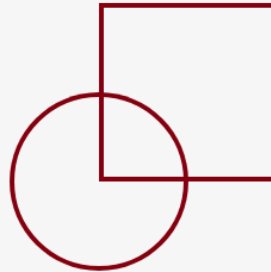
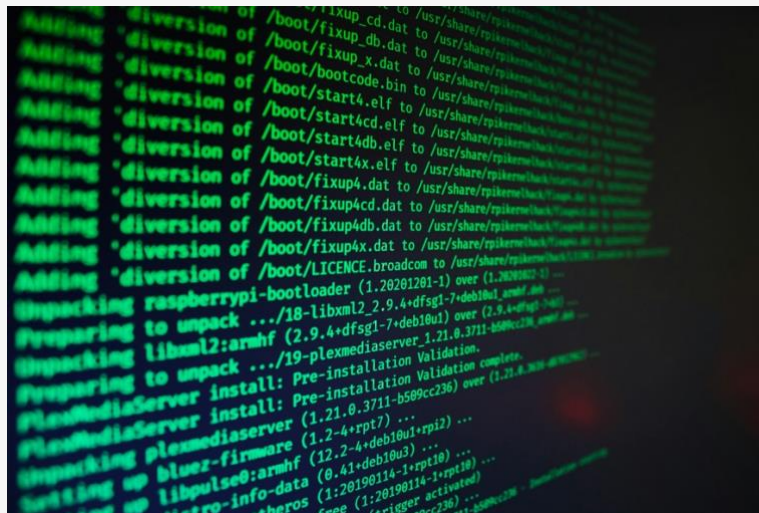


LES PAPIERS DE LA LIGNE FINE N°10



LA LIGNE FINE

Institut



Cyberguerre stratégique Série : Fondements Stratégiques

Auteurs : Alek UMONT
Date de publication : 9 avril 2026

Résumé exécutif

La cyberguerre occupe désormais une place permanente dans les doctrines de défense, les stratégies de sécurité nationale et la compétition entre puissances. Cette reconnaissance ne signifie pourtant pas que le cyberspace soit devenu un théâtre de guerre comparable, dans son fonctionnement, aux domaines terrestre, maritime ou aérien. Les opérations cyber ont des caractéristiques propres : elles peuvent être préparées longtemps avant leur emploi, reposer sur des infrastructures civiles utilisées quotidiennement par l'ensemble de la société, rester clandestines pendant plusieurs mois ou plusieurs années, être difficiles à attribuer immédiatement et produire des effets très différents selon la configuration technique précise de la cible. La notion de « cyberguerre stratégique » doit donc être utilisée avec suffisamment de précision pour distinguer l'espionnage informatique, la cybercriminalité, les opérations d'influence, le sabotage et l'emploi de capacités numériques directement intégré à une confrontation militaire.

L'importance stratégique du cyber ne vient pas principalement de la possibilité théorique de provoquer à distance l'effondrement d'un État. Les scénarios de paralysie générale des infrastructures nationales ont durablement structuré l'imaginaire associé à la cyberguerre, mais ils conduisent souvent à surestimer l'autonomie de l'instrument cyber et à sous-estimer les conditions nécessaires pour produire des effets durables. Une attaque contre une infrastructure complexe exige généralement une connaissance détaillée de son architecture, de ses dépendances et de ses procédures de fonctionnement. Les systèmes informatiques évoluent, les vulnérabilités sont corrigées, les accès sont détectés, les configurations sont modifiées et les opérateurs peuvent restaurer les services. Une capacité offensive n'est donc pas nécessairement reproductible à volonté : elle peut dépendre d'une vulnérabilité précise, d'un accès préparé longtemps à l'avance ou d'un ensemble de conditions techniques qui disparaissent après son utilisation.

La transformation décisive est ailleurs. La numérisation des administrations, des infrastructures critiques, des économies et des forces armées permet désormais aux États de rechercher en permanence des accès aux systèmes de leurs concurrents. Ces accès peuvent servir à collecter du renseignement, à cartographier les réseaux, à préparer des options de sabotage ou à soutenir des opérations militaires ultérieures. La même présence clandestine dans un réseau peut ainsi remplir plusieurs fonctions successives. Une intrusion initialement exploitée pour le renseignement peut être conservée afin de permettre une action différente en période de crise. L'État victime ne dispose pas nécessairement des éléments permettant de déterminer l'intention réelle de l'attaquant au moment où il découvre cette présence. Cette incertitude fait du repositionnement dans les réseaux une question stratégique à part entière.

La reconnaissance institutionnelle du cyberspace comme domaine d'opérations traduit cette évolution. L'OTAN reconnaît officiellement le cyberspace comme domaine d'opérations depuis le sommet de Varsovie de 2016. Son approche actuelle associe la protection de ses propres réseaux, le soutien aux opérations de l'Alliance, l'amélioration de la résilience nationale des Alliés et la possibilité de consultation et d'action collective. L'Alliance précise également qu'une cyberattaque suffisamment grave pourrait, selon les circonstances, conduire à l'application de l'article 5, sans définir un seuil automatique fondé sur une catégorie technique particulière¹².

Cette approche est cohérente avec la nature du domaine. Un incident cyber ne peut pas être évalué uniquement à partir de l'outil utilisé. Les conséquences, la cible, la durée de l'interruption, l'intention probable et le contexte politique déterminent sa portée. Une intrusion

¹ Allied Command Transformation. (n.d.). *Cyber defence*. NATO. <https://www.act.nato.int/activities/cyber/>

² North Atlantic Treaty Organization. (2024, July 30). *Cyber defence*. NATO. <https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence>

dans un serveur administratif, la compromission silencieuse d'un fournisseur de logiciels, une attaque provoquant l'arrêt temporaire d'un service public et une opération affectant directement un système militaire critique relèvent de niveaux de gravité très différents. La réponse politique doit donc être fondée sur les effets et les circonstances plutôt que sur une classification automatique de la technique employée.

La numérisation de l'économie élargit considérablement le périmètre de cette compétition. Une grande partie des infrastructures dont dépend un État appartient ou est exploitée par des entreprises privées : télécommunications, services cloud, logiciels, réseaux énergétiques, transports, plateformes logistiques, centres de données, systèmes de paiement ou équipements industriels. Les administrations et les forces armées utilisent elles-mêmes des technologies commerciales et des chaînes d'approvisionnement internationales. La distinction entre réseau militaire et environnement civil reste juridiquement importante, mais elle ne suffit plus à décrire la structure réelle des dépendances. Une attaque contre un fournisseur peut affecter simultanément plusieurs administrations, entreprises ou infrastructures ; inversement, la défense d'une capacité militaire peut dépendre de mesures prises par un acteur privé extérieur à la chaîne de commandement.

Le panorama des menaces publié par l'Agence de l'Union européenne pour la cybersécurité illustre l'ampleur de cet environnement. L'*ENISA Threat Landscape 2025* analyse 4 875 incidents survenus entre le 1er juillet 2024 et le 30 juin 2025. L'agence décrit un paysage dans lequel acteurs liés à des États, groupes criminels et hacktivistes utilisent des techniques parfois convergentes et exploitent les mêmes vulnérabilités ou infrastructures. Cette diversité complique la distinction entre les différentes formes de menace et oblige les autorités à analyser la finalité et le contexte des opérations plutôt que leur seul mode opératoire³.

La porosité entre acteurs étatiques et non étatiques représente un autre élément important. Les États peuvent conduire directement leurs opérations à travers leurs services de renseignement ou leurs forces armées, mais ils peuvent également bénéficier d'écosystèmes comprenant des entreprises, des groupes criminels ou des acteurs intermédiaires. Les relations entre ces groupes et le pouvoir peuvent être étroites, opportunistes ou volontairement difficiles à établir. En juillet 2026, le Conseil de l'Atlantique Nord a ainsi condamné ce qu'il qualifie d'activités cyber russes persistantes s'appuyant sur un « cyber ecosystem » pour viser des Alliés et partenaires. Ce type de formulation montre que l'analyse de la menace dépasse désormais la recherche d'une unité militaire ou d'un service de renseignement identifié et doit prendre en compte les relations plus complexes entre acteurs étatiques et réseaux extérieurs⁴.

