

Texte
LAURA AUDEMAR

Géopolitique du numérique : **SE RÉARMER DANS LES NOUVEAUX RAPPORTS DE FORCE**

Le 8 avril, à l'Alliance Française, experts, responsables politiques et acteurs industriels se sont réunis pour aborder un enjeu désormais central : la géopolitique du numérique. Derrière cette notion se joue la maîtrise des infrastructures, des technologies et des données, dans un contexte marqué par l'intensification des rivalités entre puissances.

Comment reprendre le contrôle de nos infrastructures, de nos technologies et de nos données à l'heure des rivalités entre puissances ? Cette question était au cœur du colloque « Géopolitique du numérique », organisé par L'Hémicycle en partenariat avec

l'École de Guerre Économique, et accueilli à l'Alliance Française de Paris, le 8 avril dernier. Le numérique n'est plus seulement un levier de performance économique : il s'impose désormais comme un terrain de confrontation stratégique. « *La notion de souveraineté numérique a émergé en 2018, parce qu'on s'est aperçu que le numérique était un monde de prédation. Depuis le cloud, les grandes plateformes et l'IA, nous sommes dans un univers de désintermédiation et de captation* », contextualise l'amiral Arnaud Coustillière, président du Pôle d'Excellence Cyber.

GUERRE NUMÉRIQUE

Le politologue Gilles Kepel propose une lecture particulièrement incisive des recompositions en cours. Selon lui, les conflits contemporains franchissent un

seuil inédit : « *Cette guerre est la première véritable guerre numérique* », affirme-t-il, au sujet du conflit au Moyen-Orient. Cette mutation se traduit, selon lui, par une transformation des modes d'organisation militaires. « *Face aux bombardements américains ciblés, ils ont décentralisé le pouvoir militaire à travers tout le territoire. C'est leur stratégie de défense mosaïque, qui leur a permis de résister sur le terrain intérieur* », analyse-t-il, soulignant une logique de dissémination rendue possible par les outils numériques. Dans ce cadre, le numérique ne relève plus du seul registre de l'appui opérationnel ou économique : il devient un espace structurant des rapports de force. Les infrastructures numériques, en particulier dans les pays du Golfe, s'imposent désormais comme des actifs stratégiques à part entière, ces États ayant engagé des investissements massifs dans l'intelligence artificielle et les data centers. « *Les États du Conseil de coopération du Golfe avaient commencé à construire une transition post-pétrole vers l'intelligence artificielle et le numérique, notamment en attirant des data centers grâce à une énergie bon marché* », rappelle-t-il. Mais cette montée en puissance s'accompagne de nouvelles fragilités. « *Un simple drone peut aujourd'hui rendre inopérant un data center* », observe-t-il, mettant en évidence la vulnérabilité physique d'infrastructures

pourtant devenues centrales pour l'économie mondiale. De ce constat découle un basculement stratégique majeur : celui d'un numérique devenu simultanément capital, intensif et vulnérable : « *Le numérique, qui demande des investissements monstrueux, peut devenir l'arme du faible, avec des conséquences que nous n'avons pas encore mesurées* », conclut-il.

CÂBLES, SATELLITES, FRÉQUENCES : LES NOUVELLES LIGNES DE FRONT

Longtemps invisibles, les infrastructures du numérique – câbles sous-marins, satellites, data centers – s'imposent désormais au cœur des tensions géopolitiques. Pour Ophélie Coelho, chercheuse en géopolitique du numérique associée à l'Iris, ces équipements ne peuvent être appréhendés isolément : « *Nous sommes face à des modèles systémiques* », marqués par une « *concentration de nombreuses couches technologiques, du réseau jusqu'à la couche logicielle* ». Elle met en avant une double dynamique : d'un côté, une dépendance croissante des économies et des États ; de l'autre, une concentration du pouvoir, largement au bénéfice des États-Unis, où « *les entreprises s'inscrivent dans une logique soutenue par l'État* », tandis que l'Europe demeure fragmentée. Dans ce contexte, elle plaide pour une étape préalable : « *Cartographier nos dépendances* ». L'objectif est d'identifier les secteurs essentiels au fonctionnement des sociétés – santé, sécurité, éducation, administration, mobilité, énergie – afin de mieux en mesurer les vulnérabilités. Mais cette cartographie ne peut se limiter à une logique défensive. Elle doit également servir de levier pour une politique industrielle plus offensive : repérer les domaines où l'Europe dispose d'avantages, ceux où elle peut émerger, et transformer cette connaissance en capacité d'action – voire en instrument d'influence – dans l'écosystème numérique mondial. Didier Dillard, président-directeur général d'Orange Marine, rappelle que les câbles sous-marins, qui assurent l'essentiel du trafic mondial, constituent des vulnérabilités stratégiques majeures : « *Internet ne peut pas fonctionner sans les câbles sous-marins : ils sont l'épine dorsale des échanges* », souligne-t-il, même si les satellites jouent un rôle complémentaire. Didier Dillard met toutefois en garde contre un déséquilibre croissant : « *Les Gafam sont les plus grands propriétaires de câbles sous-marins* ». À l'inverse, les industriels qui les fabriquent et les armateurs comme Orange Marine – qui dispose de six navires câbliers sur une cinquantaine au total dans le monde – montrent

