Le cyberespace : conflictualité et coopération entre les acteurs

Introduction :

Lors de l'élection présidentielle américaine de 2016, la société britannique Cambridge Analytica, spécialisée dans l'analyse de données et l'influence de l'opinion sur Internet, a été accusée d'avoir massivement recouru à la désinformation sur les réseaux sociaux pour favoriser l'élection de Donald Trump. Le cyberespace, c'est-à-dire l'environnement d'information et de communication créé par l'interconnexion planétaire des systèmes et des réseaux numériques, s'affirme comme un espace majeur de coopération, mais aussi de conflictualité entre ses différents acteurs.

Depuis le début du XXI^{e} siècle, le cyberespace est en effet devenu un lieu incontournable de production de la connaissance. Les activités politiques, sociales, culturelles et surtout économiques en sont de plus en plus dépendantes, ce qui en fait un espace stratégique pour les États, les FTN et les citoyens. Cependant, le cyberespace est également un potentiel lieu de confrontation militaire entre États. Pour parer aux risques d'une cyberguerre, certains États, comme les pays membres de l'OTAN ou de l'Union européenne, coopèrent dans le domaine de la cyberdéfense, et affirment leur souveraineté numérique.
Par conséquent, nous pouvons nous demander quels sont les enjeux du cyberespace aujourd'hui.

Nous analyserons dans un premier temps le cyberespace comme enjeu géopolitique majeur du monde contemporain avant de nous intéresser à la cyberdéfense entre coopération européenne et souveraineté nationale.

I Le cyberespace, un enjeu géopolitique majeur

Du fait de son poids sans cesse croissant dans les domaines économique, scientifique, culturel, militaire et politique, le **cyberespace**, contrôlé par un

nombre restreint d'acteurs, permet aux États d'affirmer leur puissance.

a Un espace d'affirmation de la puissance des États contrôlé par un nombre restreint d'acteurs

Le cyberespace recouvre les infrastructures matérielles et logicielles qui permettent l'existence d'Internet (comme par exemple les **data centers** ou les câbles sous-marins qui relient les continents entre eux) ainsi que l'espace immatériel ou sont créées et circulent les données. L'existence d'Internet est en effet permise par des centaines de câbles de télécommunications sous-marins longs de milliers de kilomètres qui assurent la transmission des données intercontinentales. Ces autoroutes de l'information véhiculent 99 % des communications mondiales contre 1 % pour les satellites. Ces contraintes matérielles assurent par conséquent à un nombre restreint d'acteurs une position dominante dans le cyberespace. Au premier rang de ces acteurs, on trouve les États-Unis. Leur position centrale dans le réseau de câbles sous-marins fait d'eux un point de transit incontournable pour 97 % des données échangées entre l'Europe et l'Asie par exemple.
De plus, les États-Unis abritent sur leur territoire 40 % du total mondial des data centers. Enfin, les **GAFAM** dominent très nettement la dimension immatérielle d'Internet.

Exemple

> Le moteur de recherche Google assure 90 % des recherches mondiales sur Internet (plus de 3 milliards par jour), tandis que Facebook comptait 2,7 milliards d'utilisateurs actifs à travers le monde au deuxième trimestre 2020.

Définition

> **GAFAM :**
>
> Acronyme désignant les très grosses entreprises américaines dispersées dans plusieurs pays et qui dominent les technologies du numérique (Google, Amazon, Facebook, Apple et Microsoft).

Cette forte concentration des acteurs de l'Internet tend à placer les GAFAM dans une situation **oligopolistique** (un faible nombre d'acteurs très puissants empêchant l'émergence de nouveaux acteurs sur un marché à forte demande) qui leur permet de drainer la plus grande partie du marché du numérique.

Exemple

> Microsoft et Apple, par exemple, détiennent 95 % du marché des systèmes d'exploitation pour ordinateur de bureau.

Cette forte concentration des acteurs du numérique a également un impact sur la circulation des contenus depuis le début des années 2000. Les GAFAM se positionnent en effet comme intermédiaires dans la diffusion de l'information (moteurs de recherche, algorithmes de réseaux sociaux) et dans la communication entre les internautes (messageries, réseaux sociaux).

→ Grâce à leurs moteurs de recherche Google Chrome et Microsoft Edge, Google et Microsoft détiennent à eux seuls 80 % du marché des navigateurs.

