Numérique et cyber : enjeux de souveraineté

Dominique LUZEAUX

Ingénieur général de 1re classe de l'armement, directeur de l'Agence du numérique de défense (AND).

Contexte géostratégique : la *Revue nationale stratégique*

La *Revue nationale stratégique*, publiée en novembre 2022 par le Secrétariat général de la défense et de la sécurité nationale (SGDSN) [1], 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, sont donc affirmées comme clés 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 (ZEE), et est dotée 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 les dommages subis en octobre 2022 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 deux ans. En attaques cyber, rappelons-nous en novembre 2015 l'attaque subie par l'aéroport d'Arlanda à

[1] SGDSN, *Revue nationale stratégique*, 2022, 56 pages (http://www.sgdsn.gouv.fr/).

Stockholm qui a perturbé le trafic aérien pendant de nombreuses heures, sans oublier les attaques sur certaines infrastructures énergétiques (distribution de carburant en Iran en 2022) ou sur des centrifugeuses de centrales. Ainsi, 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.

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.

La France doit intégrer l'inéluctabilité du rattrapage et de la dissémination dans le domaine technologique. Les GAFAM (Google, Apple, Facebook, Amazon et Microsoft) ou d'autres acteurs privés, s'imposent comme des acteurs non étatiques dont les contributions actives ou passives, par les outils qu'ils mettent à disposition, doivent être intégrées comme données d'entrée dès les phases de contestation.

En conséquence, la recrudescence de comportements inamicaux dans nos approches territoriales implique de disposer de moyens robustes de détection, remédiation et réponse, y compris dans l'Espace et dans le cyberespace. Ces capacités demandent ainsi à être renforcées et articulées dans le cadre de l'effort global de l'État pour affronter des crises de grande ampleur. Aucun moyen ne suffit pour envisager un bouclier cyber qui mettrait en échec toute cyberattaque menée contre la France, mais renforcer son niveau de cybersécurité est essentiel pour préparer le pays à davantage de menaces. De même, l'application d'une logique dissuasive dans le cyberespace qui forcerait tout attaquant à la retenue contre la France est illusoire mais adopter des stratégies de réponses mobilisant l'ensemble des leviers de l'État, européens et internationaux permet de rendre les cyberattaques particulièrement coûteuses pour les attaquants.

L'effort doit porter sur l'amélioration de notre résilience cyber. Celle-ci consiste à disposer de capacités adaptées et organisées, permettant de prévenir ou, le cas échéant, de réduire l'impact et la durée des cyberattaques menées à l'encontre de la France, *a minima* pour les fonctions les plus critiques.

Renforcer la résilience cyber et numérique

Les acquis fondamentaux du modèle français, établi en 2008 puis régulièrement renforcé et adapté, doivent être consolidés. La gouvernance de la sécurité numérique de l'État a été rénovée et peut désormais être déployée. La capacité nationale à concevoir et mettre en œuvre des politiques publiques est illustrée par la création d'Équipes régionales de réponse aux incidents (*CSIRT*), par l'ouverture du Campus Cyber et par l'émergence d'un écosystème de cyberdéfense à Rennes. Enfin, à l'issue de sa présidence du Conseil de l'Union européenne (janvier-juin 2022), la France est reconnue par ses pairs comme une référence sur les questions de cybersécurité.

Ceci dit, le niveau de cybersécurité de l'ensemble des services publics doit être fortement rehaussé. Cela passe par des actions à mener selon plusieurs axes, techniques, financiers, sociétaux, juridiques, politiques :

• **L'investissement dans des infrastructures résilientes :** consolider un socle numérique de l'État homogène et sécurisé, et renforcer les établissements et administrations encore trop fragiles (réseau physique dédié pour assurer une résilience des acteurs d'importance vitale en cas de crise, architecture multi-*cloud* pour la résilience des données vitales et administratives).

• **La mise en place d'un écosystème industriel souverain :** l'action de la France doit être démultipliée en s'appuyant sur un écosystème cyber public et privé dynamique. L'État ne peut agir seul sur les enjeux de cybersécurité et doit être en mesure de mobiliser l'ensemble des acteurs en cas de crise majeure. Il doit pouvoir exploiter les gisements de compétences disponibles au niveau des réservistes, mais aussi des retraités ayant travaillé au profit de cet écosystème cyber et numérique public et privé. L'effort doit également porter sur la responsabilité des fournisseurs de services numériques et la sécurisation des chaînes d'approvisionnement (stocks de matériels : des éléments actifs de réseau aux solutions de calcul et de stockage). Enfin, la France peut soutenir et favoriser l'apparition d'offres de confiance robustes et souveraines au niveau national comme européen.

