France Diplomatie

La France et la cybersécurité

Sommaire

De nouvelles pratiques destructrices se développent dans le cyberespace : utilisations criminelles d'internet (cybercriminalité), y compris à des fins terroristes, propagation de fausses informations ou manipulations à grande échelle, espionnage à visée politique ou économique, attaques contre les infrastructures critiques (transport, énergie, communication…) à des fins de sabotage, etc.

Émanant de groupes étatiques ou non-étatiques, les cyberattaques :

- **se jouent des frontières** et des distances ;
- **sont difficilement attribuables** : il est très difficile d'identifier formellement le véritable attaquant, qui agit souvent sous couvert de relais involontaires (botnets) ou d'intermédiaires (proxies) ;
- **peuvent être réalisées relativement facilement**, à bas coût et à très faible risque pour l'attaquant. Elles visent à mettre en péril le bon fonctionnement des systèmes d'information et de communication (SIC) utilisés par les citoyens, les entreprises et les administrations, voire l'intégrité physique d'infrastructures essentielles à la sécurité nationale.

La cybersécurité recouvre l'ensemble des mesures de sécurité susceptibles d'être prises pour se défendre contre ces attaques. L'augmentation constante du niveau de sophistication et d'intensité des cyberattaques a conduit ces dernières années la plupart des pays développés à renforcer leur résilience et à adopter des stratégies nationales de cybersécurité.

Un dispositif national robuste qui monte en puissance

Dès 2015, la France s'est dotée d'une Stratégie nationale pour la sécurité du numérique (https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf). Destinée à accompagner la transition numérique de la société française, elle répond aux nouveaux enjeux nés des évolutions des usages numériques et des menaces qui y sont liées. Elle met en avant cinq lignes d'action :

- Garantir la souveraineté nationale ;
- Apporter une réponse forte contre les actes de cybermalveillance ;
- Informer le grand public ;
- Faire de la sécurité numérique un avantage concurrentiel pour les entreprises françaises ;
- Renforcer la voix de la France à l'international.

Cette stratégie a par la suite été étoffée par :

- La Stratégie internationale de la France pour le numérique
  Présentée par le ministre de l'Europe et des Affaires étrangères en décembre 2017, ce texte synthétise l'ensemble des orientations stratégiques que la France promeut dans le monde numérique autour de trois piliers : gouvernance, économie, sécurité.
- La Revue stratégique de cyberdéfense (http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf)

Confiée par le premier ministre au secrétaire général de la défense et de la sécurité nationale et présentée en février 2018, elle définit une doctrine de gestion des crises cyber. Cette revue clarifie les objectifs d'une stratégie nationale de cyberdéfense et confirme la pertinence du modèle français et la responsabilité première de l'État en la matière.

Aux niveaux techniques et opérationnels, divers acteurs contribuent à l'efficacité du dispositif français :

- Créée en 2009, l'**Agence nationale de sécurité des systèmes d'information** (http://www.ssi.gouv.fr/) (ANSSI) est l'autorité nationale en matière de cybersécurité. Véritable « pompier » du cyberespace français, elle est **chargée de la prévention (y compris en matière normative) et de la réaction aux incidents informatiques visant les institutions sensibles**. Elle organise par ailleurs des exercices de gestion de crises au niveau national. L'ANSSI embauche aujourd'hui 600 personnes et continue de croître.
- Le **ministère des Armées** a la double mission d'assurer la protection des réseaux qui sous-tendent son action et d'intégrer le combat numérique au cœur des opérations militaires. Afin de consolider l'action du ministère dans ce domaine, un commandement de cyberdéfense (http://www.defense.gouv.fr/portail-defense/enjeux2/cyberdefense) (COMCYBER), placé sous les ordres du chef d'État-major des Armées, a été créé début 2017.
- Le **ministère de l'Intérieur (http://www.interieur.gouv.fr/A-votre-service/Ma-securite/Conseils-pratiques/Sur-internet)** a pour mission de **lutter contre toutes les formes de cybercriminalité, visant aussi bien les institutions et les intérêts nationaux, les acteurs économiques et les collectivités publiques, que les particuliers**. Il mobilise à cette fin les services centraux spécialisés et les réseaux territoriaux de la police nationale, de la gendarmerie nationale et de la sécurité intérieure. Ceux-ci sont chargés des enquêtes visant à identifier les auteurs d'actes de cybermalveillance et à les déférer à la justice. Ces services contribuent en outre à la prévention et à la sensibilisation des publics concernés.

Stabilité et sécurité internationale dans le cyberespace

Le renforcement de la stabilité stratégique et de la sécurité internationale dans le cyberespace est l'un des objectifs prioritaires de la France. Le ministère de l'Europe et des Affaires étrangères coordonne les travaux de la France en matière de « cyberdiplomatie ».
Cette action se décline dans un cadre européen et internationale.

