

COMPRENDRE :

LA CYBERGUERRE ENTRE LES ÉTATS

LES ENJEUX STRATÉGIQUES D'UN MONDE CONNECTÉ

Le cyberspace est le monde d'internet et des réseaux connectés. Espace sans frontières et en perpétuel mouvement, il est devenu le terrain de jeu des cybercriminels et un champ d'affrontement entre États. Les menaces y sont multiples, les attaques toujours plus innovantes. La cybersécurité est aujourd'hui au cœur des défis politiques, économiques et sociétaux de notre monde connecté.

CHIFFRES CLÉS



+ de 6 milliards
d'utilisateurs d'internet
(UIT) en 2025 soit 73 %
de la population



+ de 100.000
cyber attaques par an
(Check Point Research)



10 500 Mds \$
Coût mondial de la
cybercriminalité en 2025
(estimation)

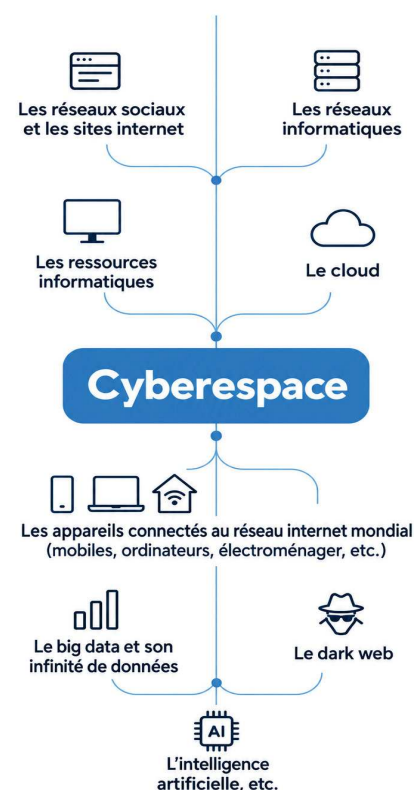
Qu'est ce que le cyberspace ?

Le cyberspace est le monde d'internet et des réseaux connectés. Il est partout autour de nous, dès lors que nous surfons sur un site web ou que nous nous connectons au cloud pour stocker des données.

Cet espace transnational connaît une expansion continue et permet la circulation de volumes considérables de données. Le cyberspace constitue également un terrain d'action privilégié pour les cybercriminels. Les menaces traversant le cyberspace sont multiples et les attaques toujours plus innovantes. L'enjeu de la cybersécurité est au cœur de ce monde connecté.

L'émergence du cyberspace est étroitement liée au développement d'Internet. Le cyberspace est un espace dématérialisé qui repose sur des infrastructures physiques permettant les interconnexions planétaires. Cet espace technologique comprend toutes les technologies numériques.

Le cyberspace, contrairement au monde physique, transcende les frontières géographiques, tout en demeurant soumis à des juridictions nationales. Les informations circulent librement d'un continent à un autre. Il est aussi en perpétuel mouvement : les nouvelles technologies et la multiplicité des ressources informatiques agrandissent constamment ce cyberspace. Cet environnement et l'infinité d'opérations qu'il abrite représentent un véritable défi pour la sécurité numérique.



Comment fonctionne le cyberspace ?

Pour comprendre ce qu'est le cyberspace, il est nécessaire de s'intéresser à son mode de fonctionnement. Il s'appuie sur une organisation interconnectée faisant intervenir de nombreux acteurs majeurs.

L'organisation du cyberspace : entre réseau physique et réseau dématérialisé

Le cyberspace est composé de différents éléments. Il est question de trois niveaux, ou de trois couches, permettant la connexion et la circulation des informations à travers cet univers. La première couche est représentée par tout le matériel physique nécessaire aux échanges. Cela comprend les câbles sous-marins, les satellites, les centres de données (datas centers), mais aussi les ordinateurs et l'ensemble des appareils connectés.

Le second niveau est appelé la couche logicielle. Ce sont toutes les applications contribuant aux échanges de données. Cette seconde couche compte les processus techniques permettant le bon fonctionnement entre le matériel physique, les dispositifs connectés et les utilisateurs.

La dernière couche représente tout le contenu informationnel. Il s'agit de la partie sémantique permettant de créer des données, d'associer et d'organiser les informations.

