous soyons tenus de nous réjouir du fait que quatre ou cinq ingénieurs et un génie du marketing, dont le nez perle encore de la Blédine aient « levé » des dizaines voire des centaines de millions d'euros sur une idée « disruptive » avec des pépites d'IA à l'intérieur. Par décence, attendez voir que ça marche ou que ça crache un peu avant de parler de ce qui a été pompé. Dans ce monde si responsable et durable et bas carbone et inclusif et solidaire, représentez-vous un peu, si tout ce discours a un sens quelconque, ce que 100 millions peuvent représenter pour un Français qui a déjà du mal à s'offrir un vivasteak. Arrêtez de nous mentir, tout ça ne vaut pas tout ça, évidemment. Enfin pas tout à fait. Et puis tout ne se règle pas à coup de virements quand même. Parlez nous de souveraineté, d'humanité, de rentabilité, de pérennité, parlez-nous d'avancées, de percées, de service, de prouesses, de noblesse, de conquêtes… Parlez-nous de la France de la tech discrète, attelée, ouvragière, productive, opiniâtre… Parlez-nous de la tech UTILE ici et maintenant. Pas, ou en tout cas un tout petit peu moins de celle qui gagne au grattage ou au tirage. Et par pitié, arrêtez, par souci d'hygiène mentale, de psalmodier ces montants obscènes qui ne représentent en vérité que de lointains paris faits sur 9 canassons dans le seul espoir que le 10ème gagne la course.

Bertrand Leblanc-Barbedienne

Nous recevons aujourd'hui [Dominique Luzeaux], qui est Directeur de l'[Agence du Numérique de Défense]

La souveraineté en matière de défense n'est pas une option.

□□ Le grand entretien

1/ En matière de défense, la souveraineté vous paraît-elle être une option ? Et si non, quelle définition personnelle en donneriez-vous ?

Une définition assez largement répandue aujourd'hui est celle de Louis Le Fur, né en 1870 : « la souveraineté est la qualité de l'État de n'être obligé ou déterminé que par sa propre volonté ».
Une telle définition repose cependant sur une hypothèse où on avait des environnements fermés ou tout au moins où les

échanges entre divers environnements politico-économiques étaient maîtrisés en quantité et qualité. Ce n'est plus le cas aujourd'hui dans un monde ouvert, où l'incertain et le complexe règnent, d'autant plus quand on aborde la question du numérique, lequel pose un espace sans frontières sur l'espace géo-politico-industriel.

Pour avoir une définition plus opérationnelle, je pense qu'il faut prendre les choses autrement, en partant de la liberté d'appréciation, de décision et d'action. Les différentes éditions des Livres Blancs pour la Défense et la Revue Nationale Stratégique soulignent que l'autonomie stratégique est perçue comme le moyen pour un État d'exercer sa souveraineté, afin de détenir cette liberté d'appréciation, de décision et d'action. D'ailleurs, cette recherche d'autonomie stratégique est un des principes fondateurs de notre politique de dissuasion nucléaire depuis des décennies, théorisée par le général Lucien Poirier : c'est « la faculté pour un peuple de choisir librement, à l'abri de toute pression étrangère, le projet politique qu'il juge conforme à ses intérêts et à ses ressources ».

Par conséquent, pour un État, sauf à avoir intégré dans sa politique le fait de dépendre d'un autre pour se défendre, la souveraineté en matière de défense n'est pas une option.

Ceci dit, au-delà de cette réflexion axée sur la stratégie politique, on peut aussi s'intéresser à la souveraineté industrielle, à la souveraineté technologique, concepts qui reprennent la définition générale en la particularisant respectivement au domaine de la production industrielle, ou à telle ou telle technologie. La question tient alors de la maîtrise : dans la mesure où il n'est pas possible de tout vouloir maîtriser, selon les niveaux souhaités sur cette autonomie souhaitée, on aura des niveaux différents de souveraineté : souveraineté dégradée, quand on recherche maîtrise et résilience limitées au périmètre vital ; souveraineté partielle, maîtrise et résilience de activités critiques ; souveraineté complète, maîtrise et résilience étendues. Le vrai sujet est donc de définir ces différents

périmètres, en fonction de la stratégie politique en amont, et en fonction des ressources budgétaires et humaines en aval.