La difficulté d'attribution ne signifie cependant pas que les opérations cyber soient anonymes par nature. Les gouvernements, services de renseignement, agences de cybersécurité et entreprises spécialisées disposent de moyens techniques et non techniques permettant de relier des campagnes à des acteurs déterminés. L'analyse peut prendre en compte les infrastructures utilisées, les méthodes d'accès, les familles de logiciels malveillants, les habitudes opérationnelles, les cibles choisies, les horaires d'activité ou des renseignements obtenus par d'autres sources. La question centrale devient le niveau de confiance nécessaire pour agir. Une évaluation interne peut suffire à prendre des mesures défensives avant qu'un gouvernement dispose des éléments qu'il estime nécessaires pour procéder à une attribution publique ou coordonnée avec ses partenaires.

Cette temporalité limite les modèles simples de dissuasion. La menace d'une riposte immédiate perd en crédibilité lorsqu'il faut d'abord établir l'origine d'une opération ou

³ European Union Agency for Cybersecurity. (2025, October 1). *ENISA threat landscape 2025*. ENISA. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>

⁴ North Atlantic Treaty Organization. (2026, July 13). *Statement of condemnation by the North Atlantic Council of Russia's malicious cyber activities*. NATO. <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2026/07/13/statement-of-condemnation-by-the-north-atlantic-council-of-russias-malicious-cyber-activities>

déterminer le niveau de responsabilité d'un État. La dissuasion cyber repose donc sur plusieurs mécanismes complémentaires : rendre l'attaque plus difficile, améliorer la détection, limiter les mouvements d'un attaquant déjà présent dans le réseau, restaurer rapidement les fonctions perturbées, attribuer les opérations lorsque les éléments sont suffisants et disposer d'une gamme de réponses ne se limitant pas nécessairement au cyberspace. Sanctions, mesures diplomatiques, poursuites judiciaires, opérations cyber et instruments militaires peuvent être combinés en fonction du niveau de gravité.

La politique de l'Union européenne met particulièrement l'accent sur la résilience et la gestion de crise. Le *Cyber Solidarity Act*, entré en vigueur le 4 février 2025, vise à renforcer les capacités européennes de détection, de préparation et de réponse aux incidents significatifs ou de grande ampleur. Il prévoit notamment un système européen d'alerte fondé sur des centres cyber nationaux et transfrontaliers et un mécanisme européen d'urgence. Une réserve européenne de cybersécurité composée de fournisseurs de services de réponse aux incidents doit pouvoir être mobilisée afin de soutenir les États membres, institutions et autres entités éligibles confrontés à des crises importantes⁵⁶.

Cette politique traduit une évolution utile de la conception de la cybersécurité. Aucun système suffisamment complexe ne peut raisonnablement être considéré comme inaccessible à tout adversaire. Les performances doivent donc être évaluées non seulement à partir de la prévention, mais aussi selon la rapidité de détection, la capacité à contenir l'intrusion, la protection des fonctions prioritaires et le délai nécessaire pour restaurer un service. La continuité de fonctionnement prend une valeur stratégique lorsque les infrastructures visées participent directement au fonctionnement de l'État ou de ses forces.

La résilience ne doit cependant pas être assimilée à une simple sauvegarde informatique. Les infrastructures critiques combinent souvent systèmes numériques, équipements physiques, procédures humaines et dépendances extérieures. Une attaque contre un environnement industriel peut modifier le fonctionnement d'un processus matériel ; son impact dépendra alors des dispositifs de sécurité, des possibilités d'intervention manuelle, des stocks disponibles, de la capacité des techniciens à rétablir l'installation et des éventuelles interdépendances avec d'autres secteurs. Une cyberopération capable de produire un effet physique important nécessite souvent une compréhension beaucoup plus précise de la cible qu'une campagne de vol de données ou de déni de service.

Ce rapport à la matérialité permet de préciser le rôle militaire du cyber. Les opérations numériques ne remplacent pas les moyens conventionnels ; elles peuvent en revanche améliorer leur efficacité lorsqu'elles sont coordonnées avec eux. Perturber un réseau logistique, retarder une transmission, compromettre certaines données ou limiter temporairement une capacité de communication peut avoir un effet opérationnel important si l'action intervient au moment où une force en dépend fortement. La valeur militaire d'une cyberopération ne peut donc pas être déduite uniquement de l'ampleur des perturbations techniques. Une action limitée mais correctement synchronisée peut présenter davantage d'intérêt qu'une campagne spectaculaire dépourvue de lien direct avec l'objectif militaire poursuivi.

L'évolution de l'OTAN confirme cette intégration. L'Alliance poursuit l'opérationnalisation du domaine cyber et a développé des exercices collectifs, dont *Cyber Coalition*, qui rassemblent personnels militaires, experts nationaux et partenaires afin de tester la coordination, le partage d'informations et la réponse aux incidents. L'édition 2025 a réuni environ 1 300 cyberdéfenseurs issus de 29 Alliés et de sept pays partenaires. Le NATO Integrated Cyber

⁵ European Commission. (2026, August 17). *EU Cyber Solidarity Act*. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity>

⁶ European Commission. (2025, August 26). *ENISA to operate the EU Cybersecurity Reserve*. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/news/enisa-operate-eu-cybersecurity-reserve>

Defence Centre doit également réunir des compétences civiles, militaires et industrielles afin d'améliorer la connaissance de situation et la résilience collective⁷⁸.

La dimension internationale reste néanmoins marquée par l'absence d'un régime de contrôle aussi précis que ceux développés historiquement pour certaines catégories d'armement. Les Nations unies ont progressivement construit un cadre de discussion sur les menaces, les normes volontaires de comportement responsable, les mesures de confiance, le renforcement des capacités et l'application du droit international. Le Groupe de travail à composition non limitée sur la sécurité des technologies de l'information et de la communication a achevé son cycle 2021-2025 avec l'adoption consensuelle d'un rapport final en juillet 2025. Un mécanisme mondial permanent consacré aux technologies de l'information et de la communication dans le contexte de la sécurité internationale a commencé ses travaux en 2026⁹¹⁰.

Ces évolutions ne suppriment pas les divergences entre États sur l'interprétation concrète du droit international, les seuils de gravité ou les modalités de réponse. Elles confirment cependant que le cyberspace est désormais intégré au débat sur la stabilité internationale et que la prévention des incidents majeurs ne peut pas relever uniquement de dispositifs techniques nationaux.

La cyberguerre stratégique doit par conséquent être analysée comme une composante permanente du rapport de force entre puissances, combinant renseignement, préparation, perturbation et intégration aux opérations militaires. Elle se distingue d'une guerre autonome parce que ses effets sont généralement dépendants d'infrastructures spécifiques et gagnent souvent leur portée lorsqu'ils sont articulés à d'autres instruments. Elle se distingue également de la simple cybersécurité parce que les États ne cherchent pas seulement à protéger leurs propres réseaux : ils développent des capacités leur permettant de comprendre, pénétrer et, si nécessaire, affecter ceux de leurs concurrents. La question principale devient alors celle de l'équilibre entre deux exigences simultanées : conserver des options d'action dans les systèmes adverses et réduire suffisamment les vulnérabilités nationales pour qu'une opération adverse ne puisse pas provoquer un effet politique ou militaire disproportionné.

⁷ Allied Command Transformation. (2025, December 5). *NATO Cyber Coalition 2025: Advancing cyber defence and strengthening Alliance resilience*. NATO. <https://www.act.nato.int/article/cyber-coalition-2025/>

⁸ North Atlantic Treaty Organization. (2025, October 9). *NATO Secretary General at Cyber Defence Conference 2025: "No one stands alone in NATO"*. NATO. <https://www.nato.int/en/news-and-events/articles/news/2025/10/09/nato-secretary-general-at-cyber-defence-conference-2025-no-one-stands-alone-in-nato>

⁹ United Nations, Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025. (2025, July 1). *Final report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025 [Draft]* (A/AC.292/2025/L.1). United Nations. <https://digitallibrary.un.org/record/4084927>

¹⁰ United Nations. (2025, July 14). *Statement attributable to the Spokesperson for the Secretary-General – on the conclusion of the Open-ended Working Group on security of and in the use of information and communications technologies 2021–2025*. <https://www.un.org/sg/en/content/sg/statements/2025-07-14/statement-attributable-the-spokesperson-for-the-secretary-general-the-conclusion-of-the-open-ended-working-group-security-of-and-the-use-of-information-and>

Problématique

Le développement des capacités cyber a profondément élargi les moyens dont disposent les États pour recueillir du renseignement, perturber une infrastructure ou préparer une opération militaire. Cette évolution n'a pourtant pas produit une définition stabilisée de la « cyberguerre ». Le terme peut être employé pour qualifier une campagne d'espionnage, une attaque par ransomware contre un hôpital, une intrusion dans une administration publique, une opération visant une infrastructure énergétique ou une action directement intégrée à une campagne militaire. Une catégorie aussi large finit par réunir des opérations dont les finalités, les auteurs et les conséquences sont trop différentes pour être analysées de la même manière.