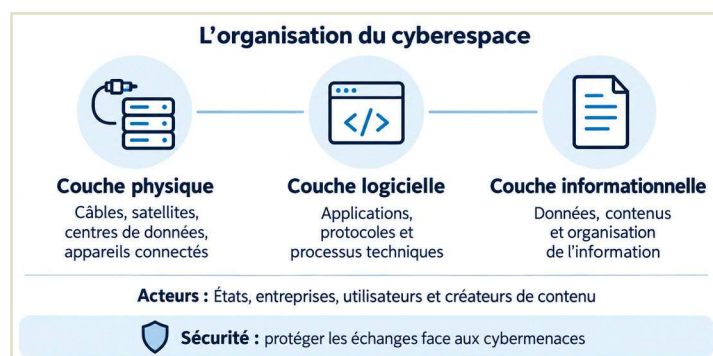
Les acteurs du cyberspace : des États au simple utilisateur connecté

Les acteurs de ce cyberspace sont nombreux et diversifiés. Les États, les grandes entreprises comme les GAFAM (Google, Amazon, Apple, etc.) et les FTN (firmes transnationales) jouent un rôle principal. Ce sont eux qui déploient les infrastructures physiques et dématérialisées pour permettre

les échanges. Ils mettent en place les moyens techniques clés pour que le monde numérique se développe.

Tout utilisateur et créateur de contenu est un acteur de cet espace multiconnecté. Les cybercriminels participent eux aussi à la vie dans le cyberspace. Ils se classent en trois grands groupes, aux menaces différentes. On distingue notamment les pirates informatiques, les collectifs d'activistes dont les plus célèbres sont Anonymous et Wikileaks. Enfin, les groupes criminels, ou les cyberterroristes contribuent à ce qu'il est possible d'appeler la guerre du cyberspace. Quelle est l'importance de la mise en place d'un cyberspace sécurisé ?

Derrière les usages quotidiens d'Internet se dessinent des enjeux et des menaces majeurs, tant politiques qu'économiques. Les cyberattaques constituent désormais l'une des menaces les plus sérieuses sur notre monde physique.



Les enjeux économiques et politiques d'un cyberspace sécurisé

Pour les États, l'enjeu de la sécurité du cyberspace est majeur. Outre le cyberespionnage redouté des services de défense de tous les pays, les menaces du cyberterrorisme se développent. Ce type d'attaque vise à remettre en cause la sûreté d'un État, en visant des infrastructures clés comme les télécommunications, la santé ou les finances.

Les grandes entreprises dépendent elles aussi de la mise en place d'un cyberspace sécurisé. Avec une activité exclusive au monde numérique, une attaque visant à arrêter son fonctionnement peut avoir un impact économique désastreux, en plus de nuire à l'intégrité et à l'image de marque.

Des menaces multiples pour déstabiliser les États et les entreprises

La mise en place d'un cybermonde sécurisé réduit les menaces et l'efficacité des intrusions. Aujourd'hui, les cyberattaques sont multiples et visent différents objectifs. Les pirates informatiques cherchent le gain financier quand les cyberterroristes souhaitent nuire à un pays. Les techniques vont du sabotage des systèmes d'information (ransomware, hacking, botnets, etc.) à l'espionnage en passant par la menace la plus forte : la subversion. Les cybercriminels mettent en place une série d'actions pour affaiblir le pouvoir d'un État ou l'activité d'une entreprise.

La désinformation : limiter la propagation des fake news.

La propagande des activistes en ligne et le déploiement de fausses informations comptent également comme une menace issue du cyberspace. Avec un manque de contrôle sur l'infinité des échanges, la diffusion en ligne de fake news est facilitée. Cette désinformation est une menace à la fois poli-

tique et économique. Pour éviter les dérives, il est primordial de poser un cadre et de renforcer les mécanismes de vérification des informations avant leur diffusion.

Sécuriser le cyberspace

Protéger les États, les entreprises et l'information



États

Souveraineté et infrastructures critiques

Télécommunications • Santé • Finances



Entreprises

Continuité d'activité et protection des données

Impacts économiques • Réputation

Des menaces multiples



Espionnage

Vol d'informations sensibles



Sabotage et rançongiciels

Perturbation ou arrêt des systèmes



Cyberterrorisme

Menaces contre des infrastructures clés



Désinformation

Manipulation et déstabilisation



Réduire les risques

Sécuriser les systèmes et préparer la continuité d'activité
Vérifier les sources et recouper les informations avant diffusion

Comment assurer une utilisation sûre et responsable du cyberspace ?

Le cyberspace est un environnement sans contrôle strict. Chaque pays tente de mettre en place des stratégies de défense, mais il ne s'agit plus ici de protéger un territoire, mais un ensemble de facteurs. Pour lutter contre les cyberattaques et limiter les impacts des opérations de guerre informatique, des mesures doivent être prises.

Coopération entre les États avec une législation commune sur le contrôle des données

Pour contrôler un espace aussi grand que l'univers connecté, les États doivent déployer des moyens de défense communs. Une politique générale de cyberdéfense, organisée de la même façon que l'institution de l'OTAN, pourrait réduire l'efficacité des attaques.