Les GAFAM et leurs homologues asiatiques investissent par ailleurs massivement dans l'installation de câbles sous-marins.

Exemple

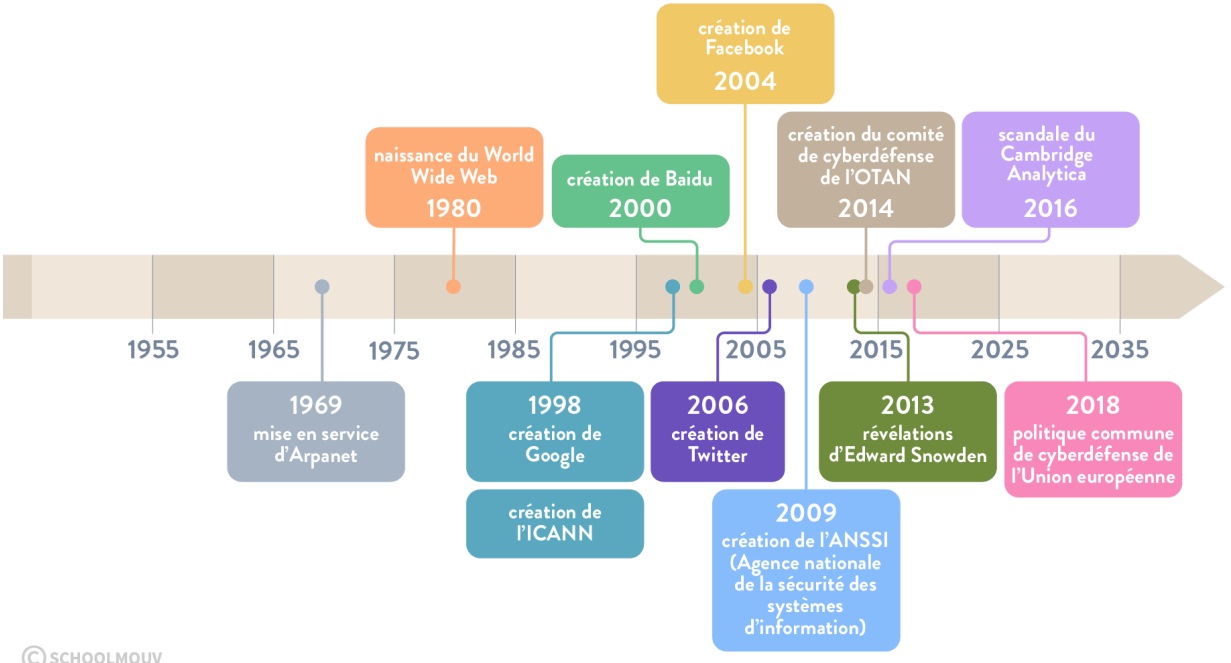
> Le câble sous-marin Hong Kong-Americas (HKA) par exemple, long de 13 780 kilomètres et reliant Hong Kong en Asie à Los Angeles et San Franciso sur la côte ouest des États-Unis, est la propriété de Facebook, Telstra (entreprise australienne de télécommunication), Tata Communications (FTN indienne), China Telecom et China Unicom.

La circulation de l'information étant un **enjeu géopolitique majeur**, des États contestent la domination américaine sur le cyberespace. En 2011, Cuba et le Venezuela, deux États socialistes hostiles à la diplomatie américaine ont ainsi financé la pose d'un câble sous-marin optique en mer des Caraïbes pour éviter les risques d'espionnage de leurs communications. De nouveaux acteurs du numérique émergent également dans le monde,

comme en Chine et en Russie. La Chine, pays qui compte le plus d'internautes au monde, s'affirme de plus en plus dans le cyberespace mondial alors même qu'Internet a réellement fait son entrée dans le pays à la fin des années 1990. La Chine poursuit un double objectif à travers le développement des **BATX** chinoises. Elle entend à la fois s'imposer économiquement et politiquement sur le cyberespace, tout en contrôlant étroitement les contenus auxquels les internautes chinois ont accès. Si les GAFAM prônent le principe de l'Internet libre et celui de la libre circulation des informations, le parti communiste chinois a promu le numérique à des fins économiques et géopolitiques, tout en appliquant une stricte censure dans le cyberespace.