La distinction doit d'abord être faite à partir de l'objectif poursuivi. L'espionnage cherche à obtenir des informations. Il peut viser des secrets militaires, des données diplomatiques, des technologies, des négociations commerciales ou des informations personnelles susceptibles d'alimenter d'autres opérations. Le sabotage vise à altérer ou interrompre une capacité. La cybercriminalité recherche principalement un avantage financier. L'influence agit sur l'environnement informationnel et sur les perceptions. Le prépositionnement consiste à maintenir un accès permettant une action future. Les mêmes outils ou vulnérabilités peuvent apparaître dans plusieurs de ces activités, mais leur signification stratégique n'est pas identique.

La possibilité de passer d'une fonction à l'autre rend toutefois la distinction moins nette qu'elle ne l'est dans d'autres domaines. Une présence clandestine dans un système informatique peut être utilisée pendant plusieurs mois pour collecter des renseignements puis devenir, en période de crise, le point de départ d'une opération destinée à modifier ou supprimer des données. L'État victime peut découvrir l'intrusion avant que l'auteur n'ait activé cette seconde fonction. Il doit alors décider comment traiter une capacité dont l'intention exacte reste incertaine. Cette question devient particulièrement sensible lorsque l'accès concerne une infrastructure essentielle ou un système militaire.

L'importance du prépositionnement tient à la temporalité des opérations. Une cyberattaque complexe ne peut pas toujours être conçue après le début d'une crise. L'attaquant doit avoir identifié la cible, compris son architecture, trouvé ou créé une voie d'accès, maintenu cet accès malgré les mises à jour et vérifié que l'effet recherché reste possible. Une option cyber peut donc exiger plusieurs mois de préparation. La compétition se déroule en conséquence bien avant que l'emploi politique de la capacité soit décidé.

Cette situation transforme la relation entre renseignement et opération offensive. Dans plusieurs cas, la première étape est identique : accéder au système sans être détecté. La différence porte sur ce que l'acteur fait ensuite de cet accès. Les services de renseignement et les forces cyber peuvent donc poursuivre des objectifs étroitement liés, ce qui explique l'importance accordée à la coordination entre renseignement technique et planification militaire.

Le second problème concerne l'effet stratégique. Les cyberattaques sont régulièrement évaluées à partir de leur ampleur technique : quantité de données volées, nombre d'ordinateurs affectés, durée d'un déni de service ou coût financier estimé. Ces indicateurs sont utiles mais ne suffisent pas à déterminer la portée stratégique d'une opération. Une attaque touchant plusieurs milliers de postes de travail peut rester politiquement limitée si l'organisation dispose de sauvegardes et restaure rapidement ses fonctions essentielles. Une perturbation beaucoup plus réduite peut produire un effet militaire important si elle intervient sur un système critique à un moment précis.

Cette différence oblige à replacer la cyberopération dans son contexte. Dans une confrontation militaire, l'intérêt d'une attaque contre un réseau ferroviaire ne dépend pas seulement du nombre de trains retardés : il dépend de la relation entre ce réseau et les mouvements de forces ou de matériel au moment de l'opération. Une perturbation de communications n'a pas la même valeur selon qu'elle intervient dans une période de faible activité ou pendant une phase décisive d'une campagne. Le cyber agit ainsi sur des fonctions dont la valeur varie avec la situation stratégique.

La troisième difficulté est liée à la persistance de l'effet. Une infrastructure détruite par une frappe conventionnelle nécessite généralement une réparation physique. Un système numérique peut parfois être restauré beaucoup plus rapidement si les sauvegardes sont disponibles, si les composants matériels sont intacts et si l'organisation a correctement préparé la reprise. Cette caractéristique réduit la capacité de certaines cyberopérations à produire des effets prolongés. L'attaquant peut devoir maintenir son action, disposer de plusieurs accès ou combiner l'opération numérique avec une action physique afin d'empêcher la restauration.

À l'inverse, une compromission discrète peut rester utile pendant longtemps si elle n'est pas détectée. Le cyber présente donc une différence notable entre opérations clandestines et opérations destructives : l'accès peut posséder une durée de vie longue tant qu'il reste secret, tandis qu'une capacité offensive révélée par son emploi peut perdre rapidement sa valeur. Une vulnérabilité exploitée peut être corrigée dès que l'attaque est analysée. L'emploi d'un outil comporte par conséquent un coût d'opportunité. Un État peut choisir de conserver un accès pour une crise plus grave plutôt que de le révéler pour obtenir un avantage limité à court terme.

Ce calcul explique en partie pourquoi l'espionnage et le prépositionnement sont beaucoup plus fréquents que les cyberattaques stratégiques destructives. Une opération d'espionnage peut fournir continuellement du renseignement sans obliger l'acteur à révéler toutes les possibilités techniques dont il dispose. Une attaque majeure détruit souvent une partie de la valeur future de la capacité utilisée, puisque la victime dispose ensuite d'informations pour corriger les vulnérabilités ou modifier son architecture.

La quatrième difficulté porte sur l'attribution. Une cyberopération traverse généralement plusieurs infrastructures et peut utiliser des systèmes compromis appartenant à des tiers. L'adresse technique d'origine n'identifie donc pas directement l'auteur réel. L'analyse doit reconstruire la campagne à partir d'un ensemble d'indices et, lorsque cela est possible, les combiner avec des informations de renseignement non publiques.

L'attribution doit également distinguer l'auteur technique et la responsabilité politique. Un groupe peut être directement intégré à un service étatique, agir pour son compte, coopérer ponctuellement avec lui ou poursuivre ses propres objectifs dans un environnement où les autorités choisissent de ne pas intervenir. Cette diversité permet aux États de bénéficier d'un certain niveau d'ambiguïté, mais elle complique aussi leur propre contrôle sur les opérations menées depuis leur territoire ou par des groupes qui leur sont proches.

Les prises de position collectives de l'OTAN contre des activités cyber attribuées à la Russie montrent que l'attribution est de plus en plus utilisée comme instrument diplomatique. En juillet 2026, l'Alliance a publiquement lié plusieurs activités malveillantes à un environnement cyber russe et les a qualifiées de menace pour la sécurité alliée. Une telle déclaration ne constitue pas seulement un diagnostic technique ; elle cherche également à réduire la possibilité pour l'auteur présumé de bénéficier durablement de l'ambiguïté et à montrer que les Alliés peuvent coordonner leur appréciation politique¹¹.

¹¹ North Atlantic Treaty Organization. (2026, July 13). *Statement of condemnation by the North Atlantic Council of Russia's malicious cyber activities*. NATO. <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2026/07/13/statement-of-condemnation-by-the-north-atlantic-council-of-russias-malicious-cyber-activities>

La cinquième difficulté concerne le seuil entre compétition et conflit. Les États acceptent depuis longtemps l'existence de l'espionnage, même s'ils cherchent à l'empêcher. Le vol massif d'informations par des moyens numériques peut être considéré comme hostile sans être traité comme une attaque armée. Le sabotage pose une question plus délicate lorsque ses conséquences deviennent comparables à celles d'une action militaire. L'OTAN maintient volontairement une marge d'interprétation en indiquant que les cyberactivités peuvent, dans certaines circonstances, conduire à la défense collective, mais sans établir un seuil technique fixe. Cette approche permet d'évaluer l'effet réel de l'opération plutôt que de créer une règle qu'un adversaire pourrait chercher à contourner¹².

La problématique centrale n'est donc pas de déterminer si le cyber peut être utilisé comme une arme, ce qui est déjà établi, mais de comprendre comment des capacités préparées en permanence dans les réseaux adverses peuvent être intégrées à une stratégie de puissance sans que la compétition quotidienne ne conduise mécaniquement à une escalade. Cette question oblige à analyser ensemble l'offensive et la défense : la valeur d'une option cyber dépend de la capacité à obtenir un accès chez l'adversaire, tandis que la vulnérabilité nationale dépend du temps nécessaire pour détecter, contenir et restaurer après une intrusion similaire.