Des actions ont déjà été mises en place, comme les échanges entre les différents CSIRT mondiaux (Computer Security Incident Response Team).

La communication sur les menaces rencontrées, sur les techniques de défense réalisées ou sur l'identification des cybercriminels est nécessaire pour adopter une stratégie de défense commune efficace.

Définir la responsabilité des acteurs du cyberspace

Chaque acteur doit prendre conscience de ses devoirs et instaurer des mesures de défenses fortes. Les grandes entreprises appartenant au secteur privé ont la responsabilité des données qu'elles génèrent. C'est donc à elles de mettre en place des technologies et des techniques performantes en matière de cybersécurité.

Aux États également de prendre leurs responsabilités, notamment dans la mise en place d'un cadre juridique propre aux menaces et attaques du cyberspace. La prévention appartient au domaine des autorités publiques. Si chaque uti-

lisateur est alerté et informé des menaces numériques à son échelle, les risques d'attaques peuvent être réduits. Organiser des stratégies de défense autour de la cybersécurité

La coopération entre les services nationaux de cybersécurité favorise l'élaboration de stratégies de défense plus efficaces. Cependant, chaque entreprise privée doit également, au sein de son infrastructure interne, réaliser les opérations nécessaires à la sécurité informatique. La mise en conformité aux normes, notamment en matière de traitement des données, est un point majeur à respecter.

Au niveau local, les stratégies de cyberdéfense orchestrées au sein des entreprises sont indispensables pour lutter contre les intrusions. Dans le cas où la cyberattaque dépasse les compétences des services locaux, alors il revient à des organisations de plus grande envergure, comme l'ANSSI en France, de prendre le relais et de venir en aide aux victimes. Intégrer la cyberrésilience dans les ambitions de cybersécurité

Avec la montée en puissance des cyberattaques, le terme de cyberrésilience a été instauré et pris une importance croissante. Le concept repose sur des stratégies de cybersécurité, dans la détection des intrusions, la protection des systèmes et réseaux et la réaction rapide. La résilience ajoute la continuité de l'activité.

En cas de cyberattaque et quelle que soit son importance, l'entreprise continue de délivrer ses services. La cyberrésilience intervient pour limiter les pertes financières. Aujourd'hui, la cybersécurité occupe tous les esprits. Pourtant, le maintien de l'activité est essentiel à la survie d'une entreprise.

Quels avantages peut-on tirer du cyberspace ?

Malgré ses vulnérabilités, le cyberspace constitue un vecteur majeur de développement économique, social et culturel. En facilitant la circulation de l'information et les échanges mondiaux, il réduit les contraintes géographiques et rapproche individus, organisations et institutions. Selon l'Union internationale des télécommunications (UIT), près de 6 milliards de personnes utilisaient Internet en 2025, soit 74 % de la population mondiale. Cette interconnexion favorise l'accès aux connaissances, à la culture et aux services numériques, ainsi que les collaborations scientifiques et les échanges économiques. Toutefois, 2,2 milliards de personnes demeuraient privées d'accès à Internet en 2025.

Le cyberspace transforme également des secteurs essentiels. Dans l'éducation, les plateformes pédagogiques et les cours en ligne ouverts à tous (MOOC) facilitent l'apprentissage et la formation continue, notamment à distance. Dans la santé, la télémedecine permet les consultations, le suivi des patients et l'accès à une expertise médicale sans déplacement systématique. Le télétravail favorise quant à lui la flexibilité professionnelle, limite certains déplacements et peut améliorer l'équilibre entre vie personnelle et professionnelle. Ces évolutions nécessitent néanmoins des infrastructures fiables, une maîtrise des outils numériques et une protection adaptée des données personnelles.

Enfin, l'interconnexion des équipements ouvre de nouvelles perspectives aux particuliers, aux entreprises et aux administrations. Les objets connectés permettent de piloter des équipements domestiques, de surveiller des installations ou d'optimiser la consommation énergétique. Dans les orga-

nisations, les technologies numériques facilitent le partage d'informations, la coordination des activités et la continuité des services. Leur développement contribue également au renforcement de la cybersécurité, grâce à l'amélioration des dispositifs de prévention, de détection et de réponse aux incidents. Le cyberspace apparaît ainsi comme un levier de progrès et d'innovation, à condition de garantir l'accessibilité, la confiance numérique et la résilience.

Cyberspace

Progrès, risques et confiance

Les bénéfices



Accès aux connaissances

Culture, éducation et formation à distance



Santé

Télémedecine et suivi des patients



Travail

Télétravail et collaboration



Économie et innovation

Échanges mondiaux et services numériques



Objets connectés

Pilotage des équipements et optimisation énergétique



Continuité des services

Partage d'informations et coordination

Quels sont les défis/risques du cyberspace ?