Définition

> **BATX :**
>
> FTN chinoises du numérique (Baidu, Alibaba, Tencent et Xiaomi).



Désireux de contrôler l'information à laquelle la population chinoise à accès, le parti communiste chinois a encouragé le développement de FTN chinoises du numérique, tout en fermant son marché intérieur aux GAFAM. C'est ainsi que sont apparues les BATX.
Baidu, qui a vu le jour en 2000 est par exemple l'équivalent chinois de

Google, tandis qu'Alibaba, créé en 1999 par Jack Ma et aujourd'hui la plus grosse capitalisation boursière d'Asie (le groupe est valorisé à 479 milliards de dollars en 2019) est spécialisé dans le domaine du commerce en ligne, comme Amazon. Enfin, Tencent, fondé en 2008, est le concurrent direct de Facebook, tandis que Xiaomi, fabricant chinois de smartphones, est celui d'Apple.

Bien que moins puissantes que les GAFAM américaines, les BATX chinoises commencent à leur faire de l'ombre. Tencent, par exemple, atteignait une capitalisation boursière de 457 milliards de dollars fin 2018 contre 404 milliards pour Facebook. Fortes du soutien de l'État chinois, les BATX envisagent maintenant de conquérir le marché international.
Cette ambition chinoise dans le domaine du numérique est au cœur de la guerre commerciale qui fait rage entre la Chine et les États-Unis depuis 2016.


Exemple

> Chaque minute, 3,8 millions de recherches sont par exemple formulées sur le moteur de recherche Google.


À retenir

> Le cyberespace est un espace d'affirmation de la puissance des États. Cependant, cet espace est dominé par un nombre restreint d'acteurs. Les États-Unis et la Chine, entre autres, s'y livrent une **guerre commerciale et d'influence**. Longtemps dominé par les GAFAM, le cyberespace voit émerger de nouveaux acteurs depuis les années 2010, notamment les BATX chinoises, dont le développement bénéficie du soutien du gouvernement chinois, qui applique une censure stricte d'Internet sur son territoire. Les GAFAM et les BATX se livrent à une guerre commerciale au centre de laquelle se trouvent les **données des utilisateurs**.
>
> → Le **stockage et le traitement des données** qui circulent sur le cyberespace sont en effet un fondement majeur de l'**économie** d'aujourd'hui et le seront encore plus demain.

b Un espace en proie aux tensions

Le cyberespace représente un important enjeu de souveraineté et de puissance pour les États.

Définition

> **Souveraineté :**
>
> Droit absolu d'exercer une autorité (législative, judiciaire, politique) sur une région, un pays ou un peuple. La souveraineté nationale désigne l'indépendance de l'État-nation par rapport à d'autres États ou à des instances internationales.

L'organisation institutionnelle, économique et politique des États, ainsi que la vie quotidienne des populations, dépend en effet toujours plus des espaces numériques. Les États s'efforcent donc de protéger au mieux les données qui transitent dans le cyberespace des menaces extérieures. Au contraire, certains États, comme la Chine, contrôlent les données qui circulent dans leur cyberespace en censurant ce dernier et en imposant à leurs ressortissants l'utilisation d'outils numériques sur lesquels l'État exerce un contrôle (Pékin n'a autorisé Google à développer ses activités en Chine qu'à la condition que les autorités chinoises puissent contrôler les recherches effectuées sur le moteur de recherche google.cn).

Depuis le début du XXI^{e} siècle, la souveraineté des États fait l'objet d'un nombre grandissant de menaces dans le cyberespace. Ces menaces prennent trois formes : le sabotage, l'espionnage et la subversion (c'est-à-dire la contestation de l'ordre établi).
Elles sont initiées par différents acteurs : États, groupes criminels (terroristes, mafieux) ou d'activistes et entreprises.

→ Ces menaces, qui prennent forme au cœur du cyberespace, laissent présager la possibilité pour certains États ou groupes terroristes de s'engager dans de véritables **cyberguerres** à brève échéance.

Définition

> **Cyberguerre :**

> Guerre menée dans le cyberespace au moyen d'ordinateurs et d'Internet dans le but de paralyser complètement un adversaire.