Contexte structurel

La cyberguerre stratégique s'inscrit dans un environnement numérique qui n'a pas été conçu comme un champ de bataille. Internet, les réseaux d'entreprise, le cloud, les logiciels professionnels et une grande partie des infrastructures numériques ont d'abord été développés pour permettre la communication, l'automatisation, le stockage et l'échange de données. Leur intégration progressive à presque toutes les fonctions économiques et administratives a ensuite créé une surface d'exposition beaucoup plus large. La sécurité nationale dépend aujourd'hui de systèmes dont une proportion importante appartient à des acteurs privés, utilise des composants internationaux et évolue selon des cycles industriels qui ne correspondent pas nécessairement aux temporalités de la défense.

La numérisation des infrastructures critiques

Les infrastructures énergétiques, les transports, les télécommunications, les services financiers, la santé et les administrations reposent tous sur des systèmes numériques dont l'importance varie selon les fonctions. Cette dépendance ne signifie pas que tous les secteurs puissent être neutralisés de la même manière. Les architectures techniques sont différentes, les niveaux de segmentation varient, les dispositifs de secours ne sont pas identiques et certains processus peuvent être maintenus manuellement pendant une interruption. Une stratégie de cyberdéfense doit donc éviter une approche uniforme des « infrastructures critiques » et identifier précisément les fonctions dont l'arrêt produirait des conséquences en chaîne.

Le paysage européen décrit par l'ENISA montre la diversité de ces menaces. Les 4 875 incidents analysés dans son rapport 2025 couvrent des modes opératoires et des acteurs très différents, et l'agence souligne la convergence de certaines techniques employées par groupes criminels, hacktivistes et acteurs liés à des États. L'existence de menaces nombreuses et hétérogènes impose aux organisations de maintenir un niveau de défense permanent, même lorsqu'aucune crise géopolitique particulière n'est en cours¹³.

¹² North Atlantic Treaty Organization. (2024, July 30). *Cyber defence*. NATO. <https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence>

¹³ European Union Agency for Cybersecurity. (2025, October 1). *ENISA threat landscape 2025*. ENISA. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>

Cette situation a une conséquence stratégique importante : les capacités défensives mobilisées contre la criminalité ou les incidents ordinaires participent également à la préparation d'un État contre des opérations plus graves. Une bonne gestion des identités, des mises à jour, des sauvegardes, de la segmentation ou de la journalisation ne distingue pas entre un attaquant criminel et un service de renseignement. Les mêmes pratiques peuvent empêcher ou limiter plusieurs catégories de menace. La défense nationale bénéficie donc directement d'un niveau général élevé de cybersécurité dans l'économie.

Les chaînes d'approvisionnement numériques

La sécurité d'un réseau dépend de composants, logiciels et prestataires auxquels l'organisation accorde différents niveaux de confiance. Une entreprise peut protéger correctement son infrastructure interne tout en utilisant un produit vulnérable ou un fournisseur compromis. Les attaquants peuvent donc chercher à pénétrer une cible par l'intermédiaire de sa chaîne d'approvisionnement plutôt qu'en l'attaquant directement.

Cette approche peut être particulièrement attractive lorsqu'un fournisseur dessert un grand nombre d'organisations. La compromission d'un produit largement utilisé permet potentiellement d'obtenir plusieurs accès à partir d'une même opération initiale. La concentration de certains marchés technologiques augmente donc l'importance stratégique des politiques de sécurité de quelques entreprises.

L'Union européenne tente de réduire ce risque par plusieurs instruments réglementaires. Le *Cyber Resilience Act* impose des exigences de cybersécurité aux produits comportant des éléments numériques et cherche notamment à renforcer la sécurité dès la conception et pendant le cycle de vie. La Commission a également proposé en janvier 2026 une révision du *Cybersecurity Act* visant, entre autres, à renforcer la sécurité des chaînes d'approvisionnement des technologies de l'information et de la communication¹⁴¹⁵.

Ces politiques ne permettent pas d'éliminer le risque. Elles cherchent à réduire le nombre de vulnérabilités évitables et à organiser la responsabilité des acteurs. Leur intérêt stratégique tient à l'effet cumulatif : un écosystème dans lequel les produits sont maintenus plus longtemps, les vulnérabilités corrigées plus rapidement et les obligations mieux définies augmente le coût nécessaire pour conduire une campagne durable.

L'imbrication civil-militaire

Les forces armées disposent de réseaux protégés et de systèmes spécifiques, mais leurs activités utilisent également les infrastructures générales de l'économie. Les personnels communiquent, les chaînes logistiques utilisent des logiciels commerciaux, les fournisseurs de défense dépendent de services cloud ou de télécommunications et les bases industrielles comportent de nombreux sous-traitants. Une architecture strictement militaire peut donc être sécurisée tout en restant dépendante de systèmes extérieurs plus vulnérables.

Cette situation rend nécessaire une conception élargie de la cyberdéfense. Protéger uniquement les réseaux classifiés ne suffit pas si la mobilisation ou la continuité des opérations dépendent d'infrastructures civiles facilement perturbables. Les exercices de crise européens commencent précisément à intégrer ce type de problématique, en testant des scénarios dans lesquels plusieurs secteurs économiques sont affectés et doivent coordonner leur réponse.

¹⁴ European Commission. (2026, September 7). *Cyber Resilience Act*. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act>

¹⁵ European Commission. (2026, January 20). *Proposal for a Regulation for the EU Cybersecurity Act*. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act>

L'OTAN suit une logique similaire en cherchant à rapprocher acteurs civils, militaires et industriels au sein du NATO Integrated Cyber Defence Centre. Le projet vise à améliorer la connaissance de situation collective et la coopération entre des organisations qui détiennent chacune une partie des informations nécessaires pour comprendre une campagne¹⁶.

Une compétition sans phase de mobilisation clairement identifiable

Une campagne cyber importante peut être préparée sans mouvements visibles de forces. Les premières étapes consistent souvent à identifier les technologies utilisées, collecter des informations sur les employés, rechercher des vulnérabilités et construire des accès. Une partie de ces activités peut ressembler à des opérations criminelles ordinaires ou à de l'espionnage classique. Les indicateurs stratégiques sont donc moins visibles que dans plusieurs domaines militaires.

Cette absence de mobilisation clairement identifiable ne signifie pas qu'aucun signe précurseur ne puisse être détecté. Les services peuvent observer une augmentation des scans, du phishing, des tentatives d'accès ou d'autres comportements. Mais ces phénomènes sont suffisamment fréquents en temps normal pour que leur interprétation reste difficile. L'enjeu devient celui de la corrélation : plusieurs signaux faibles peuvent acquérir une signification lorsqu'ils sont rapprochés d'informations politiques, militaires ou de renseignement.

La cyberdéfense doit par conséquent fonctionner à un rythme permanent. Il n'est pas réaliste de maintenir un niveau faible de sécurité en temps de paix puis de renforcer rapidement la protection quelques jours avant une crise. Si un adversaire est déjà installé dans les réseaux, l'amélioration tardive des contrôles peut ne pas suffire. Les audits, exercices et opérations de recherche de compromission doivent donc avoir lieu avant que la nécessité politique soit évidente.

L'évolution rapide des technologies

Le renouvellement constant des technologies constitue une contrainte particulière. Les systèmes sont mis à jour, de nouveaux services cloud sont adoptés, des équipements deviennent obsolètes et de nouvelles dépendances apparaissent. Cette évolution peut supprimer un accès adverse mais également introduire des vulnérabilités inattendues. La sécurité n'atteint donc jamais un état stable.

L'intelligence artificielle accentue cette dynamique. Elle peut accélérer certaines tâches offensives telles que l'analyse de données, la préparation de messages d'ingénierie sociale ou la recherche de configurations vulnérables. Elle peut aussi renforcer la défense en facilitant la détection d'anomalies, l'analyse d'événements ou la priorisation des alertes. Son impact stratégique dépendra moins de la simple disponibilité des modèles que de leur intégration aux opérations et de la qualité des données auxquelles les acteurs ont accès.

Il faut éviter d'en déduire que l'automatisation supprimera les contraintes fondamentales des opérations complexes. Produire un effet physique précis sur une infrastructure industrielle nécessite toujours de comprendre l'environnement ciblé. Maintenir un accès clandestin continue de dépendre de la discipline opérationnelle et de la connaissance de l'architecture. L'intelligence artificielle peut réduire certains coûts, mais elle ne rend pas automatiquement interchangeables les cibles ou les campagnes.

