Notes de l'Institut Synopia
N°35 – Février 2026

CYBERDÉFENSE : LA FRANCE EST-ELLE À LA HAUTEUR DES ENJEUX ?

Synthèse du Off de l'Institut Synopia avec l'amiral Arnaud Coustillière



1. Le cyberespace, nouveau champ de confrontation

Le cyberespace n'est désormais plus un simple support technique au service des activités économiques ou administratives. En l'espace de deux décennies, il est devenu un champ de confrontation à part entière, au même titre que la terre, la mer et l'air.

Pour les dirigeants publics et privés, ce basculement implique un changement radical de paradigme stratégique, car il redéfinit la nature même du conflit. La confrontation y est permanente, largement invisible et hybride, mêlant acteurs étatiques et non étatiques, opérations offensives et défensives, intérêts militaires, criminels, économiques et idéologiques, actions dans les champs immatériels et matériels. Dans cet état de conflictualité permanente, la frontière entre paix et crise a disparu et la nature des armes a changé ; l'arme principale devient l'information.

Ainsi, depuis les années 2010, toutes les grandes puissances militaires ont engagé une structuration méthodique de leurs capacités cyber et développé des dispositifs de cyberdéfense, chaîne opérationnelle complète – action bien sûr mais aussi protection, prévention, détection, réaction et remédiation – mobilisée en continu.

2. Un espace instable car faiblement régulé

Ce nouveau champ de confrontation constitue aujourd'hui une zone grise juridique. Contrairement aux domaines maritime ou aérien, encadrés par des décennies de normes et de jurisprudence stabilisées, le cyberespace n'est régi par aucun code de conduite international réellement structurant. Au sein des Nations Unies, les discussions et les tentatives de régulation n'ont débouché que sur des consensus limités, largement non contraignants.

Cette absence de régulation forte crée un environnement instable et propice au développement de la criminalité, entraînant un risque d'escalade incontrôlée. Les infrastructures numériques sont par nature complexes et transfrontalières, permettant aux outils d'attaque de circuler librement entre groupes criminels, mercenaires et acteurs étatiques ; des codes malveillants peuvent être réutilisés, modifiés et partagés, rendant l'attribution des attaques extrêmement complexe. Un État peut ainsi être tenté de répondre à une attaque sans être en mesure d'identifier formellement son auteur, avec un risque réel d'escalade.

L'absence de normes contraignantes sur le comportement des États, la volatilité juridique des flux numériques qui échappent aux frontières physiques, et la prolifération d'outils hybrides brouillant les responsabilités politiques permettent ainsi l'apparition de diverses menaces d'un genre nouveau.

3. Des menaces polymorphes : de la paralysie technique à la déstabilisation sociétale

Cette instabilité favorise l'émergence de menaces qui ciblent à la fois les infrastructures critiques et la cohésion sociale de nos démocraties.

Sur le plan technique, les attaques ne relèvent plus d'initiatives isolées mais sont devenues quasi industrielles et hautement sophistiquées. L'évolution observée depuis les années 2010 montre une professionnalisation croissante des attaquants et une recherche systématique d'effets stratégiques. Infiltrations persistantes et sabotages par malwares, exfiltrations massives de données sensibles, attaques par saturation des services ou encore rançongiciels structurés en véritables modèles économiques criminels : les modes d'action se multiplient et se perfectionnent pour neutraliser les systèmes et paralyser l'action étatique. Aucun secteur n'est épargné, des hôpitaux aux administrations centrales, en passant par les opérateurs d'importance vitale (OIV). L'épisode Stuxnet, l'essor des cryptolockers depuis 2018, l'usage des attaques cyber dans la guerre en Ukraine, ou encore la neutralisation des activités de la Poste et de France Travail dernièrement témoignent de cette prolifération des attaques cyber contre des infrastructures critiques.

