FICHE « Pour approfondir » : **La cybersécurité : quelles réponses aux menaces nouvelles ?**

Face à la multiplication des attaques menées à partir d'Internet, les États se sont progressivement dotés de nouveaux moyens technologiques et institutionnels pour se protéger contre cette nouvelle menace. C'est l'ensemble de ces moyens que l'on désigne par le terme de "cybersécurité".

I - Qu'est-ce que la cybersécurité ?

1 - Cyberattaque et cyberdéfense

Le préfixe *cyber* (du grec *kuberneïn*, diriger) renvoie aux ordinateurs et à Internet. La "cybersécurité" porte à la fois sur la cyberattaque et sur la cyberdéfense, c'est-à-dire l'usage de moyens informatiques pour mener ou riposter à une agression. On peut distinguer deux types d'attaques :

- l'infiltration de réseaux de communications à des fins d'espionnage, d'altération de données ou de prise de contrôle ;
- les campagnes d'influence sur le Net, visant à orienter l'opinion publique.

2 - Le cyberespace, champ de bataille planétaire

Le "cyberespace" est l'espace de communication ouvert par l'interconnexion de tous les ordinateurs via Internet. Il comprend des zones publiques (un blog) et privées (une messagerie, l'intranet d'une entreprise). C'est l'espace sur lequel s'exerce la cybermenace. La particularité du cyberespace est d'abolir les distances et les frontières nationales. Par son caractère planétaire, **la cybermenace bouleverse donc les repères traditionnels de la sécurité**.

3 - Les acteurs de la cybersécurité

La cybersécurité implique des acteurs de statut et de taille très diverses. Parmi eux, on trouve :

- les États et leurs forces armées ;
- les acteurs économiques (de la PME à la multinationale).

La particularité du cyberespace est de brouiller les critères traditionnels de la puissance. Ainsi, les géants du numérique ont souvent des capacités d'action comparables à celles des États. De même, un individu isolé peut à lui seul mettre en danger les systèmes informatiques d'une grande entreprise ou d'un État.

4 - Les intérêts en jeu

Les motivations à l'origine de ces cyberattaques sont principalement de nature économique et politique.

Intérêts économiques :

- vol d'argent à un particulier ou à une entreprise (via de faux e-mails incitant à fournir ses identifiants bancaires par exemple) ;
- campagne de dénigrement d'une entreprise visant à capter sa clientèle ;
- espionnage industriel, etc.

Intérêts politiques :

- campagne d'influence visant à orienter le résultat d'un vote ;
- espionnage politique et militaire ;
- prise de contrôle des outils de communication à distance, etc.

5 - Le cas du cyberterrorisme

Des groupes terroristes ont pu investir le cyberespace pour mener leur combat. Ils y ont vu un moyen de rééquilibrer le rapport de force à leur avantage, Internet permettant de **mener des offensives d'envergure avec des moyens limités**. Ainsi, ils ont pu récolter des fonds, recruter des combattants ou encore pirater des sites internet à des fins de propagande grâce à l'outil numérique.

Mais les autorités craignent aujourd'hui des attaques de plus grande envergure, comme la prise de contrôle d'infrastructures stratégiques. En février 2017, le Conseil de sécurité des Nations unies a adopté une résolution incitant les États à se préparer pour **intervenir efficacement en cas d'attaque contre les infrastructures essentielles**.

II - Quelles réponses contre la cybermenace ?

1 - La surveillance d'Internet

Pour surveiller les cybercommunications et lutter contre la cybercriminalité, les États se sont dotés de dispositifs de surveillance dédiés à Internet. Des organes inter-étatiques de surveillance existent, comme le réseau Échelon. Géré conjointement par les États-Unis, le Canada, l'Australie, le Royaume-Uni et la Nouvelle-Zélande, **Échelon est le plus gros réseau de surveillance des télécommunications** et cybercommunications au monde. Toutefois, de tels outils sont à double tranchant puisqu'ils peuvent servir à des fins d'espionnage (économique, militaire) ou de contrôle des populations.

2 - La collaboration avec les géants du Net

Pour exercer leur autorité sur le cyberespace, les États doivent compter sur la **coopération des géants du Net**. En plus d'avoir des moyens techniques et financiers supérieurs à de nombreux États, ces derniers ont le pouvoir de dissimuler ou au contraire de rendre publiques les informations qui circulent via leurs services.

3 - Une difficile réponse internationale

Face au caractère international de la cybermenace, les États ont tôt pressenti **la nécessité d'une réponse internationale commune**. Mais celle-ci se heurte à la lenteur des procédures de coopération nationale, ainsi qu'à la réticence des États à partager certaines informations. Les carences de la coopération internationale en matière de cybersécurité sont ainsi apparues au grand jour à l'occasion des attentats terroristes qui ont frappé l'Europe ces dernières années. En réponse à ces attaques, les différents gouvernements se sont engagés à plus de coopération.

4 - Vers un droit international de la cybersécurité ?

Malgré les appels répétés de nombreux responsables politiques, **il n'existe toujours pas de droit international contraignant en matière de cybersécurité**. En effet, il existe des divergences de fond quant à la manière dont les États envisagent leur cybersécurité.