¹⁶ North Atlantic Treaty Organization. (2025, October 9). *NATO Secretary General at Cyber Defence Conference 2025: "No one stands alone in NATO"*. NATO. <https://www.nato.int/en/news-and-events/articles/news/2025/10/09/nato-secretary-general-at-cyber-defence-conference-2025-no-one-stands-alone-in-nato>

Rapports de force

Comparer les capacités cyber est beaucoup plus difficile que comparer des flottes navales ou des forces aériennes. Les capacités les plus importantes sont généralement secrètes, précisément parce que leur valeur dépend de la non-divulgaration. Un État ne publie pas la liste des vulnérabilités qu'il peut exploiter, des réseaux auxquels ses services ont accès ou des outils qu'il conserve pour une situation de crise. Les indicateurs publics doivent donc être interprétés avec prudence.

La puissance cyber peut néanmoins être analysée à partir de plusieurs facteurs : qualité des services de renseignement, volume de personnels qualifiés, profondeur du secteur technologique, accès aux infrastructures mondiales, relations avec les fournisseurs, niveau de cybersécurité de l'économie nationale, capacité de coordination entre agences et aptitude à intégrer les opérations cyber à une stratégie plus large.

Les États-Unis : capacités considérables et surface d'exposition très large

Les États-Unis disposent d'avantages importants dans presque chacune de ces dimensions. Leur secteur technologique occupe une position centrale dans les logiciels, les services cloud, les semi-conducteurs et de nombreuses infrastructures numériques mondiales. Les agences de renseignement et forces armées disposent de ressources importantes, tandis que le réseau d'alliances permet un partage étendu d'informations.

Cette position n'est cependant pas équivalente à une supériorité automatique. La numérisation très avancée de l'économie américaine crée une surface d'attaque considérable. De nombreux services essentiels reposent sur des opérateurs privés dont le niveau de sécurité peut varier. La puissance offensive et la vulnérabilité interne peuvent donc progresser simultanément.

L'intégration des capacités cyber aux opérations militaires constitue un avantage particulièrement important. Une opération préparée par les services compétents peut être synchronisée avec d'autres moyens, ce qui augmente sa valeur militaire. Cette intégration dépend toutefois du maintien des accès et de la capacité à transmettre suffisamment tôt les besoins opérationnels aux unités cyber. Une cible identifiée au dernier moment ne peut pas toujours être compromise avec la précision nécessaire.

La Chine : profondeur industrielle et renseignement stratégique

La Chine possède une importante base technologique, un volume considérable de compétences et un appareil de sécurité capable d'inscrire les opérations cyber dans des objectifs économiques, politiques et militaires plus larges. Le renseignement technologique et industriel constitue une dimension importante de cette activité, en complément des objectifs directement militaires.

Le rapport de force avec les États-Unis occupe une place particulière en raison de l'interdépendance entre les deux économies et de leur compétition technologique. La capacité à comprendre les réseaux, infrastructures et chaînes d'approvisionnement adverses présente une valeur qui dépasse la seule préparation d'une guerre. Elle permet également d'évaluer les dépendances, de collecter des informations sur les technologies prioritaires ou de suivre des décisions politiques.

La montée en puissance chinoise dans les technologies numériques réduit progressivement certaines dépendances extérieures tout en créant ses propres infrastructures à protéger. Comme dans le domaine spatial, l'expansion de la capacité nationale augmente donc

simultanément les moyens disponibles et le nombre de fonctions vulnérables à une action adverse.

La Russie : exploitation des asymétries et écosystème hybride

La Russie dispose de capacités reconnues dans les opérations de renseignement, de perturbation et d'influence numérique. Son poids économique et technologique global est inférieur à celui des États-Unis ou de la Chine, mais le cyberspace offre des moyens d'action qui ne nécessitent pas de reproduire la puissance conventionnelle ou industrielle de l'adversaire.

Les activités dénoncées publiquement par l'OTAN en juillet 2026 montrent également l'importance accordée à l'environnement d'acteurs proches ou tolérés. L'existence d'un écosystème comprenant plusieurs types de groupes complique l'attribution et permet d'exercer des pressions sans que chaque opération doive être directement conduite par une structure officielle identifiable¹⁷.

Ce modèle présente également des limites. Des acteurs criminels ou semi-autonomes peuvent poursuivre leurs propres intérêts, provoquer des incidents non souhaités ou attirer une attention internationale préjudiciable. L'ambiguïté augmente la flexibilité mais réduit le contrôle complet.

L'Europe : résilience collective et fragmentation opérationnelle

L'Union européenne dispose d'une capacité réglementaire importante et a progressivement construit un cadre couvrant les opérateurs essentiels, les produits numériques, la préparation aux crises et la réponse aux incidents majeurs. Le *Cyber Solidarity Act* complète notamment les mécanismes existants en organisant la détection et une capacité de soutien collective¹⁸.

Cette puissance réglementaire ne correspond pas à une capacité offensive européenne centralisée. Les moyens de renseignement et d'action cyber restent principalement nationaux. Cette répartition reflète les compétences des États membres en matière de défense et de sécurité nationale, mais elle impose une coordination importante lorsqu'une campagne affecte plusieurs pays.

L'Europe dispose donc d'un rapport de force particulier : elle peut relever le niveau moyen de sécurité de son marché par la réglementation et mobiliser des mécanismes collectifs de réponse, tout en dépendant des capacités nationales pour l'attribution sensible et les opérations offensives. Cette architecture peut fonctionner si les procédures de partage d'informations sont rapides et si les responsabilités ont été définies avant la crise.

Les acteurs non étatiques

Le cyberspace permet à des groupes non étatiques de produire des effets qui seraient difficiles à obtenir dans d'autres domaines. Des groupes criminels peuvent interrompre temporairement les activités d'une grande entreprise ou d'une administration. Des hacktivistes peuvent perturber des sites, publier des données ou conduire des campagnes médiatiquement visibles.

¹⁷ North Atlantic Treaty Organization. (2026, July 13). *Statement of condemnation by the North Atlantic Council of Russia's malicious cyber activities*. NATO. <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2026/07/13/statement-of-condemnation-by-the-north-atlantic-council-of-russias-malicious-cyber-activities>

¹⁸ European Commission. (2026, August 17). *EU Cyber Solidarity Act*. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity>

Il faut néanmoins distinguer cette capacité de nuisance d'une capacité stratégique comparable à celle d'un État disposant d'un renseignement structuré, d'une préparation de long terme et d'une intégration aux autres instruments de puissance. Les opérations les plus complexes exigent un niveau de connaissance, de patience et de ressources qui réduit considérablement le nombre d'acteurs capables de les mener durablement.

Intérêts en présence

Les États cherchent dans le cyberspace à protéger leurs propres infrastructures tout en conservant la capacité de comprendre et d'affecter celles de leurs concurrents. Ces deux objectifs ne peuvent pas être séparés. Une puissance dépourvue de capacité offensive perd une partie de ses moyens de renseignement et d'action ; une puissance incapable de protéger et restaurer ses systèmes offre à l'adversaire un levier susceptible de neutraliser les avantages obtenus ailleurs.

Le renseignement constitue généralement l'intérêt le plus constant. Une présence dans un réseau adverse peut fournir des informations politiques, militaires, économiques ou technologiques sans produire immédiatement d'incident visible. L'espionnage bénéficie ainsi d'un rapport coût-utilité particulièrement favorable lorsqu'un accès peut être maintenu pendant une longue période.

Le sabotage répond à une logique plus restrictive. Son utilisation révèle souvent la présence de l'attaquant et provoque une réaction défensive. Il est donc rationnel de réserver certaines capacités aux situations où l'effet immédiat justifie la perte éventuelle de l'accès.

Le prépositionnement se situe entre ces deux fonctions. Il permet de conserver une option sans l'utiliser immédiatement. Sa valeur dépend directement de la capacité à rester clandestin et de la stabilité de l'architecture cible.

La protection des infrastructures critiques constitue l'intérêt défensif principal. Le nombre de systèmes concernés oblige toutefois à hiérarchiser les priorités. Un État ne peut pas protéger toutes les entreprises avec le même niveau d'exigence. Il doit identifier les fonctions dont l'arrêt aurait un effet systémique, les opérateurs qui les assurent et les fournisseurs dont ils dépendent.