Parallèlement, la désinformation s'est imposée comme une arme à part entière, qui dépasse largement la diffusion de fausses informations ponctuelles. Avec les progrès de l'intelligence artificielle, ces campagnes deviennent plus difficiles à détecter, plus crédibles et plus massives. Leur objectif est de fragmenter la cohésion nationale, d'éroder la confiance dans les institutions, les médias et entre les citoyens eux-mêmes. Autrement dit, la désinformation s'attaque au ciment qui fait tenir nos sociétés et nos démocraties, dans un but de division et de déstabilisation.

Ainsi, le cyberespace permet de profondes ingérences portées par des États, en premier lieu la Russie. Cependant, le virage stratégique opéré dernièrement par les États-Unis pourrait mener à une croissance importante du nombre d'ingérences américaines en Europe, facilitées par le soutien des entreprises américaines de la tech. Le cyber est devenu un instrument central des stratégies de puissance contemporaines, dans un contexte géopolitique de plus en plus incertain.

4. La réponse française : une architecture robuste et originale

Face à cette montée en puissance des menaces, la France a engagé, dès la fin des années 2000, une refondation méthodique et profonde de sa cyberdéfense. Partie d'une structure embryonnaire en 2009, elle s'est dotée en une quinzaine d'années d'une architecture institutionnelle complète et cohérente.

Dès 2009, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est créée au sein du Secrétariat général de la défense et de la sécurité nationale (SGDSN), rattaché au Premier ministre. Cette nouvelle cellule a vocation à renforcer la protection des administrations civiles et des opérateurs d'importance vitale, contribuant à une amélioration réelle de la résilience des grandes infrastructures telles que les OIV. Depuis 2021, elle se tourne vers les collectivités, les régions et les autres entreprises.

Le ministère des Armées est également réformé, notamment entre 2011 et 2017, avec la création du Commandement de la cyberdéfense (COMCYBER) sous l'impulsion de l'amiral Arnaud Coustillière. Cette initiative a permis de regrouper les capacités militaires cyber au sein d'une autorité interarmées permanente, intégrant à la fois des missions défensives et offensives. En parallèle, la création de la Direction générale du numérique (DGNUM) est venue structurer la gouvernance du numérique de défense, assurant le pilotage de la transformation numérique du ministère ainsi que la cohérence des systèmes d'information. Elle est aujourd'hui remplacée par le Commissariat Numérique de Défense (CND), regroupant toutes les entités en charge des projets et systèmes numériques du ministère.

Cette architecture repose sur un principe clé : la coordination interministérielle. La cyberdéfense française n'est pas uniquement militaire. Elle associe les armées, les forces de sécurité intérieure, les services de renseignement, les autorités judiciaires, ainsi que des structures spécialisées comme VIGINUM, qui lutte contre les ingérences informationnelles. Cette approche globale constitue l'un des principaux points forts du modèle français, souvent cité comme référence en Europe.

5. Une doctrine offensive sous contrôle politique et juridique

La lutte informatique offensive (LIO), qui correspond à l'emploi de capacités numériques afin de perturber, dégrader ou neutraliser les systèmes d'un adversaire, constitue un versant sensible de la cyberdéfense française. Cette capacité est pleinement reconnue comme un outil militaire à part entière, mais son emploi s'inscrit dans un cadre juridique et politique particulièrement strict des opérations militaires, reflet de la volonté de maîtrise de l'escalade et du respect du droit international.

En effet, l'action offensive dans le cyberespace relève des travaux de planification militaire, comme tout autre engagement des Armées, dont le cyber est une composante à part entière et doit donc coordonner son action avec celles des autres composantes – terre, mer, air, espace, forces spéciales –, validée au plus haut niveau de l'État. Chaque opération cyber comporte un risque d'escalade dans un environnement opaque et faiblement régulé.