À défaut de pouvoir déclencher une véritable cyberguerre, certains États disposant des ressources informatiques nécessaires comme les États-Unis, Israël ou la Chine se livrent à des **cyberattaques** ciblées à l'encontre de leurs adversaires. La finalité de ces cyberattaques est de porter un coup économique ou militaire à leurs adversaires sans pour autant employer de moyens militaires conventionnels.


Définition

> **Cyberattaque :**
>
> Acte malveillant envers un dispositif informatique via un réseau cybernétique.


Exemple

> Le meilleur exemple dans ce domaine est la vaste attaque informatique qui a visé les installations nucléaires iraniennes en 2010 au moyen du virus STUXNET. Ce logiciel malveillant a été conçu par la NSA en collaboration avec l'unité 8200, spécialisée dans la guerre informatique de l'armée israélienne.
> En 2010, il a été introduit dans le programme informatique de la centrale de Natanz, et a détruit un millier des 5000 centrifugeuses de ce site d'enrichissement d'uranium, clef de voûte du programme nucléaire iranien, en modifiant leur vitesse de rotation jusqu'à ce qu'elles soient hors d'usage.

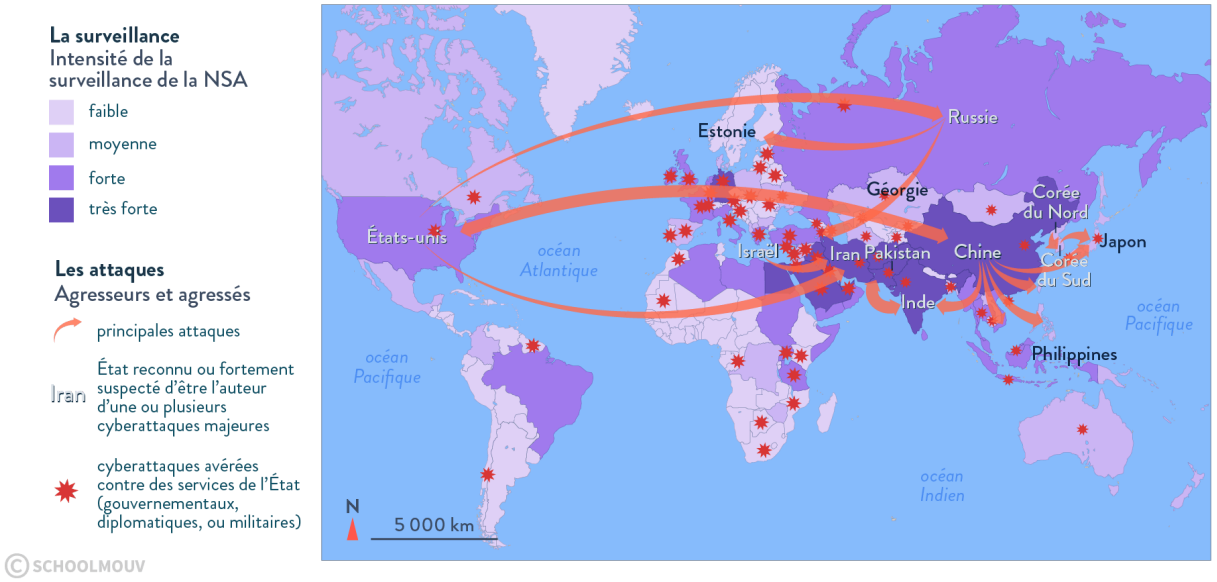
En dehors des cyberattaques de rançonnage initiées par des groupes terroristes (comme lorsque des pirates bloquent un site Internet ou dérobent des données en ligne et les restituent contre rançon), des groupes d'activistes utilisent également le cyberespace comme un instrument d'expression et de résistance face aux tentatives de censure de l'Internet. La Chine compte ainsi le plus grand nombre de **cyberdissidents** au monde.


Définition

Cyberdissident :

Dissident vis-à-vis d'un gouvernement s'exprimant essentiellement ou uniquement via Internet.