Les entreprises poursuivent leurs propres intérêts. Elles doivent maintenir leurs services, protéger leur réputation, respecter les obligations réglementaires et limiter les coûts. Ces priorités ne correspondent pas toujours exactement à celles de l'État. Une mesure de sécurité utile du point de vue stratégique peut être coûteuse à court terme pour un opérateur ; inversement, une architecture économiquement optimale peut créer une concentration de risque jugée problématique pour la sécurité nationale.

L'État doit donc organiser cette relation par la réglementation, les incitations et le partage d'informations. Le *Cyber Resilience Act* et les autres politiques européennes cherchent précisément à internaliser une partie de ces coûts de sécurité dans la conception et la maintenance des produits¹⁹.

Les alliances ajoutent un niveau supplémentaire. Une cyberattaque contre un État membre peut exploiter une infrastructure située dans un autre pays, toucher simultanément plusieurs Alliés ou dépendre d'informations détenues par des entreprises multinationales. L'intérêt collectif consiste donc à réduire les écarts de capacité entre membres et à éviter qu'un adversaire n'exploite le maillon le moins protégé d'un ensemble intégré.

¹⁹ European Commission. (2026, September 7). *Cyber Resilience Act*. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act>

Dynamiques d'évolution

L'évolution la plus importante devrait être la professionnalisation du prépositionnement. À mesure que les infrastructures deviennent mieux protégées, obtenir un accès durable exige davantage de préparation, de renseignement et de discipline. Les campagnes les plus stratégiques pourront donc être moins visibles que les attaques opportunistes qui dominent les statistiques publiques. Leur danger résidera précisément dans leur faible bruit opérationnel.

La seconde dynamique est l'augmentation des exigences de résilience. Les politiques européennes et alliées montrent que la simple prévention n'est plus considérée comme suffisante. Le *Cyber Solidarity Act* organise une capacité de détection et d'intervention collective, tandis que l'OTAN développe ses propres mécanismes de défense intégrée et ses exercices²⁰.

Une troisième dynamique concerne la sécurité des identités et la limitation des privilèges. Les modèles traditionnels reposant sur une distinction relativement rigide entre intérieur et extérieur du réseau sont de moins en moins adaptés à des environnements utilisant le cloud, le travail distant, de nombreux fournisseurs et des services distribués. La stratégie numérique de l'OTAN adoptée en 2026 mentionne explicitement le recours aux principes Zero Trust pour renforcer la sécurité des infrastructures de l'Alliance²².

Cette approche vise à empêcher qu'une compromission initiale fournisse automatiquement à l'attaquant un accès étendu. L'identité, le contexte et les droits doivent être vérifiés de manière continue, ce qui limite les possibilités de déplacement latéral dans le réseau.

L'intelligence artificielle devrait ensuite modifier les volumes d'activité. Les campagnes d'ingénierie sociale peuvent être davantage automatisées et personnalisées ; l'analyse de code, de vulnérabilités ou de journaux peut être accélérée. Les défenseurs bénéficieront des mêmes outils pour traiter un nombre d'alertes supérieur ou détecter des comportements inhabituels. Il est donc probable que l'IA augmente simultanément le rythme de l'attaque et celui de la défense, sans déterminer à elle seule lequel des deux obtient un avantage durable.

La cinquième dynamique concerne la convergence entre cyber et opérations conventionnelles. Les forces militaires chercheront davantage à intégrer les options cyber dès les premières phases de planification. Cette évolution exigera de préparer les accès suffisamment tôt et de mieux informer les responsables cyber des objectifs opérationnels susceptibles d'apparaître en cas de crise. L'utilité de l'outil dépendra de cette anticipation : une capacité inexistante au moment où la campagne commence ne peut pas être improvisée.

Enfin, le cadre international continuera probablement à progresser lentement. Le consensus obtenu en 2025 à l'ONU fournit une base commune mais ne supprime pas les divergences entre puissances. Le mécanisme mondial lancé en 2026 institutionnalise le dialogue, ce qui peut améliorer les mesures de confiance et la compréhension mutuelle sans empêcher le développement des capacités offensives²³.

²⁰ European Commission. (2026, August 17). *EU Cyber Solidarity Act*. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity>

²¹ Allied Command Transformation. (2025, December 5). *NATO Cyber Coalition 2025: Advancing cyber defence and strengthening Alliance resilience*. NATO. <https://www.act.nato.int/article/cyber-coalition-2025/>

²² North Atlantic Treaty Organization. (2026, May 26). *NATO's Digital Transformation Implementation Strategy 2.0*. NATO. <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2026/05/26/natos-digital-transformation-implementation-strategy>

²³ United Nations, Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025. (2025, July 1). *Final report of the Open-ended Working Group on Security of and in the Use of Information and*

Scénarios prospectifs

Le premier scénario, et le plus probable, est celui d'une compétition permanente dominée par l'espionnage, le prépositionnement et des perturbations limitées. Les États continueront à pénétrer les réseaux de leurs concurrents afin de collecter des renseignements ou préparer des options, tout en évitant généralement les effets les plus destructeurs en dehors d'une crise majeure. Les groupes criminels et hacktivistes continueront parallèlement à produire un volume important d'incidents, ce qui compliquera la lecture stratégique de l'environnement.

Cette configuration présente une stabilité relative mais non garantie. Les opérations peuvent rester sous le seuil de l'affrontement ouvert pendant une longue période, mais la découverte d'un accès dans une infrastructure critique peut provoquer une réaction politique importante si elle intervient au moment d'une crise. L'absence d'effet destructeur ne signifie donc pas l'absence de risque d'escalade.

Le deuxième scénario correspond à une intégration systématique du cyber à un conflit conventionnel. Les opérations commenceraient avant les premières actions militaires visibles afin de collecter des informations, perturber certains réseaux et préparer des effets synchronisés. Les cibles seraient choisies en fonction de leur contribution à la campagne : logistique, communications, défense aérienne, commandement, transport ou production industrielle. Les opérations cyber ne chercheraient pas nécessairement une paralysie générale. Une interruption temporaire correctement synchronisée pourrait fournir un avantage suffisant.

Le troisième scénario serait celui d'une campagne majeure contre plusieurs infrastructures civiles essentielles. Une telle opération chercherait à créer des effets cumulatifs : perturbation de l'énergie, des télécommunications, de certains transports ou services financiers. Sa réussite exigerait toutefois de maintenir plusieurs accès simultanément et de réduire la capacité de restauration. Plus la campagne serait large, plus elle augmenterait également la probabilité d'attribution et d'une réponse internationale importante.

Le quatrième scénario concerne une attaque dont les conséquences dépassent les intentions initiales. Les infrastructures numériques sont fortement interconnectées et un logiciel malveillant peut se propager au-delà de la cible prévue. Une opération conçue pour produire un effet local peut affecter des entreprises ou États tiers, ce qui élargirait la crise et compliquerait la décision politique de l'attaquant comme de la victime.

Le cinquième scénario serait une augmentation de la fragmentation numérique mondiale. Les considérations de sécurité pourraient conduire les États à imposer davantage de restrictions sur les fournisseurs, les données, les infrastructures cloud ou les équipements de télécommunications. Une telle évolution réduirait certaines dépendances mais augmenterait les coûts, accélérerait la constitution d'écosystèmes technologiques distincts et pourrait réduire les possibilités de coopération sur la sécurité des réseaux.

Recommandations

La première priorité est de fonder les politiques de cybersécurité sur les fonctions à maintenir plutôt que sur la protection uniforme de l'ensemble des systèmes. Chaque administration ou opérateur critique doit identifier les services dont l'interruption aurait les conséquences les plus graves, préciser les dépendances techniques nécessaires à leur fonctionnement et déterminer le niveau minimal qui doit pouvoir être maintenu pendant une crise. Cette analyse permet

d'allouer les ressources aux systèmes dont la compromission aurait un effet réellement stratégique.

La deuxième priorité porte sur la détection. Une organisation peut disposer de protections importantes tout en restant compromise pendant plusieurs mois si elle ne sait pas identifier les comportements anormaux. Les capacités de journalisation, de supervision, de recherche proactive de menaces et d'analyse des événements doivent donc être considérées comme des fonctions essentielles. Le délai entre l'accès initial et la détection fournit un indicateur plus utile que le simple nombre d'incidents bloqués.