2/ Les temps étranges que nous traversons vous paraissent-ils propices à un rapprochement entre les mondes civil et militaire ?

En fait, il n'y jamais deux mondes indépendants qui s'ignoreraient. De nombreuses technologies et applications civiles sont issues de développements issus du monde militaire, et réciproquement le monde militaire se nourrit des innovations et développements civils. Il est donc essentiel que ces deux mondes s'appuient l'un sur l'autre, tant en matière d'innovation que sur le plan industriel.
Si l'on peut dire qu'en général le monde civil avance plus vite, notamment dans le domaine numérique, et que le monde militaire a alors intérêt à profiter de cette dynamique, il convient aussi de noter que le monde militaire permet des investissements ciblés sur des segments de niche, ce qui peut ensuite entraîner des applications inédites dans le monde civil. D'un côté, la logique de rentabilité court terme et d'agilité, de l'autre côté l'investissement plus long terme et davantage de conservatisme pour garder une maîtrise permanente de ses moyens. Ceci dit, les révolutions technologiques s'enchaînent, et les distinctions évoquées ci-dessus tendent à s'effacer, en particulier dans la mesure où les conflits actuels sont souvent asymétriques, le « faible » recherchant dans la disruption provenant du monde civil un avantage sur le « fort » qui, lui, s'appuie sur son existant issu du monde militaire. On le voit en Ukraine, mais cela avait déjà été le cas en Irak ou en Afghanistan.

3/ Quelles sont les métamorphoses auxquelles nos armées doivent se préparer ?

L'objectif recherché par les armées est de détenir la capacité convergente d'analyse, d'intégration et de partage au sein d'un système qui orchestre les milieux (Terre, Air, Mer, Espace) et les champs (informationnel, électromagnétique,

cybernétique) entre eux, incarnant le bout-en-bout métier tactique-opératif-stratégique. Il s'agit de se doter d'une capacité de conduite et de commandement interarmées d'une opération OTAN interconnectant les différentes plateformes dédiées aux milieux ou aux champs, ce que l'on appelle le concept multi-milieu multi-champ (M2MC).
L'effet final recherché est de pouvoir transporter, partager, exploiter en temps réel, stocker, administrer et sécuriser des données via les services/applications métier standard, en mode « plug and fight » avec nos alliés et partenaires de circonstance d'une opération majeure.

Aujourd'hui, l'efficacité des armées est intrinsèquement dépendante de leur environnement numérique, primordial pour les opérations comme pour les activités organiques, qui ne cesse de s'étendre et de se complexifier. Cet environnement numérique constitue désormais :
– la trame de la connectivité (compréhension des situations) et du combat collaboratif en M2MC (multi-domaine multi-champ) ;
-la toile de l'interopérabilité technique, déterminante pour notre ambition nation-cadre (OTAN, coalition ad hoc, UE).
Au plan opérationnel, la maîtrise de notre environnement numérique est centrale pour « gagner la guerre avant la guerre ». Elle est liée aux 6 aptitudes structurantes des armées:
– moyen de la supériorité informationnelle et du renseignement préalable à l'action (Anticiper) ;
– maîtrise de la donnée, de la réactivité des forces et de l'orchestration des effets (Combattre), aptitude d'autant plus prégnante en engagement de haute intensité ;
– clé de l'intégration M2MC (Intégrer) ;
– facteur de continuité tout au long de la chaîne de commandement, de résilience des forces et des systèmes d'armes (Se protéger) ;
– moyen de renforcer l'assise organique des armées (flux logistiques, gestion des stocks, optimisation de la disponibilité des moyens, etc.) (Soutenir et durer) ;

– support propre au champ informationnel et trame du milieu cyber (Influencer).

Le numérique modifie le contexte militaire tout autant qu'il transforme notre société : rapidité de transmission d'informations, nouveaux espaces de conflictualité tels le cyberespace, mais aussi l'espace avec sa militarisation éventuelle et les menaces sur les différents satellites. Il convient donc de s'y adapter en permanence.

4/ Est-ce que l'une des manières de limiter l'exposition de nos données militaires à un ennemi potentiel n'est pas simplement d'en produire moins en nous montrant plus efficaces ? Le mot à la mode est sobriété, n'est-ce pas ?