Principales cyberattaques dans le monde en 2018



Principales provenances des cyberattaques selon le domaine ciblé en 2018

finance (17 % du total des cyberattaques)	États-Unis : **42 %**	Chine : **8 %**	Royaume-Uni : **6 %**
technologie (17 % du total des cyberattaques)	Chine : **37 %**	États-Unis : **21 %**	Russie : **5 %**
domaine du commerce et des services (12 % du total des cyberattaques)	États-Unis : **26 %**	Chine : **15%**	France : **10 %**
éducation (11 % du total des cyberattaques)	États-Unis : **25 %**	Pays-Bas : **16 %**	Vietnam : **15 %**
gouvernement (9 % du total des cyberattaques)	États-Unis : **37 %**	Allemagne : **14 %**	France : **13 %**

Source : ©NTT Security

Le groupe d'activistes **Anonymous**, créé en 2003, mène depuis 2008 de nombreuses cyberattaques. En 2011, les Anonymous ont par exemple

soutenu les cyberdissidents tunisiens lors de la **Révolution du Jasmin** et ont lancé des attaques contre des sites djihadistes en 2015, en représailles à l'attentat commis contre le journal satirique *Charlie Hebdo*.

Enfin, le cyberespace constitue une arme géopolitique pour les États. Il leur permet en effet d'influencer l'opinion publique nationale ou internationale.

Exemple

> En 2011, suite à des manifestations étudiantes à Karthoum en plein Printemps arabe, le président soudanais Omar el-Béchir décida de la création de groupes de cyberdjihadistes, dont la mission était de faire taire les groupes anti-gouvernementaux sur les réseaux sociaux.
> L'État islamique, pour sa part, a utilisé la propagande et les cyberattaques pour influencer l'opinion publique mondiale en sa faveur. En avril 2015, le groupe terroriste a piraté la chaîne de télévision TV5 Monde, interrompant les programmes et diffusant des messages de soutien à la cause djihadiste sur les réseaux sociaux de la chaîne internationale francophone.

À retenir

> Le cyberespace est en proie à de nombreuses **tensions** générées par différents acteurs. Les cyberattaques prennent plusieurs formes : sabotage d'installations industrielles ou de câbles sous-marins, espionnage ou espionnage industriel et subversion. Les acteurs de ces attaques sont multiples.
> À côté des États, on retrouve des groupes d'activistes, des organisations terroristes ou encore des organisations criminelles qui pratiquent le **rançonnage ou le vol de données en ligne**.

2 La cyberdéfense entre coopération européenne et souveraineté nationale

La multiplication des cyberattaques (82 % des entreprises françaises ont déclaré avoir été victime d'au moins une cyberattaque en 2015) dans le monde et les liens troubles qui existent entre certains cybercriminels et des États, rendent difficile la coopération dans le domaine de la **cyberdéfense**.

a Une gouvernance mondiale en construction

Pendant de nombreuses années, seuls les États-Unis ont été en mesure de mettre en œuvre une politique coordonnée de cyberdéfense. Eux seuls disposaient des moyens technologiques nécessaires grâce aux GAFAM et à **l'ICANN**.

Définition

ICANN :

Organisation à but non lucratif installée en Californie et qui administre les ressources numériques d'Internet comme les noms de domaines et l'adressage IP. L'ICANN œuvre pour la préservation de la sécurité, de la stabilité et de l'interopérabilité de l'Internet. Originellement dépendante de l'administration américaine, elle est indépendante depuis 2016.

Définition

Cyberdéfense :

Ensemble des moyens physiques et virtuels mis en place par un pays dans le cadre de la guerre informatique menée dans le cyberespace.

Aujourd'hui, de nombreux États et certaines FTN comme Siemens et Microsoft souhaitent voir émerger une **gouvernance** élargie dans les domaines de la cyberdéfense et de la protection des données. Depuis 2014, Microsoft plaide pour l'adoption de normes internationales de sécurisation du cyberespace et pour la création d'une agence chargée de leur application sur le modèle de l'Agence internationale de l'énergie atomique.

Définition

Gouvernance :

Coordination de l'ensemble des règles, des mesures et des acteurs qui constituent une autorité afin d'assurer le bon fonctionnement et le

> contrôle d'un État, d'une institution ou d'une organisation, qu'elle soit publique ou privée, régionale, nationale ou supranationale.

Cependant, les entraves à la mise en place d'une gouvernance mondiale sont nombreuses.

- Tout d'abord, le cyberespace étant un espace virtuel, seuls les matériels qui le sous-tendent, comme les serveurs ou les câbles sous-marins peuvent être physiquement rattachés à un territoire.
- De plus, il est impossible d'attribuer avec certitude une cyberattaque à un acteur défini, ce qui rend inopérant le principe de légitime défense.
- Enfin, du point de vue juridique, le droit des conflits ne s'applique au cyberespace que si les cyberattaques interviennent dans le contexte d'une guerre conventionnelle. Par conséquent, les cyberattaques qui se déroulent en dehors de ce cadre légal échappent au droit international.

