TRIBUNE

l'Opinion

Cette guerre que l'Europe refuse de voir

Le conflit en Iran montre l'importance du champ de bataille numérique. Pour une grande partie du monde occidental, cette réalité est encore mal comprise, estime Sébastien Crozier.



La guerre contre l'Iran a commencé sur le champ de bataille numérique. - Image générée par IA

Par Sébastien Crozier
président du think tank
Géopolitique du numérique

Publié le 21 Mai 2026

Lorsque les États-Unis et Israël ont déclenché l'opération « Epic Fury » contre l'Iran, le numérique n'a pas attendu les interventions militaires. Des cyber-opérations coordonnées ont précédé les frappes cinétiques : désorganisation des chaînes de commandement, brouillage des capteurs, paralysie des communications. Le général Dan Caine l'a confirmé : la coordination cyber-cinétique était au coeur du dispositif. La guerre n'a pas eu une dimension numérique : elle a commencé par là.

Le blackout comme instrument de contrôle

La réponse iranienne a été immédiate : couper internet. La connectivité est tombée à 2 % de son niveau normal. Quatre-vingt-dix millions de personnes plongées dans le silence, plus de 1200 heures de déconnexion. Internet n'est pas un espace neutre : c'est une infrastructure politique, structurée par des rapports de force entre États.

La déconnexion n'a pas suffi. Des équipements américains (Cisco, Juniper, Fortinet..) ont connu des redémarrages inattendus, accessibles via d'autres vecteurs. À Téhéran, une hypothèse s'impose : ces infrastructures pourraient intégrer des accès à distance. Qu'elle soit avérée ou surestimée, elle pose un principe que l'Europe peine à traduire en actes : le choix de l'origine d'un équipement réseau est une décision stratégique.

La déconnexion n'a pas suffi. Des équipements américains (Cisco, Juniper, Fortinet..) ont connu des redémarrages inattendus, accessibles via d'autres vecteurs. À Téhéran, une hypothèse s'impose : ces infrastructures pourraient intégrer des accès à distance. Qu'elle soit avérée ou surestimée, elle pose un principe que l'Europe peine à traduire en actes : le choix de l'origine d'un équipement réseau est une décision stratégique.

Câbles sous-marins et data centers : la vulnérabilité invisible

Les câbles du détroit d'Ormuz transportent une part significative du trafic mondial. L'Iran a laissé entendre qu'ils pourraient devenir des cibles. Début mars, trois centres de données d'Amazon aux Émirats et à Bahreïn ont été endommagés par des drones.

Ce basculement est majeur : des infrastructures critiques du numérique peuvent désormais être frappées par des moyens low tech, peu coûteux, mais augmentés par l'IA—navigation autonome, ciblage assisté, coordination en essaim. Ce n'est pas seulement de la cyberguerre : c'est une guerre hybride où le « hard tech » devient vulnérable à des systèmes légers, distribués et difficilement détectables.

Quelle doctrine, quelle surveillance, quelle résilience l'Europe a-t-elle pour protéger ses propres infrastructures numériques ?

Starlink et GPS : la connectivité sous contrainte

Environ 50 000 terminaux Starlink auraient été introduits clandestinement en Iran, à la demande de Donald Trump auprès d'Elon Musk pour soutenir les opposants. L'Iran a répondu par un brouillage de haute intensité, ciblant à la fois Starlink et les systèmes GPS dans le Golfe, perturbant plus la navigation de plus d'un millier de navires civils et même militaires. La guerre électronique s'inscrit désormais dans le même continuum que la cyberguerre.

Ce face-à-face révèle une réalité : une infrastructure critique peut dépendre d'un acteur privé, tandis que sa neutralisation relève des États en conflit, au détriment des populations civiles.

La saturation informationnelle comme stratégie

Des milliers de deepfakes ont circulé depuis le 28 février : faux bombardements, fausses destructions, fausse image du corps de Khamenei. Le New York Times en a identifié plus de 110 à message pro-iranien en quelques semaines. Les systèmes de Meta ont été dépassés.

L'enjeu n'est plus de convaincre, mais de saturer, de confondre, d'épuiser la capacité critique. La cognition devient un champ de bataille et les démocraties y sont structurellement plus exposées.

L'Europe face à l'épreuve de l’autonomie stratégique

Ce conflit n'est pas lointain. Il révèle, en temps réel, les vulnérabilités européennes : dépendance aux équipements étrangers, fragilité des câbles, des datacenters, concentration du pouvoir satellitaire, exposition des infrastructures critiques à des systèmes low tech augmentés, impuissance face à la désinformation algorithmique.

La question n'est pas de savoir qui va gagner. Elle est de savoir si la France et l'Europe sont prêtes à tirer les conséquences de ce qu'elles observent.

Construire une autonomie stratégique dans le numérique n'est plus une perspective de long terme. C'est une exigence immédiate. Chaque mois d'inaction accroît notre dépendance et réduit notre capacité à peser dans les rapports de force à venir.

Sébastien Crozier, président du think tank Géopolitique du numérique.

Cette guerre que l’Europe refuse de voir - l'Opinion