que l'Europe reste mieux représentée sur les segments industriels et opérationnels de cette chaîne critique. Dans le domaine spatial, Jean-François Fallacher, Président-Directeur Général d'Eutelsat, insiste sur le rôle « vital » des satellites. Face à Starlink, Eutelsat OneWeb – qui sont les deux constellations sur l'orbite terrestre basse – défend un modèle européen basé sur « *une gouvernance, une stabilité et une prédictibilité que d'autres n'ont pas* ». Il souligne, toutefois, une faiblesse majeure : la fragmentation européenne, qui limite la capacité du continent à rivaliser à grande échelle. « *Nos adversaires combinent satellites, câbles et cyberspace dans une même stratégie* », constate Guy-Philippe Goldstein, chercheur à l'École de Guerre Économique. Du prépositionnement aux attaques hybrides et jusqu'aux frappes visant à « aveugler » ou à imposer des coûts économiques, ces infrastructures sont désormais pleinement intégrées aux stratégies de puissance.

TECHNOLOGIES CRITIQUES : REPRENDRE LE CONTRÔLE DE NOS OUTILS STRATÉGIQUES

Derrière les infrastructures se déploient d'autres formes de dépendance, plus diffuses mais tout aussi structurantes : logiciels, composants, licences et chaînes d'approvisionnement. Elles révèlent une vulnérabilité majeure : la capacité d'usage. Mathilde Velliet, chercheuse à l'Ifri, décrit une « *confrontation technologique entre la Chine et les États-Unis* » marquée par la montée en puissance chinoise et une réponse américaine fondée sur le contrôle des flux technologiques. Dans ce contexte, les stratégies de « *dérisking* » reposent sur une cartographie fine des dépendances et la réduction ciblée des vulnérabilités. Frédéric Fauchère, directeur de la division BtoB mobile de Samsung Electronics France, insiste sur la nécessité de « *se soumettre à l'État de droit et au droit européen* », en apportant des « *preuves tangibles* » de conformité, de sécurité et de continuité de service. L'enjeu porte aussi sur le contrôle des chaînes de valeur et la gouvernance des partenariats stratégiques. Baptiste Cazagou, associé cyber chez Deloitte, explique que la prise de conscience tardive des entreprises est due, notamment, à « *la fascination des élites politico-économiques pour la Silicon Valley* ». Il plaide pour une approche hybride, consistant à distinguer les technologies critiques à maîtriser en propre et celles dont la dépendance peut être assumée, à partir d'un « *mapping des chaînes de dépendance* ».

→

DES OUTILS AUX DONNÉES : UNE VULNÉRABILITÉ SYSTÉMIQUE

Les dépendances numériques les plus critiques concernent également les infrastructures, les modèles d'intelligence artificielle, les plateformes économiques et les systèmes de données. Pour Isabelle Rauch, députée de la Moselle, l'enjeu est autant cognitif que technique : « *Que sommes-nous en capacité de confier à ces IA génératives ?* », alors que se pose le risque d'une perte d'esprit critique. La réponse passe, selon elle, par quatre leviers : conscientiser les dépendances, réguler, investir dans des solutions européennes et former aux usages de l'IA. Pour Sébastien Crozier, président de la CFE-CGC Orange, la vulnérabilité se concentre dans les plateformes structurantes, « *vitales pour l'autonomie stratégique* », notamment dans des secteurs comme la santé, les paiements ou les réseaux sociaux. Cédric Voisin, VP Platform & Security de Doctolib, rappelle que, pour une plateforme de santé, l'enjeu est aussi opérationnel car il s'agit « *d'améliorer l'accès aux soins et de rendre le temps du praticien plus efficace* », affirme-t-il, tout en garantissant le respect d'exigences fortes en matière de sécurité et de protection des données. Enfin, Sébastien Crozier défend une logique de souveraineté par la règle, estimant que « *les États*

peuvent imposer leurs règles aux acteurs qui opèrent sur leur territoire », et appelant à un cadre européen plus cohérent et plus exigeant.

« LE RÉARMEMENT NUMÉRIQUE EUROPÉEN »

En ce sens, Benjamin Haddad, ministre délégué chargé de l'Europe, appelle à un « *réarmement lucide, ambitieux, national et européen* », combinant sécurisation des chaînes de valeur, soutien aux technologies stratégiques et renforcement du marché unique, encore jugé trop fragmenté. S'il souligne la solidité de l'arsenal réglementaire européen, notamment avec le Digital Services Act, il met en garde contre une illusion : « *Celui qui impose l'usage, celui qui façonne la norme, c'est l'innovateur, c'est l'entrepreneur* ». L'Europe ne peut donc plus se limiter à un rôle de régulation et doit investir davantage dans l'innovation et les technologies critiques. Enfin, il fixe un horizon politique clair : « *D'ici 2030, avoir une Europe numérique autonome, innovante, sécurisée* ». L'Europe est désormais face à son destin : bâtir sa souveraineté ou devenir une « *colonie numérique* » des puissances étatiques, alerte le ministre. ▀

/

**« La cartographie ne peut se limiter
à une logique défensive mais servir de levier
pour une politique industrielle plus offensive.
Il s'agit de repérer les domaines où l'Europe
dispose d'avantages et de transformer cette
connaissance en capacité d'action dans
l'écosystème numérique mondial. »**

/