Depuis 2006, le secrétaire général des Nations Unies a mis en place un Forum mondial sur la gouvernance de l'Internet qui vise, entre autres points, à traiter les questions de politique publique relatives aux principaux éléments de la gouvernance de l'Internet afin de contribuer à la viabilité, à la sécurité, à la stabilité et au développement de l'Internet. Cependant, les efforts internationaux sont entravés par les réticences de certains États qui s'opposent à l'application du droit international dans le cyberespace et à l'émergence d'une véritable gouvernance mondiale.

Exemple

> C'est particulièrement le cas de **l'Organisation de coopération de Shanghai**, organisation intergouvernementale régionale créée en 2001 qui regroupe la Chine, la Russie, le Kazakhstan, le Kirghizistan, le Tadjikistan et l'Ouzbékistan et a pour but d'assurer la sécurité des États adhérents. On mesure l'étendue du défi posé par cette opposition à l'essor d'une gouvernance mondiale dans le domaine de la cybersécurité lorsque l'on sait que la Russie est l'un des pays d'où proviennent le plus grand nombre de cyberattaques.

Toutefois, on observe des avancées notables depuis 2015. En 2015, l'ONU a en effet réussi à faire adopter un rapport sur les comportements dans le cyberespace qui préconise aux États membres de coopérer avec les États victimes d'attaques, de lutter contre la prolifération de logiciels malveillants et de ne pas endommager les infrastructures vitales des autres États. Le rapport encourage également le partage des informations dans le domaine de la cybersécurité.

→ L'appel de Paris du 12 novembre 2018 pour la confiance et la cybersécurité, lancé par le président Macron à l'occasion de la réunion à l'UNESCO du Forum sur la gouvernance de l'Internet, a reçu le soutien de 67 États et 497 organisations internationales et FTN. Cependant, c'est aux échelons régional et national que l'on assiste à la mise en place de coopérations efficaces.

À retenir

> Depuis le milieu des années 2000, de nombreux États et des FTN plaident pour la mise en place d'une gouvernance mondiale dans le domaine de la cyberdéfense afin d'entraver les menaces qui pèsent sur la liberté d'Internet et la protection des données numériques. Cependant, des oppositions restreignent ces efforts soutenus par l'ONU. L'Organisation de coopération de Shangai, par exemple, rejette toute forme d'atteinte à sa souveraineté dans le contrôle du cyberespace.

b La France et la coopération européenne dans le domaine de la cyberdéfense

La première cyberattaque documentée à avoir paralysé un État européen a eu lieu en 2007. Le pays visé était l'Estonie, membre de l'Union européenne depuis le 1er mai 2004. Fin avril 2007, les autorités estoniennes ont pris la décision de déplacer le monument érigé en l'honneur des soldats de l'armée rouge qui avaient participé à la libération du pays en 1944 du centre-ville de Tallinn, la capitale, vers un cimetière militaire.
Contestée par le gouvernement russe mais également par l'importante population russophone du pays (un tiers des habitants), cette décision a entraîné, dès le 27 avril 2007, c'est-à-dire au lendemain du déplacement de la statue, une vague d'attaques informatiques contre les sites Internet

gouvernementaux et publics du pays, ainsi que contre ceux d'opérateurs téléphoniques, de banques et de médias.
Ces cyberattaques visaient à saturer les sites concernés par une multitude de demandes de connexions simultanées. Les perturbations engendrées par ces attaques, si elles culminèrent le 9 mai 2007, s'étendirent sur un mois et demi et eurent de graves conséquences. L'Estonie est en effet l'un des pays les plus en avance dans le domaine des services en ligne. 95 % des opérations bancaires s'effectuent par exemple par communication électronique.

La cyberattaque de 2007 a donc considérablement perturbé la vie quotidienne des habitants ainsi que le fonctionnement de l'État. Son ampleur laisse à penser qu'un État en est responsable ou l'a commandité. Les soupçons se sont portés vers les services secrets russes sans pour autant que des preuves tangibles aient pu être rassemblées pour corroborer cette accusation.