Dans un environnement où les infrastructures sont transnationales et les outils largement mutualisés ou recyclés, il est très difficile d'identifier de manière certaine l'auteur d'une cyberattaque. Ainsi, la capacité dissuasive du cyber demeure intrinsèquement limitée, car les acteurs avancent masqués. La prolifération massive des compétences et des outils rend chaque acteur — étatique ou non — potentiellement offensif. Cette démocratisation de l'arme cyber affaiblit les mécanismes classiques de dissuasion, fondés sur l'identification claire de l'adversaire et la crédibilité de la riposte. Dans ce contexte, la doctrine française privilégie une approche prudente, fondée sur la maîtrise politique de l'emploi de la force, plutôt que sur une logique d'affichage ou de surenchère.

6. Faiblesses structurelles : capital humain et souveraineté numérique

Face à la montée en puissance des enjeux cyber, la France a certes su bâtir un système institutionnel solide et élaborer une stratégie encadrée. Cependant, deux faiblesses structurelles majeures limitent les capacités françaises en matière cyber.

La première concerne le capital humain. En effet, alors que la puissance cyber repose avant tout sur les compétences, la France, comme ses voisins, fait face à une pénurie de talents massive ; elle manque de professionnels formés pour protéger ses infrastructures critiques. Cette difficulté provient notamment de la faiblesse du socle mathématique dès l'enseignement initial, de la concurrence du secteur privé, notamment étranger, du manque d'attractivité des carrières publiques ainsi que de la sous-représentation des femmes dans les filières techniques, alors qu'elles représentent 50 % du vivier de talents mobilisable. Sans investissement de long terme dans la formation, la fidélisation et la diversification des profils, les capacités techniques et les effectifs resteront insuffisants face à l'ampleur des menaces.

À côté de ce défi humain, la seconde faiblesse française renvoie à un enjeu central de pouvoir et d'autonomie stratégique. Il s'agit de la souveraineté numérique, qui repose sur une interrogation fondamentale : qui contrôle réellement les outils – données, infrastructures et plateformes – dont dépend désormais l'ensemble de notre vie collective ? Aujourd'hui, les données françaises sont en grande partie hébergées par des infrastructures américaines, les plaçant de facto sous la loi de régimes juridiques extraterritoriaux tels que le Cloud Act. Ainsi, la souveraineté ne se décrète pas que par la norme ; elle se construit en premier lieu par le contrôle de l'architecture technique, et en particulier le Cloud. Le RGPD ou l'AI Act sont des outils vains si les serveurs et les câbles physiques échappent au contrôle européen. Dans un contexte de dérégulation croissante des plateformes numériques, cette situation expose les données françaises et européennes à des risques majeurs de captation et d'exploitation.

Or, en l'état actuel, ni la France ni l'Europe ne disposent des leviers nécessaires pour maîtriser leurs données et les usages qui en sont faits. Cette vulnérabilité est due au retrait de l'écosystème industriel français et européen face aux géants numériques américains, tant en capacité d'investissement qu'en rapidité d'innovation. Faute d'acteurs de taille adéquate et de financements suffisants, l'autonomie stratégique apparaît difficile à atteindre. Il est souvent plus simple, plus rapide et perçu comme moins risqué de recourir à des solutions « clés en main » étrangères que de développer des outils souverains. Pour acquérir la souveraineté numérique indispensable à notre sécurité, des efforts substantiels devront être fournis à la fois par les acteurs publics et privés.

Le revirement rapide de la posture stratégique américaine, dans laquelle l'Europe est devenue une cible à affaiblir, voire à démanteler, confère un caractère d'urgence à la correction de ce déséquilibre, qui de commercial est devenu stratégique.

7. IA générative, IA argentique et quantique : une course à la puissance de calcul

La France devra également continuer de faire évoluer sa stratégie cyber, afin de s'adapter aux progrès technologiques qui redéfinissent en permanence le cyberespace.