Le développement du cyberspace s'accompagne de défis majeurs en matière de sécurité des échanges, de protection des données personnelles et de respect de la vie privée. L'interconnexion des systèmes informatiques multiplie les possibilités d'accès à l'information, mais également les risques de cyberattaques, de vols de données et d'intrusions malveillantes. À ces menaces s'ajoutent la désinformation et la manipulation des contenus, susceptibles de fragiliser la confiance envers les institutions. Face à ces enjeux, la protection du cyberspace exige une responsabilité partagée entre États, entreprises et utilisateurs. En Europe, le Règlement général sur la protection des données (RGPD) encadre le traitement des données personnelles, tandis que la directive NIS 2 renforce les exigences de cybersécurité de nombreuses organisations publiques et privées.

Le cyberspace constitue également un espace de confrontation stratégique entre États, où cyberespionnage, sabotage et déstabilisation peuvent être conduits à distance, parfois sans identification immédiate de leurs auteurs. Les attaques contre les réseaux électriques ukrainiens en 2015 ou les communications satellitaires lors de l'invasion russe de l'Ukraine en 2022 démontrent que ces opérations peuvent perturber des infrastructures essentielles, avec des conséquences matérielles et potentiellement humaines. Elles soulèvent également des difficultés d'attribution et de réponse internationale. Pour les États, l'enjeu dépasse donc la seule protection des données : il concerne la continuité des services publics, la sécurité nationale et la souveraineté.

Enfin, l'évolution rapide des technologies impose une adaptation permanente des dispositifs de cybersécurité et de cyberdéfense. L'informatique en nuage, les objets connectés

Les risques et défis



Cyberattaques et intrusions

Perturbation des systèmes et vols de données



Vie privée

Protection des données personnelles



Désinformation

Manipulation des contenus et perte de confiance



Confrontations entre États

Espionnage, sabotage et déstabilisation



Interdépendances technologiques

Vulnérabilités et effets en cascade



Les conditions de confiance



Accessibilité et formation



Sécurité et coopération



Résilience : anticiper, limiter les effets, rétablir

et l'intelligence artificielle offrent de nouvelles possibilités, mais créent également des vulnérabilités. Les interdépendances technologiques peuvent amplifier les conséquences d'une attaque. La prévention doit donc s'accompagner d'une véritable cyberrésilience, permettant d'anticiper les incidents, d'en limiter les effets et de rétablir les activités essentielles. La formation des personnels, la sécurisation des infrastructures, la coopération entre acteurs publics et privés et la préparation aux crises constituent des leviers indispensables pour renforcer durablement la confiance dans le cyberspace.

DÉFENSE & SÉCURITÉ

LA CYBERGUERRE

Trois notions à distinguer



CYBERATTQUES

Perturber les systèmes, les données ou les services.

01



Estonie • 2007

Des attaques DDoS perturbent les services publics, les banques et les médias.

02



WannaCry • 2017

Un rançongiciel chiffre les fichiers et paralyse des ordinateurs dans le monde.



CYBERESPIONNAGE

Obtenir clandestinement des informations sensibles.

01



Shadow Network • 2010

Des documents et courriels sensibles sont dérobés. Rapport publié en 2010.

02



Newscaster • 2011-2014

Des réseaux sociaux servent à approcher des cibles militaires et politiques.



CYBERGUERRE

Viser des capacités militaires ou stratégiques.

01



Stuxnet • 2010

Un logiciel malveillant sabote des centrifugeuses nucléaires en Iran.

02



Ukraine • 2015

Une attaque contre la distribution électrique provoque des coupures de courant.

Classification éditoriale selon la finalité dominante : les catégories peuvent se recouper.

EN ACTION

Quinze opérations emblématiques

03



Géorgie • 2019

Des sites institutionnels sont défigurés et des chaînes de télévision perturbées.

04



Israël • 2019-2020

Une campagne présumée cible Israël et plusieurs autres pays.

05



Albanie • 2022

Une attaque destructrice touche les services publics et provoque une crise diplomatique.

03



OPM • 2015

Des données personnelles sensibles du personnel fédéral américain sont volées.

04



G20 / Turla • 2017

Une invitation piégée pourrait permettre l'installation d'une porte dérobée.

05



SolarWinds • 2020

Des mises à jour compromises ouvrent un accès indirect aux organisations clientes.

03



NotPetya • 2017

Un logiciel destructeur paralyse des organisations, notamment en Ukraine.

04



KA-SAT • 2022

Les communications satellitaires sont perturbées au début de l'invasion de l'Ukraine.

05



Pologne • 2025

Une attaque contre le secteur énergétique est déjouée, selon les autorités.

Ce classement ne préjuge pas de la qualification juridique ni d'une attribution étatique certaine.