→ En somme, l'exemple estonien illustre parfaitement les conséquences que peut avoir une cyberattaque sur la vie institutionnelle et quotidienne d'un pays et l'urgence pour les États européens de construire une gouvernance commune en matière de cyberdéfense. Pour faire face à ces attaques, les États européens se dotent progressivement de moyens en matière de cybersécurité.

L'OTAN joue un rôle prépondérant dans la cybercoopération en Europe.

 Définition

> **OTAN :**
>
> Organisation politico-militaire mise en place par les pays signataires du traité de l'Atlantique nord en 1949, afin de pouvoir remplir leurs obligations de sécurité et de défense collectives.

En 2013, l'OTAN a proposé de transposer le droit international aux cyberconflits dans un guide rédigé par un groupe d'expert. Ce guide, intitulé ***Manuel de Tallinn***, définit également la qualification d'une cyberattaque dans la conduite des hostilités lors d'un conflit armé international.
En 2016, l'OTAN a adopté une stratégie de cybersécurité dont la clef de

voûte réside dans la protection de ses réseaux numériques et dans la formation de ses États membres à la cybersécurité. Cette coopération au sein de l'OTAN se double d'efforts pour la mise en place d'une gouvernance européenne dans le domaine de la cybersécurité. Cette ébauche de gouvernance passe par la conclusion d'accords de coopération bilatérale entre États membres de l'Union européenne, à l'image de l'accord conclu entre la France et l'Estonie en 2010.
Depuis 2018, on assiste à une accélération des efforts dans la mise en place d'une gouvernance européenne dans le domaine de la cybersécurité avec la mise en place d'une politique commune de cyberdéfense. L'année suivante, en 2019, les États membres ont adopté un règlement nommé **Cybersecurity Act** qui pérennise l'ENISA, agence européenne pour la cybersécurité créée en 2004. Cette agence a pour mission d'apporter son soutien à la coopération opérationnelle entre les États membres.
Enfin, la même année, l'Union européenne et l'OTAN ont annoncé le renforcement de leur coopération sur la cyberdéfense.

→ Malgré ces progrès récents, l'Union européenne demeure encore très dépendante des États-Unis et de leurs moyens matériels, notamment dans le cadre de l'OTAN, pour assurer sa cybersécurité.

À retenir

Cibles de nombreuses cyberattaques, les États européens mettent progressivement en place une gouvernance européenne dans le domaine de la cyberdéfense. Cette coopération repose sur la conclusion d'accords bilatéraux de coopération entre États membres de l'Union européenne et sur la mise en place d'une politique commune de cybersécurité. Cependant, en dépit de progrès notables, les pays de l'Union européenne demeurent dépendants de l'OTAN, c'est-à-dire des États-Unis, pour assurer leur cyberdéfense.

Conclusion :

Le cyberespace est un enjeu géopolitique majeur du monde contemporain. Espace d'affirmation de la puissance des États, le cyberespace est contrôlé par un nombre restreint d'acteurs, au premier plan desquels on retrouve les États Unis avec les GAFAM et une poignée d'États disposant de moyens technologiques et matériels de pointe, comme la Chine qui encourage l'essor des BATX.

Cependant, le rôle sans cesse croissant, joué par le cyberespace dans l'économie et la sphère politique, fait naître de nombreuses tensions entre ses différents acteurs. Si le risque d'une cyberguerre est à craindre à long terme, à court terme, on observe une recrudescence des cyberattaques menées par des activistes, des cybercriminels, voire les services militaires ou de renseignement de certains États.

Pour remédier à ces menaces, la communauté internationale, soutenue par des FTN comme Microsoft, encourage l'émergence d'une gouvernance mondiale dans le domaine de la cyberdéfense. Cependant, cette initiative portée par l'ONU est en proie à l'opposition de certains États comme la Russie ou la Chine, qui refusent tout abandon de souveraineté.

C'est au niveau régional que s'observent les avancées les plus significatives dans ce domaine. L'Union européenne a, par exemple, adopté une politique commune de cybersécurité et ses États membres ont conclu des accords bilatéraux pour renforcer leur défense dans le cyberespace. Malgré cela, les pays de l'Union européenne demeurent dépendants des États-Unis pour assurer leur cyberdéfense grâce aux moyens matériels de l'OTAN.