La troisième priorité concerne la segmentation et le contrôle des privilèges. Une compromission locale ne doit pas permettre à l'attaquant d'accéder automatiquement à l'ensemble du système. Les principes Zero Trust, la limitation des droits, l'authentification renforcée et la séparation des environnements critiques doivent réduire l'effet potentiel d'un accès initial. L'objectif n'est pas de rendre toute intrusion impossible mais de limiter ce qu'un attaquant peut faire lorsqu'il parvient à entrer.

La quatrième priorité est la restauration. Les sauvegardes doivent être isolées de l'environnement principal, régulièrement testées et accompagnées de procédures permettant de reconstruire réellement les services. Une sauvegarde qui n'a jamais été restaurée dans des conditions de crise ne constitue pas une garantie suffisante. Les opérateurs doivent connaître le temps nécessaire pour remettre en fonctionnement leurs services les plus importants.

La cinquième priorité est la sécurisation de la chaîne d'approvisionnement. Les fournisseurs doivent être classés selon l'accès dont ils disposent et la criticité des services qu'ils fournissent. Les obligations contractuelles doivent couvrir la gestion des vulnérabilités, la notification des incidents, les mises à jour et les droits d'audit. Les politiques européennes sur les produits numériques fournissent un cadre utile, mais la responsabilité finale de la cartographie des dépendances appartient aux organisations elles-mêmes²⁴.

La sixième priorité est le partage d'informations. Les campagnes étatiques touchent souvent plusieurs organisations avant qu'une image complète puisse être construite. Les informations techniques doivent pouvoir être échangées rapidement entre opérateurs privés, autorités nationales, agences européennes et alliés. Les mécanismes doivent prévoir la protection des informations sensibles afin que les entreprises ne soient pas dissuadées de signaler rapidement les incidents.

La septième priorité concerne les exercices. Ceux-ci doivent associer responsables techniques, directions d'entreprise, autorités politiques, forces de sécurité et, lorsque le scénario le justifie, forces armées. Une cybercrise majeure ne produit pas uniquement des problèmes informatiques : elle pose des questions de communication publique, de responsabilité, de continuité économique, d'attribution et de réponse internationale. Les exercices de l'OTAN et les mécanismes européens constituent des modèles utiles pour tester cette coordination²⁵.

La huitième priorité est la préparation de l'attribution politique. Les États doivent définir à l'avance les procédures permettant de combiner renseignements techniques et autres sources, les niveaux de confiance nécessaires pour différents types de réponse et les mécanismes de coordination avec les alliés. Une attribution publique ne doit pas être improvisée sous la pression d'une crise.

²⁴ European Commission. (2026, July 27). *Cyber Resilience Act*. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act> Stratégie numérique européenne

²⁵ Allied Command Transformation. (2025, December 5). *NATO Cyber Coalition 2025: Advancing cyber defence and strengthening Alliance resilience*. NATO. <https://www.act.nato.int/article/cyber-coalition-2025/>

La neuvième priorité concerne les capacités offensives. Leur développement doit rester lié à des objectifs politiques et militaires précis. Maintenir un accès dans un réseau possède un coût et une valeur qui peuvent être perdus après utilisation. L'emploi doit donc être décidé en fonction de l'effet attendu, de la possibilité de propagation, du risque d'attribution et de l'intérêt de conserver la capacité pour une situation ultérieure. Une doctrine offensive crédible ne se mesure pas au nombre d'outils développés mais à la capacité à employer ceux-ci dans un cadre stratégique cohérent.

La dixième priorité concerne la coopération européenne. Les instruments récemment créés doivent être testés dans des situations réellement complexes. Le *Cyber Solidarity Act* et la réserve européenne peuvent fournir des capacités supplémentaires, mais leur efficacité dépendra des délais de mobilisation et de l'articulation avec les autorités nationales²⁶.

Enfin, la France doit traiter la cyberdéfense comme une composante commune de la continuité de l'État, de la sécurité économique et de la préparation militaire. La séparation administrative entre ces domaines ne doit pas empêcher la circulation des informations nécessaires. Les infrastructures critiques civiles, les entreprises de défense et les réseaux publics doivent être analysés comme un ensemble de dépendances dont la perturbation peut affecter différentes fonctions nationales.

Implications stratégiques

La première implication concerne la temporalité de la compétition. Le cyber permet aux États de préparer des options bien avant que l'utilisation de ces capacités soit politiquement décidée. Cette caractéristique rend les réseaux adverses comparables à un espace de renseignement permanent dans lequel les acteurs cherchent à comprendre les architectures, identifier les dépendances et maintenir des accès. La préparation d'une future opération peut donc être difficile à distinguer d'un espionnage courant jusqu'au moment où l'accès est activé.

Cette situation réduit la valeur d'une défense uniquement réactive. Lorsqu'une crise débute, il peut être trop tard pour rechercher toutes les compromissions existantes ou reconstruire entièrement les architectures les plus vulnérables. Le niveau de sécurité atteint avant la crise conditionne directement la marge de manœuvre politique disponible pendant celle-ci. Les États doivent donc accepter qu'une partie du coût de préparation à la cyberguerre corresponde à des investissements permanents dont l'utilité est difficilement visible tant qu'aucun incident majeur ne survient.

La deuxième implication concerne la notion de puissance offensive. Les capacités cyber ne peuvent pas être stockées exactement comme des munitions. Un outil fondé sur une vulnérabilité peut perdre sa valeur lorsque la faille est corrigée. Un accès clandestin peut disparaître après une mise à jour ou être découvert lors d'un audit. Les capacités doivent être continuellement entretenues et renouvelées. Leur valeur dépend autant du renseignement permanent que du développement technique initial.

Cette caractéristique a plusieurs conséquences pour la planification militaire. Les commandements doivent identifier suffisamment tôt les types de systèmes susceptibles de présenter un intérêt en cas de conflit afin que les capacités nécessaires puissent être préparées. Une demande apparaissant quelques jours avant une opération ne garantit pas qu'un accès soit disponible. L'intégration du cyber à la planification ne peut donc pas se limiter à ajouter un « effet cyber » à un plan déjà achevé.

²⁶ European Commission. (2026, August 17). *EU Cyber Solidarity Act*. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity>

La troisième implication concerne les limites de l'autonomie du cyber. Une campagne numérique peut produire des effets importants, mais sa capacité à imposer seule une décision politique durable reste incertaine. Les institutions peuvent restaurer les services, les opérateurs peuvent isoler les réseaux et les sociétés peuvent s'adapter à des perturbations temporaires. Une attaque cyber produit davantage de valeur lorsqu'elle contribue à une pression plus large ou soutient une opération militaire, économique ou diplomatique.

Cette observation ne réduit pas son importance. Elle permet au contraire de mieux situer sa fonction. Le cyber peut affecter le rythme d'une campagne, compliquer la mobilisation, fournir du renseignement, imposer des coûts économiques et créer de l'incertitude. Ces effets peuvent être stratégiques lorsqu'ils sont intégrés à un objectif politique cohérent. Ils deviennent beaucoup moins utiles lorsque la perturbation est considérée comme une fin en soi.

La quatrième implication concerne la résilience nationale. Les infrastructures civiles sont désormais suffisamment importantes pour que leur sécurité affecte directement la capacité de l'État à soutenir une crise prolongée. Une armée peut disposer de réseaux très protégés tout en dépendant d'une société dont les télécommunications, le transport ou la production sont vulnérables. La cyberdéfense doit donc être articulée à la résilience générale et non limitée aux systèmes militaires.

L'Union européenne joue un rôle important dans cette dimension parce que sa réglementation peut relever le niveau de sécurité de nombreux acteurs privés. Le *Cyber Solidarity Act*, le *Cyber Resilience Act* et la politique européenne de certification interviennent sur des éléments différents de la même problématique : réduire le nombre de vulnérabilités, mieux détecter les campagnes et organiser la réponse lorsqu'une crise dépasse les capacités d'un opérateur ou d'un État²⁷.

La cinquième implication concerne les alliances. La mutualisation permet d'améliorer l'attribution, de partager des informations et de fournir du soutien à un membre moins doté. Mais elle crée également une interdépendance. Une alliance dont les réseaux sont fortement connectés doit tenir compte des écarts de maturité entre membres et des risques introduits par les infrastructures communes. L'amélioration du niveau minimum de protection devient donc un intérêt collectif.