5 - L'exception européenne

En 2001, le Conseil de l'Europe est à l'origine du **premier traité de coopération internationale sur la cybersécurité**. Connu sous le nom de **Convention de Budapest**, ce traité a été signé par les 45 États membres du Conseil de l'Europe, même si tous ne l'ont pas ratifié par la suite.

Au sein d'Europol, l'Union européenne (UE) a inauguré, en 2013, le **Centre européen de lutte contre la cybercriminalité**, visant à faciliter la coopération entre États européens dans la lutte contre le cybercrime.

La Commission européenne a proposé, en septembre 2017, le "**paquet cybersécurité**" qui comprend un ensemble de mesures dont l'introduction d'une certification de cybersécurité à l'échelle de l'UE et la consolidation de l'Agence permanente de l'UE pour la citoyenneté.

III - Le cas français

La France fait de la cybersécurité sa priorité depuis les années 2000. Le retour de la menace terroriste en 2015 l'a poussée à intensifier ses efforts en la matière. La Stratégie nationale pour la sécurité du numérique a fixé cinq objectifs :

- garantir la souveraineté nationale ;
- répondre aux actes de cybermalveillance ;
- informer le grand public ;
- faire de la sécurité numérique un avantage concurrentiel pour les entreprises ;
- renforcer la voix de la France à l'international.

1 - La surveillance d'Internet

La lutte contre la cybercriminalité passe d'abord par **la surveillance d'Internet**. **Le décret n°2015-125** permet le blocage administratif des sites pédopornographiques et faisant l'apologie du terrorisme. En 2015 est votée la loi « Renseignement », qui renforce les moyens d'action des services de renseignement dans la sphère numérique. À la suite des attentats de Paris en 2015, le gouvernement a également lancé l'opération "**Stop Djihadisme**" afin de contrecarrer les campagnes de propagande jihadiste sur les réseaux sociaux.

2 - La cybersécurité dans le droit français

En France, la cybercriminalité est prise en compte dans le droit depuis la **loi informatique et libertés** (1978) qui réglemente la liberté de ficher les personnes humaines. Aujourd'hui, les pratiques numériques sont encadrées par un dispositif juridique prévoyant **des peines allant jusqu'à cinq ans d'emprisonnement et 75 000 euros d'amende** pour les attaques informatiques. La loi prévoit en outre une aggravation des peines dans le cas de cyberattaques visant directement l'État.

3 - Traquer les cybercriminels

La police et la gendarmerie disposent de **divers organes dédiés à la répression de la cybercriminalité**. Parmi eux :

- l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) au sein de la Police judiciaire ;
- le Centre de lutte contre les criminalités numériques (C3N) au sein de la Gendarmerie nationale ;
- la Brigade d'enquête sur les fraudes liées aux technologies de l'information (BEFTI) au sein de la préfecture de police de Paris.

4 - Défendre les usagers

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée en 2009 pour défendre et protéger les systèmes d'information et les usagers du numérique contre les cyberattaques. Ses missions sont les suivantes :

- surveiller les réseaux afin de détecter les attaques et permettre de réagir au plus vite ;
- développer des produits et services de cybersécurité à destination des usagers ;
- apporter son expertise et son assistance aux administrations et aux entreprises ;
- sensibiliser le public sur les cybermenaces.

Le gouvernement a lancé en 2017 un dispositif national d'assistance aux victimes d'actes de cybermalveillance. Incubé par l'ANSSI et copiloté avec le ministère de l'Intérieur, la plateforme **cybermalveillance.gouv.fr** permet de mettre en relation des victimes de cyberattaques - particuliers, entreprises ou collectivités territoriales - et des prestataires de services susceptibles de les aider dans leurs démarches.

5 - La cyberdéfense

Créé en 2017 et dépendant du ministère des armées, le **Commandement de la cyberdéfense** (COMCYBER) a la responsabilité de la cyberdéfense militaire qui recouvre l'ensemble des actions défensives et offensives conduites dans le cyberespace. **Le COMCYBER est constitué de 3 400 cyber-combattants**, auxquels viendront s'ajouter 1 000 combattants supplémentaires d'ici 2025.

Le 18 janvier 2018, la ministre des armées a présenté **la doctrine de lutte informatique offensive (LIO)** qui complète la lutte informatique défensive (LID). La ministre a ainsi officialisé le volet offensif de la doctrine cybermilitaire française. La LIO et la LID renforcent la posture permanente de cyberdéfense (PPC) créée par **la loi de programmation militaire 2019-2025**. La PCC permet de **protéger en permanence tous les réseaux militaires** et de réagir à toute attaque contre les intérêts de la défense de la France.

Livre blanc de la cyberdéfense, **la Revue stratégique de cyberdéfense** a été publiée en février 2018 par le Secrétariat général de la défense nationale (SGDN).

Source : **https://www.vie-publique.fr/eclairage/18469-la-cybersecurite-quelles-reponses-aux-menaces-nouvelles**
28 janvier 2019 (+précisions et mises à jour personnelles)