• **La sensibilisation et la formation :** tous les acteurs du monde numérique doivent être formés et sensibilisés au risque cyber. Il s'agit de mobiliser le grand public, systématiser son intégration dans les cursus éducatifs et renforcer l'attractivité des métiers de la filière. Des actions sont à mener de type Bac Pro numérique, mais aussi en formation continue. Un effort particulier doit porter sur les départements, régions et collectivités d'outre-mer, du fait tant de leur position géostratégique que

de la nécessité de ne pas créer de fracture numérique entre la métropole et les DROM-COM : l'éloignement de certains territoires par rapport aux grandes voies mondiales du numérique peut être une vulnérabilité stratégique, qu'il faut compenser en investissements, d'une part en infrastructures (satellites, câbles sous-marins, fibres), d'autre part en éducation et formation.

• **Le développement d'un arsenal juridique et technique au service de la détection et de la riposte :** la France doit poursuivre son investissement sur le renseignement nécessaire à l'entrave des flux illicites ou déstabilisants avec un focus particulier sur les intangibles, particulièrement vulnérables aux actions cyber, tout en confortant ses capacités d'action pour contrecarrer ces flux illicites ou déstabilisants. 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.

• **La solidarité européenne :** la résilience de la France dépend de la sécurité et de la stabilité du cyberespace dans son ensemble. Il faut donc contribuer à la montée du niveau de résilience des institutions européennes, internationales et des partenaires de la France, ainsi que poursuivre la structuration d'un marché européen des produits et des services de cybersécurité. Sur la scène internationale, la France doit porter des propositions permettant d'encadrer le commerce et de lutter contre la prolifération des armes cyber, grâce notamment à une meilleure utilisation des outils de contrôle des exportations des biens et technologies. En complément, un référentiel commun de gestion de crise cyber, tout comme des mécanismes de coopération et d'entraide permettraient aux États d'éviter les risques d'incompréhension et d'escalade incontrôlée.

Le numérique : un enjeu de puissance et de souveraineté

Comme rappelé *supra*, la cybersécurité et le numérique ont bonne place dans la *RNS*, et contribuent directement aux fonctions stratégiques – dissuasion, prévention, protection, intervention, connaissance et anticipation, influence – sur lesquelles repose la stratégie de défense et de sécurité nationale. De plus, la souveraineté numérique est clairement un pan de la souveraineté économique et industrielle. Ce constat nous amène à nous questionner sur la politique à mettre en œuvre pour aboutir à la finalité recherchée : quels acteurs sont à préserver, à déployer, à développer ? Pour quelle durée l'État doit-il mettre en œuvre des mesures protectionnistes ? Quelle politique des brevets doit être dessinée pour garantir une protection des savoir-faire et des données, à des fins de production industrielle et d'exploitation commerciale ?

La réponse réside dans l'équilibre du choix politique entre indépendance et dépendance technologique. Ce juste degré d'interdépendance suppose d'avoir le choix entre différentes solutions technologiques viables au niveau national, puis européen, le cas échéant. Afin d'arbitrer sur ses propres choix capacitaires, l'État doit être en mesure de s'approprier et pérenniser les compétences de savoir-faire sur l'ensemble du spectre numérique.

Le cyberespace peut être divisé macroscopiquement en trois domaines : les données qui sont le cœur de l'enjeu, les applications 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. Les applications 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. 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.

Si l'on rentre un peu plus dans le détail de l'espace numérique, sans être dans la sophistication technique, il est possible de dégager les différentes couches suivantes avec certains enjeux clés :

- **La couche de l'électronique et les matériels**

– La vulnérabilité principale est la disponibilité des matières premières, et la sécurité de leur approvisionnement : une filière de recyclage adaptée pourrait alors dégager des marges de manœuvre.

– L'autre enjeu est la conception et fabrication de composants clés, et là encore se pose la question de la sécurité de leur approvisionnement comme on le voit actuellement : redévelopper des capacités nationales ou européennes dans le domaine est une réponse, adapter les stocks stratégiques en est aussi une.

- **La couche des infrastructures réseaux**

– L'intégrité des câbles sous-marins et terrestres, fibres, poteaux et antennes 3G/4G/5G a montré leur vulnérabilité et l'importance de leur sécurisation ; au vu des attaques régulières sur ces infrastructures et de leur impact en termes de disponibilité mais aussi de cybersécurité, on est en droit de se poser la question de la nécessité d'un réseau résilient, protégé, dédié aux opérations d'importance vitale de l'État. N'oublions pas que le cyberespace n'est pas que virtuel et la couche de transport en est une empreinte physique majeure.

– Si le conflit en Ukraine a montré l'apport opérationnel des satellites pour les communications en cas de crise, *via* la mise à disposition de 25 000 terminaux connectés à la constellation Starlink, cela démontre en même temps la dépendance totale par rapport à ces moyens et aux services associés, dont la disponibilité en termes géographiques et de performance est programmable à distance :

sans accès aux satellites, que ce soit par déni de service ou par destruction vu que l'Espace est devenu un sujet de tension et de concurrence militaire, plus de communications spatiales. Le projet européen *IRIS²* [2] et la capacité *GOVSATCOM* [3] sont une réponse clé à venir à ces préoccupations.