La prochaine étape concerne l'intelligence artificielle générative, qui agit déjà comme un accélérateur de conflictualité à double tranchant ; elle permet à la fois d'automatiser et d'accélérer l'élaboration des attaques, et d'améliorer les capacités de détection et de réponse aux menaces. Les prochaines avancées de l'IA générative pourraient ainsi inaugurer une guerre de vitesse algorithmique.

L'IA argentique, quant à elle, commence son déploiement ; elle va automatiser de façon autonome, via des agents IA, tous les traitements de l'information et booster la performance des organisations. Mais ces progrès se feront au prix d'une course à la puissance de calcul…

À plus long terme, la grande rupture attendue dans le domaine cyber est l'avènement du quantique qui, outre l'explosion des capacités de traitement des données, pourrait remettre en cause les fondements mêmes de la cryptographie actuelle. Sa puissance de calcul risque de rendre obsolètes tous les systèmes de chiffrement qui protègent aujourd'hui nos données, induisant une refonte complète de la sécurité telle que nous la connaissons.

8. La résilience numérique, clé de la souveraineté nationale

Face à toutes ces menaces, qu'elles soient actuelles ou à venir, un concept s'impose : la résilience numérique. Il ne s'agit plus de viser une sécurité totale illusoire, mais de garantir la capacité de la Nation à encaisser un choc systémique, à subir une attaque majeure sur ses services essentiels tout en continuant à fonctionner, même en mode dégradé. La question fondamentale aujourd'hui est donc la suivante : notre résilience collective est-elle à la hauteur des défis ? Défis qui doivent s'appréhender au niveau national pour la mise en œuvre, mais surtout au niveau européen pour fixer le cadre ; nombre de décisions se situent à la Commission Européenne.

Face à l'ampleur et la multiplicité des menaces, la défense n'est plus l'apanage de quelques experts ou de l'armée : elle concerne l'ensemble de la société. La préparation à une paralysie systémique devient une priorité absolue, car une attaque coordonnée sur les infrastructures critiques — énergie, transports, flux financiers — pourrait imposer un « fonctionnement en mode dégradé ».

Cette résilience dépasse le simple cadre des plans de sauvegarde informatique : elle représente un véritable changement de trajectoire pour les décideurs. Il s'agit de passer d'une recherche sécurité totale – inatteignable – à l'élaboration d'une stratégie de survie robuste, fondée sur des exercices de crise réguliers, la segmentation des fonctions critiques et la capacité à assurer la continuité nationale, même en cas de rupture des services numériques. C'est dans cette préparation collective, technique et humaine, que se joue la véritable souveraineté numérique de la France face aux défis du cyberespace.

* * * * *

CONCLUSION

La France dispose aujourd'hui d'une architecture cyber parmi les plus avancées d'Europe, fruit d'une vision stratégique précoce et cohérente. Pour autant, face à l'intensification des menaces, aux ruptures technologiques imminentes et aux fragilités humaines et industrielles persistantes, cette avance n'est pas suffisante. Les rapports de force sont globaux et mondiaux et de plus en plus brutaux. Sans réaction forte, l'Europe restera une colonie numérique des États-Unis, de plus en plus démembrée et spoliée.

La question n'est donc plus de savoir si la France a agi, mais si elle est prête à changer d'échelle et à peser de tout son poids dans les arbitrages de la Commission Européenne. Dans le cyberespace, la puissance se mesure moins aux déclarations qu'à la capacité à durer, à s'adapter et à encaisser les chocs. C'est dans cette perspective que la cyberdéfense, aux côtés de l'IA, doit être considérée comme un pilier central de la stratégie française de souveraineté numérique, à dimension européenne – car c'est à ce niveau que se joue la compétition numérique mondiale. Dès lors, cyber, IA et infrastructures numériques forment un triptyque indissociable de résilience nationale. Pour tenir dans la durée, la France doit disposer de capacités souveraines cohérentes et équilibrées dans ces trois domaines, à la fois complémentaires et stratégiquement inséparables.