Les données sont un avantage clé : les réduire serait se priver de moyens d'appréciation, de décision et d'action. La sobriété n'est pas dans la production de données, mais dans la consommation de ressources (matérielles, énergétiques) lors de leur utilisation.
Par contre, évidemment, il faut maîtriser et réduire au maximum la recopie multiple de la même donnée, et c'est dans une telle recherche d'efficacité (partage, mutualisation), qu'il convient de raisonner en termes de sobriété.

L'enjeu clé en termes d'exposition de nos données à un ennemi potentiel est en fait celui de la sécurité des données et de leur accès. Le chiffrement, la séparation des réseaux, l'étiquetage des données en y intégrant des attributs quant à leur droit d'accès (cf. modèle ABAC) sont des éléments de réponse technique.

5/ Si Gustave Le Bon revenait à la vie, quel chapitre ajouterait-il selon vous à sa Psychologie des Foules ?

L'ouvrage de Gustave Le Bon date de la fin du XIXe siècle et est terriblement moderne. Évidemment il ne connaissait pas les réseaux sociaux numériques, mais ses considérations sur la

psychologie des foules s'appliquent directement. Les communautés d'intérêt, ou les phénomènes de « like » ou de « bashing », répondent aux principes décrits par Gustave Le Bon : la foule n'est pas une simple somme de ses membres, mais développe une « âme », qui peut soit mener à un sentiment de « puissance » et à des actes violents qu'un individu n'aurait pas commis, soit mener à un « évanouissement » de la personnalité individuelle. En effet les utilisateurs des réseaux sociaux, qui se cachent derrière l'anonymat ou un pseudonyme, manifestent les traits d'irresponsabilité notés par Gustave Le Bon, face à leurs prises de position (si tant est qu'un commentaire jeté sur un réseau social est une véritable prise de position réfléchie et assumée). Gustave Le Bon n'aurait donc pas rajouté un chapitre, mais aurait trouvé dans certaines utilisations sociétales du numérique d'autres exemples pour illustrer ses considérations !

6/ Hors la menace armée, de quoi devons-nous nous défendre aujourd'hui ?

La Revue Nationale Stratégique, publiée en novembre 2022 par le Secrétariat Général de la Défense et de la Sécurité Nationale, rappelle les intérêts nationaux de sécurité :
– protection du territoire national ;
– sécurité des États en application des traités par lesquels nous sommes liés ;
– stabilité de notre voisinage compte tenu des répercussions immédiates que toute crise y émergeant aurait sur notre propre territoire, métropolitain comme ultramarin ;
– liberté d'accès aux espaces communs dont le cyberespace, mais aussi le spatial et les espaces aéromaritimes.

La cybersécurité, la cyberdéfense, plus généralement la résilience cyber, est donc affirmée comme clé pour maintenir l'autonomie de décision et d'action de la France qui, rappelons-le, est membre permanent du Conseil de Sécurité des Nations Unies, 7e économie mondiale contrôlant la 2e Zone économique exclusive, et est doté de l'arme nucléaire.

Les espaces communs (cyber, spatial, fonds marins et espaces aéromaritimes) font aujourd'hui l'objet d'une compétition de puissance renouvelée. Leur importance opérationnelle comme géographique croît alors que les règles communes qui les gouvernent sont insuffisantes, fragilisées ou contestées.

Sans rentrer dans le détail, en attaques physiques, il suffit de se remémorer entre autres les dommages récents subis par certains câbles sous-marins qui ont ralenti le trafic Internet pour certaines régions mondiales, les dommages sur des fibres terrestres en Allemagne récemment ou en France il y a 2 ans.
La menace est donc multiforme, d'où la nécessité de rechercher des réponses variées, ce qui nécessite de faire évoluer nos modèles d'armées.

7/ Le numérique de défense obéit-il à vos yeux aux lois de la science économique ou de l'économie politique ?

En temps de paix, ces lois s'appliquent nécessairement, dans la mesure où la politique d'un gouvernement est globale et ne se concentre pas uniquement sur l'aspect défense. C'est l'enjeu de nos modèles démocratiques de savoir raisonner ainsi globalement, écouter le citoyen tout en préservant les intérêts de l'Etat, répondre aux problématiques actuelles sans obérer l'avenir.
Évidemment, le numérique de défense pourrait profiter d'une augmentation budgétaire plus forte encore, mais cela se ferait alors au détriment d'autres choix, car les ressources budgétaires sont limitées par l'exercice de recherche d'équilibre politique et économique. Ce sont donc bien les règles de l'économie et de la politique qui déterminent les ressources disponibles pour le numérique de défense.