• **La couche des logiciels** (systèmes d'exploitation, environnements collaboratifs, plateformes d'accès, *Cloud*, etc.)

– La sécurisation de l'accès à ces technologies est critique au vu de la transformation numérique de notre société ; là encore, la problématique est celle de la sécurité d'approvisionnement des logiciels, et ce n'est pas qu'une question d'éditeurs propriétaires : un exemple récent concernant les logiciels libres est le blocage, pour des comptes dans certaines régions géographiques (Crimée, Iran), de Github qui permet justement l'accès aux logiciels libres nécessaires pour faire fonctionner les applications informatiques ; quand on évoque le *Cloud*, il ne faut pas uniquement se focaliser sur la protection des données que l'on y met, il convient aussi de maîtriser les technologies permettant d'y avoir accès et de le faire fonctionner : c'est une des faiblesses actuelles des démarches dites de confiance où l'on se concentre sur le contenu, en ignorant ou en feignant d'ignorer la problématique du contenant.

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. C'est *via* la considération de ces différents points que nous pouvons envisager de construire la souveraineté numérique nécessaire à notre autonomie stratégique. Encore faut-il l'organiser.

Un cadre pour construire la souveraineté numérique dans la durée

Pour élaborer un tel cadre, nous proposons de partir de ce qui existe déjà dans le domaine, en complétant et en s'inspirant de ce qui a été fait dans le secteur de l'énergie, où sécurisation, autonomie, souveraineté, résilience sont aussi des objectifs recherchés. Le cadre proposé repose sur la mise en place d'une organisation systémique, alliant approches descendante (« *top-down* ») pour la gouvernance et ascendante (« *bottom-up* ») pour la mise en œuvre, avec une boucle de régulation, et alliant forces vives publiques et privées pour en tirer les avantages de chacun. Cela conduit à une organisation sous forme d'un triptyque : gouverner (avec un

[2] Commission européenne, « IRIS²: the new EU Secure Satellite Constellation – Infrastructure for Resilience, Interconnectivity and Security by Satellite » (https://defence-industry-space.ec.europa.eu/).

[3] European Union Agency for Space Programme (EUSPA), « GOVSATCOM » (https://www.euspa.europa.eu/).

secrétariat général), réguler (avec une commission de régulation), administrer (*via* décentralisation territoriale et délégations de service public, avec coordination solidaire pour ne pas renforcer les fractures territoriales numériques).

Gouverner et conduire

Créer un Secrétariat général pour la souveraineté numérique (SGSN) permet une coordination étroite des instances de gouvernance. En effet, la mise en œuvre efficace d'une politique de souveraineté numérique passe par une organisation alliant d'une part, gouvernance et conduite, et d'autre part, centralisation des investissements et autonomie territoriale pour l'utilisation. Ceci évite tant la dispersion initiale des efforts technologiques et industriels en conception et réalisation, que l'inertie ultérieure due à un dirigisme excessif ou une méconnaissance de spécificités territoriales en exploitation et utilisation. Le SGSN aurait comme objectif de planifier les étapes de définition capacitaire et de construction budgétaire des axes de la politique de souveraineté numérique. Il aurait également pour mandat de piloter une politique industrielle performante dans la définition et l'exécution des projets structurants *via* leur responsabilité contractuelle.

Une des premières tâches du SGSN doit être de définir les capacités clés à maîtriser au niveau national, puis les articuler selon des chaînes de valeur cohérente. Un tel exercice de définition capacitaire, accompagné d'une veille stratégique permanente, permet alors de choisir quoi préserver, quitte à renoncer à certains domaines accessoires ou inaccessibles. Par exemple, au niveau des infrastructures numériques, il est nécessaire de développer un réseau dédié en vue de disposer de moyens de communication sécurisés et résilients, sur l'ensemble des territoires français. La mise en œuvre d'un réseau dédié renforcerait la maîtrise et la protection des infrastructures numériques dans les domaines vitaux de la santé, l'énergie, l'aéronautique et la défense.

Suite à cette réflexion capacitaire, il faut établir une cartographie des acteurs industriels et étatiques, tant sur les technologies maîtrisées que sur les secteurs de vulnérabilité des chaînes de valeur, afin d'appréhender l'empreinte française, voire européenne, dans l'espace numérique. Cette cartographie priorisera les besoins à court et moyen termes pour élaborer la construction budgétaire du réseau résilient des opérateurs d'importance vitale (OIV) de demain. Pour avoir l'effet escompté, une telle politique doit, sur le plan financier, éviter tout saupoudrage et donc amener à des choix et des renoncements, assumés dans la durée.