Garantir l'autonomie stratégique numérique européenne
Au sein de l'Union européenne (UE), la France défend une vision ambitieuse et le concept « d'autonomie stratégique numérique de l'UE », gage de notre capacité collective d'initiative et d'action. Cet objectif se décline en trois axes :

- **Axe technologique**
  La politique industrielle de l'Union européenne soutient les capacités de recherche et développement de pointe afin de favoriser le déploiement de technologies et de services numériques de sécurité, dont la fiabilité doit pouvoir être évaluée. L'intégration de la sécurité dans l'ensemble des composantes numériques permettra également de donner un avantage concurrentiel aux offres européennes.
- **Axe réglementaire**
  La politique extérieure de l'Union européenne doit définir des réglementations prenant en compte les exigences de compétitivité et les potentialités du numérique tout en restant protectrices des citoyens, des entreprises, des États membres, conformément à nos valeurs communes (droit à la vie privée et protection des données à caractère personnel, protection des infrastructures critiques).
- **Axe capacitaire**
  L'Union européenne a un rôle essentiel dans la promotion et le soutien au développement des capacités de cyberdéfense des entités publiques et privées au sein des États membres ainsi que des institutions européennes elles-mêmes, en s'appuyant sur des savoir-faire européens. Elle peut également apporter son soutien dans les domaines de la formation et de l'entraînement, ce qui crée des synergies et évite les redondances de capacités..

Au-delà de ces différentes dimensions, il apparaît nécessaire de renforcer la coopération opérationnelle entre les États membres de l'Union européenne. L'objectif est de disposer, à l'échelle européenne, d'outils de partage d'information technique sur les menaces, permettant d'anticiper et de répondre rapidement à une attaque informatique. La mise en place en 2017 d'un cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance (« Boîte à outils cyberdiplomatique ») s'inscrit pleinement dans cette démarche de coopération.

Mobiliser la communauté internationale avec l'Appel de Paris
L'Appel de Paris pour la confiance et la sécurité dans le cyberespace témoigne du rôle actif joué par la France dans la promotion d'un cyberespace sûr, stable et ouvert. **Déclaration politique de haut niveau, ce texte marque une mobilisation renouvelée sur l'enjeu fondamental de la stabilité dans le cyberespace.** Présenté le 12 novembre 2018, au Paris Peace Forum et soutenu par le président de la République à l'UNESCO devant le Forum sur la gouvernance de l'internet, il témoigne de la capacité de la France à mobiliser largement autour de sa vision de la régulation dans le cyberespace.

Soutenu par plus de 500 entités (États, entreprises, etc.), ce texte rappelle des principes fondamentaux, comme l'application du droit international et des droits de l'Homme dans le cyberespace et mentionne un certain nombre de principes – comportement responsable des Etats, monopole étatique de la violence légitime, reconnaissance des responsabilités spécifiques des acteurs privés –se rattachant à la vision française d'un cyberespace sûr.

L'approche inclusive de l'Appel de Paris souligne la **nécessité d'une approche multi-acteurs pour élaborer les normes et bonnes pratiques** qui nous permettront de profiter de manière fiable et sécurisée des possibilités offertes par la révolution numérique. La France entend aujourd'hui mener une réflexion, avec ses partenaires étatiques mais aussi du secteur privé et de la société civile, sur **le rôle et les responsabilités spécifique des acteurs privés dans le renforcement de la stabilité et de la sécurité internationale du cyberespace**.

Promouvoir la stabilité du cyberespace dans les enceintes internationales
Au sein de l'ONU, où sont discutées les règles de comportement responsable dans le cyberespace, la France a participé aux cinq derniers groupes d'experts gouvernementaux (GGE) sur la cybersécurité dont les travaux ont permis d'ancrer le cyberespace dans le système international issu de la Charte des Nations Unies et d'orienter les États dans une dynamique de prévention, de coopération et de non-prolifération dans le cyberespace.

La France est engagée dans d'autres enceintes internationales où sont abordées les questions de cybersécurité, notamment :

- **Au sein de l'Alliance Atlantique**, la France a été à l'initiative dans l'adoption par les 28 Nations d'un **Engagement pour la cyberdéfense** (« Cyberdefence Pledge ») lors du Sommet de Varsovie en juin 2016. Celui-ci a reconnu le **cyberespace comme un domaine d'opérations**, engageant ainsi l'OTAN à s'y défendre comme elle le fait dans les domaines terrestre, aérien et maritime. En mai 2018, **la France a accueilli la toute première conférence dédiée au Cyberdefence Pledge**.
- **Au G7**, le groupe Ise-Shima créé en 2016 et dédié aux questions cyber a permis d'aboutir, en 2017, à l'adoption d'une déclaration ambitieuse concernant les normes de comportement responsable des États dans le cyberespace. Dans le cadre de sa présidence du G7 en 2019, la France sera force de proposition en vue de promouvoir le respect de ces normes.
- **À l'OSCE**, qui s'est imposée comme une enceinte régionale de référence pour la définition et la mise en œuvre des mesures de confiance appliquées au cyberespace, la France continue de promouvoir un agenda ambitieux d'opérationnalisation de ces mesures afin de renforcer la transparence, la coopération et la confiance entre les pays membres de l'organisation.

Mise à jour : janvier 2019