L'OTAN répond à cette question par le développement de standards, d'exercices et de structures communes. L'édition 2025 de *Cyber Coalition*, avec environ 1 300 participants issus de 29 Alliés et sept partenaires, illustre l'importance accordée à la préparation collective²⁸.

La sixième implication concerne la dissuasion. Dans le cyberspace, celle-ci ne peut pas reposer sur une seule menace de représailles. L'incertitude de l'attribution, la fréquence des incidents et la grande diversité des effets rendent une réponse automatique peu crédible. La dissuasion doit combiner plusieurs mécanismes : empêcher l'accès lorsque cela est possible, limiter les effets d'une compromission, restaurer rapidement, exposer publiquement certaines campagnes, imposer des coûts diplomatiques ou économiques et conserver des options de réponse dans plusieurs domaines.

Cette approche permet également d'éviter une symétrie artificielle. Une cyberattaque ne doit pas nécessairement recevoir une réponse cyber. L'instrument doit être choisi selon l'objectif politique. Une sanction économique, une arrestation, l'expulsion d'agents, une opération de renseignement ou une action militaire peuvent, selon les circonstances, être plus appropriées qu'une riposte technique directe.

²⁷ European Commission. (2026, July 7). *EU cybersecurity policies*. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies>

²⁸ Allied Command Transformation. (2025, December 5). *NATO Cyber Coalition 2025: Advancing cyber defence and strengthening Alliance resilience*. NATO. <https://www.act.nato.int/article/cyber-coalition-2025/>

La septième implication concerne le droit et les normes. Le consensus international sur l'idée que le droit international s'applique au cyberspace ne règle pas toutes les questions. Les États conservent des interprétations différentes concernant les seuils, la souveraineté, la diligence et la légitime défense. Le travail multilatéral reste néanmoins utile pour construire des attentes communes et des mécanismes de confiance.

La conclusion du groupe de travail 2021-2025 de l'ONU par consensus et la mise en place du mécanisme mondial à partir de 2026 offrent un cadre plus permanent pour ces discussions²⁹.

Ce cadre ne conduira probablement pas à une démilitarisation du cyberspace. Les grandes puissances continueront à développer des capacités tant qu'elles considéreront que celles-ci présentent une valeur pour le renseignement et la défense. Les progrès les plus réalistes concernent la réduction des risques, la protection des infrastructures civiles essentielles, les mécanismes de communication et la clarification progressive des comportements considérés comme particulièrement dangereux.

Conclusion

La cyberguerre stratégique ne peut pas être réduite à la multiplication des cyberattaques ni à la perspective d'un effondrement numérique des États. Elle correspond à l'intégration durable des capacités numériques aux pratiques de renseignement, aux politiques de coercition et à la planification militaire. Les États cherchent en permanence à comprendre les infrastructures de leurs concurrents, à identifier leurs vulnérabilités et à conserver des accès utilisables si le contexte politique exige une action plus directe.

Cette activité est rendue possible par la numérisation générale des sociétés. Les administrations, entreprises, infrastructures critiques et forces armées utilisent des technologies communes et dépendent de chaînes d'approvisionnement largement privées. La sécurité nationale ne peut donc plus être assurée uniquement à l'intérieur d'un périmètre militaire. Le niveau général de cybersécurité d'une économie affecte directement sa capacité à absorber une campagne hostile.

Les données de l'ENISA rendent compte de cette réalité européenne : plusieurs milliers d'incidents sont observés dans un environnement où groupes criminels, hacktivistes et acteurs liés à des États utilisent des techniques souvent proches³⁰.

Cette densité de menace complique l'analyse stratégique mais renforce également l'intérêt des mesures de sécurité de base. Les politiques destinées à limiter les privilèges, corriger les vulnérabilités, segmenter les réseaux et tester les sauvegardes sont utiles contre des menaces très différentes. La frontière entre cybersécurité courante et préparation à une confrontation majeure est donc moins nette qu'elle ne l'est pour de nombreuses capacités militaires.

La principale différence entre une organisation résiliente et une organisation vulnérable apparaîtra après la compromission. Le délai nécessaire pour identifier l'attaquant, isoler les systèmes touchés et restaurer les services déterminera souvent davantage l'effet stratégique que le succès technique initial de l'intrusion. Une opération dont les conséquences sont rapidement contenues produit peu de bénéfice politique ; une interruption prolongée peut au contraire modifier les décisions d'un gouvernement ou la conduite d'une campagne.

²⁹ United Nations, Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025. (2025, July 1). *Final report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025 [Draft]* (A/AC.292/2025/L.1). United Nations. <https://digitallibrary.un.org/record/4084927>

³⁰ European Union Agency for Cybersecurity. (2025, October 1). *ENISA threat landscape 2025*. ENISA. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>

Les investissements doivent donc porter autant sur la récupération que sur la protection. Cette évolution apparaît clairement dans les dispositifs européens, notamment le *Cyber Solidarity Act* et la réserve européenne de cybersécurité, qui ne visent pas uniquement la prévention mais également la préparation, la réponse et la récupération³¹³².

L'OTAN adopte la même logique dans un cadre militaire différent. Le cyberspace est un domaine d'opérations depuis 2016, les capacités sont intégrées à la défense collective et l'Alliance poursuit la mise en place d'organisations et d'exercices destinés à améliorer la coordination entre États, forces armées, experts civils et industrie³³.

La compétition restera cependant largement nationale dans ses fonctions les plus sensibles. Les services de renseignement, les capacités offensives et les décisions d'attribution politique continueront à relever principalement des États. Les organisations internationales permettent de coordonner, de partager et d'augmenter la résilience ; elles ne remplacent pas les capacités souveraines nécessaires pour comprendre une campagne ou décider d'une réponse.

Pour la France et les autres puissances européennes, l'enjeu consiste donc à articuler trois niveaux. Le niveau national doit conserver les capacités de renseignement, d'attribution et d'action nécessaires aux intérêts essentiels. L'Union européenne doit renforcer la sécurité générale du marché et organiser la réponse collective aux incidents dépassant les moyens d'un seul acteur. L'OTAN doit assurer l'intégration du cyber aux opérations militaires et à la défense collective.

La cyberguerre stratégique pose enfin une question de discipline analytique. Toute activité malveillante ne doit pas être interprétée comme une opération de guerre. La plupart des incidents n'ont pas une portée stratégique et de nombreuses campagnes relèvent du crime, de l'espionnage ou de formes limitées de pression. Employer la catégorie de guerre pour l'ensemble de ces phénomènes empêche de distinguer les actions susceptibles de modifier réellement un rapport de force.

L'évaluation doit porter sur la fonction visée, la durée de l'effet, le contexte politique, la capacité de restauration et l'intégration éventuelle de l'opération à une stratégie plus large. Une perturbation limitée peut être militairement décisive si elle intervient au moment où une force dépend précisément du système touché. Une attaque techniquement spectaculaire peut rester stratégiquement secondaire si les services sont rapidement rétablis et qu'aucune décision politique n'est affectée.

La place du cyber dans la puissance contemporaine se situe dans cette différence. Il n'offre pas une méthode universelle permettant de remplacer les autres instruments. Il fournit des moyens supplémentaires de renseignement, de préparation et de perturbation qui peuvent être utilisés longtemps avant le début d'un conflit et combinés ensuite à une campagne plus large. Les puissances capables d'en tirer le meilleur parti seront celles qui auront préparé suffisamment tôt les accès nécessaires tout en réduisant la possibilité pour leurs adversaires de faire de même avec leurs propres infrastructures.

Cette compétition ne sera probablement jamais totalement visible. Une partie des capacités les plus importantes restera clandestine jusqu'à son emploi ou sa découverte. L'absence d'incident majeur ne permettra donc pas de conclure à l'absence de préparation offensive. Inversement, l'existence d'intrusions récurrentes ne signifie pas qu'une guerre soit en cours au sens classique.

³¹ European Commission. (2026, August 17). *EU Cyber Solidarity Act*. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity>

³² European Commission. (2025, August 26). *ENISA to operate the EU Cybersecurity Reserve*. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/news/enisa-operate-eu-cybersecurity-reserve>

³³ Allied Command Transformation. (n.d.). *Cyber defence*. NATO. <https://www.act.nato.int/activities/cyber/>

La cyberguerre stratégique se situe précisément dans cet espace intermédiaire, entre renseignement permanent, préparation de crise et emploi militaire. C'est cette continuité, davantage que la seule puissance destructrice des outils numériques, qui explique sa place croissante dans les stratégies de puissance.