La situation serait tout autre en temps de guerre. Ceci dit, on serait alors dans un autre contexte politique et économique, avec d'autres lois. Donc, in fine, nonobstant ce changement de référentiel, on pourrait alors dire que l'on suivrait ces nouvelles lois !

8/ Les Armées pourraient-elles intégrer durablement et par défaut des solutions logicielles « souveraines », au point d'en nationaliser certaines ?

Que veut vraiment dire « nationaliser » ? Je pense qu'il faut plutôt poser la question en termes de définition de champions, par domaine, nationaux et/ou européens. Par ailleurs, ce n'est pas qu'une question qui préoccuperait potentiellement les Armées, c'est une question de défense et de résilience de l'État.

Le numérique s'exerce macroscopiquement dans trois domaines : les données qui sont le cœur de l'enjeu, les applications informatiques qui permettent leur traitement, et les réseaux qui transmettent les échanges au sein de l'espace numérique.

Chaque domaine a ses propres enjeux de maîtrise.
Pour les données, il faut en contrôler la quantité, la qualité, la propriété. Il faut maîtriser l'accès à ces données, ainsi que la perte des données, fût-elle intentionnelle ou pas.

Les applications informatiques nécessitent l'acquisition de calculateurs et logiciels de nouvelle génération ayant en particulier des capacités d'apprentissage, d'où des questions de maîtrise de la confiance de ces logiciels. Si l'on ne peut chercher à maîtriser l'ensemble de la chaîne des calculateurs (ceci dit, c'est ce que fait par exemple Amazon Web Services, construisant l'ensemble des ressources matérielles nécessaires pour fournir commercialement les services), la maîtrise de la définition et de la fabrication de certains composants électroniques est clé. Mais l'est tout autant la maîtrise de certaines matières premières, comme les terres rares ou autres éléments rentrant dans la composition des équipements électroniques. Si la découverte de gisements est possible (comme en Suède très récemment), c'est plutôt la voie du recyclage qu'il faudrait développer de manière intensive.

Enfin, pour les réseaux, la maîtrise physique de bout en bout

(terre, mer, air et espace) se décline au travers de leur sécurisation, de leur intégrité et de leur approvisionnement énergétique. N'oublions pas que le cyberespace n'est pas que virtuel et la couche de transport en est une empreinte physique majeure.

Tout ceci montre l'importance de la sécurisation et de la maîtrise de certaines technologies pour garantir la capacité à utiliser certains moyens d'action. Mais encore faut-il savoir les produire, et ensuite les distribuer et en rendre possible l'accès.
Une telle analyse doit se faire sur toute la chaîne de valeur du numérique : maîtrise des technologies ; maîtrise de la production de ces technologies, des produits et services associés ; maîtrise de la commercialisation et de la distribution des produits et services. Ces 3 dimensions sont à considérer, de la même manière qu'une maison a des fondations, des murs, et un toit.

Pour entamer un dialogue constructif avec l'industrie du numérique française, mais aussi avec certains établissements de recherche et de développement ainsi qu'avec des associations professionnelles et syndicales pour évaluer l'impact sociétal de certaines orientations, j'ai contribué à la création en 2022 du GINUM, le groupement des intervenants du numérique dans les domaines de la défense, de la sécurité et des enjeux d'importance vitale, pour un numérique souverain et responsable en France.

Les trois objectifs principaux du GINUM sont :
– fédérer l'expertise technologique, académique et industrielle des acteurs du numérique français ;
– organiser le dialogue entre institutionnels et acteurs du secteur ;
– promouvoir un numérique au bénéfice de la souveraineté et de la responsabilité sociétale et environnementale.

9/ Que vous inspire le fait que le US Special Operations Command n'ait aucun scrupule à faire usage des deepfakes dans le cadre de ses campagnes de déstabilisation ?