Enfin, le pilotage des projets structurants exige la priorisation des moyens et la 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, sans tomber dans le piège des structures intégratives. La définition

et la conduite des projets doivent être coordonnées *via* le SGSN, afin d'éviter des projets potentiellement concurrents favorisant la dispersion des efforts.

Administrer, opérer et exploiter

Autant la conduite des projets gagne à être centralisée pour pouvoir définir et mettre en œuvre une réelle politique industrielle et pour éviter des doublons potentiels, autant il faut décentraliser et confier à un acteur dédié la gestion, l'exploitation, le soutien des livrables des projets. Cet acteur pourrait être une entreprise (qui pourrait s'appeler RSF – Réseaux sécurisés de France), où seraient présents l'État et la Caisse des dépôts et consignations (CDC). Elle s'appuierait sur des ancrages territoriaux et opérerait dans le cadre d'une délégation de service public conforme à la politique industrielle numérique.

Dans le cadre de la gestion et l'exploitation de l'infrastructure, ses attributions seraient aussi d'entretenir, surveiller (en lien avec les *CSIRT* en cas d'incident de cybersécurité), moderniser et faire le lien avec les utilisateurs, ainsi que d'élaborer une tarification de l'utilisation des réseaux sécurisés numériques.

Dans le cadre du soutien, elle aurait également la responsabilité des migrations de l'existant, accélérant la transformation de l'État par le numérique et participant ainsi de l'ambition de France 2030 [(4)]. Concernant le financement de l'utilisation des livrables, il doit être à la charge de l'ensemble des acteurs publics (ministères, collectivités territoriales) et des OIV, avec une double logique de forfait de base (proportionnel à la taille de l'acteur concerné) complété par un coût à l'usage. Évidemment, la viabilité de l'ensemble de ces mesures repose sur un cadre législatif astreignant les acteurs concernés à l'utilisation des ressources déployées.

Réguler et normaliser

À l'instar du domaine de l'énergie, où a été mise en place la Commission de la régulation de l'énergie qui a une mission de régulation des réseaux, concourt au bon fonctionnement des marchés et est au service de la transition énergétique, il apparaît nécessaire de créer une Commission de régulation du numérique (CRN).

La CRN assurerait la surveillance de la gestion, la modernisation, le déploiement de l'infrastructure de réseau numérique. Outre la régulation des espaces numériques, elle serait le garant d'une cohérence globale des référentiels normatifs. En effet, le nombre de normes, référentiels, directives applicables au numérique croît en permanence, couvrant la protection des données (RGPD), l'accessibilité des applications (RGAA), la sécurité des systèmes d'information, l'utilisation de l'Intelligence artificielle (IA), etc.

[(4)] Ministère de l'Économie, des Finances et de la souveraineté industrielle et numérique, « France 2030 : un plan d'investissement pour la France », 18 novembre 2020 (https://www.economie.gouv.fr/france-2030).

La CRN aurait donc un rôle clé de cohérence d'ensemble, au service de la transition numérique sous ses différentes dimensions techniques, économiques, sociales, environnementales et de souveraineté. En particulier, elle participerait à certains travaux de normalisation menés au sein des forums internationaux correspondants, et mettrait en place les actions de régulation qui en découlent. Parmi les sujets d'importance pour ces activités, citons le *multi-cloud* avec une vision particulière liée à la protection des données personnelles et la sobriété énergétique, ainsi que le *edge-cloud* amené à représenter une nouvelle révolution des usages dans les années à venir avec le développement de l'*Internet* des objets (*IoT*) et l'hyperconnectivité.

Ces activités liées à la normalisation sont clé, car si la normalisation est une arme économique pour celui qui la manie, elle est aussi un vecteur de fragilité pour celui qui la subit. D'où l'impérieuse nécessité d'exercer cette volonté de normalisation à une échelle suffisante, *a priori* européenne plutôt que nationale. Par ailleurs, cela concourt indirectement au soutien à l'innovation technologique et au développement économique d'une partie de la filière numérique.

En guise de conclusion

Ce qui est en jeu est notre capacité à décider et notre capacité à agir. Dans le domaine militaire, ce sont respectivement d'un côté, la capacité d'anticipation et de renseignement ainsi que les processus décisionnels, de l'autre les forces et les capacités industrielles de recherche et de maîtrise des technologies pour les armements. Il en est de même dans le domaine du numérique ou de la cyber. La construction d'une souveraineté numérique nationale, amplifiée par la dynamique européenne, doit être le fruit d'une ambition politique forte. Les enjeux sont de taille, et il en est de la posture de la France, comme puissance politique et économique. ◆

Courriel de l'auteur : dominique.luzeaux@polytechnique.org

Mots-clés : Numérique, cyber, souveraineté, résilience.