La Revue Nationale Stratégique souligne que certains États utilisent de plus en plus systématiquement l'arme cyber afin de défendre leurs intérêts stratégiques ou dans le cadre de tensions géopolitiques. Ces stratégies hybrides (attaques cyber et numérique, espace) exploitent la difficulté, pour la plupart des États démocratiques, d'apporter une réponse efficace compatible avec le respect des engagements, traités et principes politiques au fondement de l'ordre international.

Un de nos enjeux est donc d'accélérer, d'adapter, de compléter notre posture stratégique face à des menaces qui évoluent dans leur allure, dans leur nature et dans leur espace, dans un cadre de plus en plus marqué par ces stratégies hybrides ou de déni d'accès pour peser sur nos intérêts (exploitation des vulnérabilités des flux ou infrastructures logistiques, des espaces aéromaritimes). Ceci amène à de nouveaux modes de réponse : LID (lutte informatique défensive), LIO (lutte informatique offensive), et désormais LII (lutte informatique d'influence), qui s'exerce dans les différentes dimensions diplomatique, militaire, économique, mais aussi culturelle, sportive, linguistique, informationnelle.

Dans le champ de la lutte contre les manipulations de l'information venant de compétiteurs étrangers, la France doit disposer d'un large éventail d'options de réponse. En particulier, il y a un besoin d'outils de riposte tant juridiques que numériques contre les intermédiaires (« proxies ») que des puissances hostiles utilisent afin de démultiplier leurs actions de contestation ou de compétition, tout en maintenant un déni plausible.

Cette posture est d'autant plus nécessaire que des entreprises privées développent progressivement des capacités offensives,

des armes et des outils d'espionnage cyber sophistiqués prêts à l'emploi. Cette course à l'armement cyber accroît le risque d'escalade. La menace cybercriminelle, qui atteint un niveau inédit de sophistication et de désinhibition, constitue donc un défi stratégique pour notre sécurité nationale.

10/ L'atlantisme technologique qui affecte notre pays vous paraît-il aller dans le sens des intérêts de notre vieille nation ?

Je ne suis pas convaincu qu'il y ait un atlantisme technologique. Il est manifeste que dans le numérique, les champions Outre-Atlantique investissent massivement chaque année. Mais sur le strict plan des ressources budgétaires, l'Europe et certains de ses membres économiquement les plus favorisés pourraient tout autant le faire.
En fait, ce qui fait la différence, c'est qu'il n'y a pas forcément de volonté d'investir durablement, au-delà des changements de majorité, et c'est là le problème.

Une compétence dans le numérique se construit sur une décennie, avec une logique d'investissement qui ne doit pas souffrir d'à-coups. Pour avoir l'effet escompté, une telle politique doit, sur le plan financier, éviter tout saupoudrage et dispersion des efforts, et donc amener à des choix et des renoncements, assumés dans la durée.
Par ailleurs, n'oublions pas que la première société de pose de câbles sous-marins était française ; que le protocole TCP-IP faisant aujourd'hui fonctionner Internet est basé sur la commutation de paquets, idée française à l'origine ; que le Minitel était un concept disruptif et novateur préfigurant le déploiement généralisé futur de l'ordinateur individuel au sein de chaque foyer, ainsi que l'accès de tout public à des sites non institutionnels, tels les 3615 préfigurant les sites Internet de charme ; que Rhône-Poulenc était il y a 30 ans un des leaders de la chimie et du traitement des terres rares…
Donc ce n'est pas le potentiel d'innovation qui nous fait potentiellement défaut. C'est par contre une volonté

politique, qui ne se cacherait pas derrière l'illusion d'un libéralisme économique élevé au niveau européen, qui n'est pas compatible simultanément des logiques de rentabilité court terme et d'investissement long terme.

La clé du changement pour un redressement de notre industrie, tant au niveau national qu'européen : priorisation des moyens et mise en œuvre d'une politique industrielle cohérente. Cela passe par : revoir les dispositifs visant à mettre en synergies les acteurs publics et privés, définir des modes de gouvernance appropriés, et mettre en place des structures coopératives dans la durée.

Pour le mot de la fin, pour traiter la problématique de la souveraineté numérique, il faudrait l'organiser suivant un triptyque, avec une double logique de centralisation de la gouvernance et de décentralisation territoriale de l'exécution, la cohérence globale de la mise en œuvre de la politique publique étant garantie par la boucle de régulation.