DROIT INTERNATIONAL APPLIQUÉ AUX OPÉRATIONS DANS LE CYBERESPACE

RÉSUMÉ

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES ARMÉES

En l'espace de deux décennies, le cyberespace est devenu un lieu de tension et de confrontation. L'instabilité et l'insécurité liées à l'accroissement des risques et des menaces dans ce milieu, ainsi que l'usage d'Internet à des fins criminelles ou terroristes, fragilisent l'ensemble des démocraties. L'augmentation constante du niveau de sophistication et d'intensité des cyberattaques a conduit ces dernières années la plupart des États à renforcer leur résilience et à adopter des stratégies nationales de cybersécurité.

Dans ce contexte, la France a adopté une position forte en publiant une stratégie nationale de cyberdéfense en février 2018 puis, dans la lignée des efforts inscrits dans la loi de programmation militaire 2019-2025, Madame Florence Parly, ministre des armées, et le général d'armée François Lecointre, Chef d'état-major des armées, ont présenté le 18 janvier 2019 deux documents fondateurs : une instruction ministérielle de lutte informatique défensive et une doctrine de lutte informatique offensive à des fins militaires, qui encadre l'emploi de la cyber-arme.

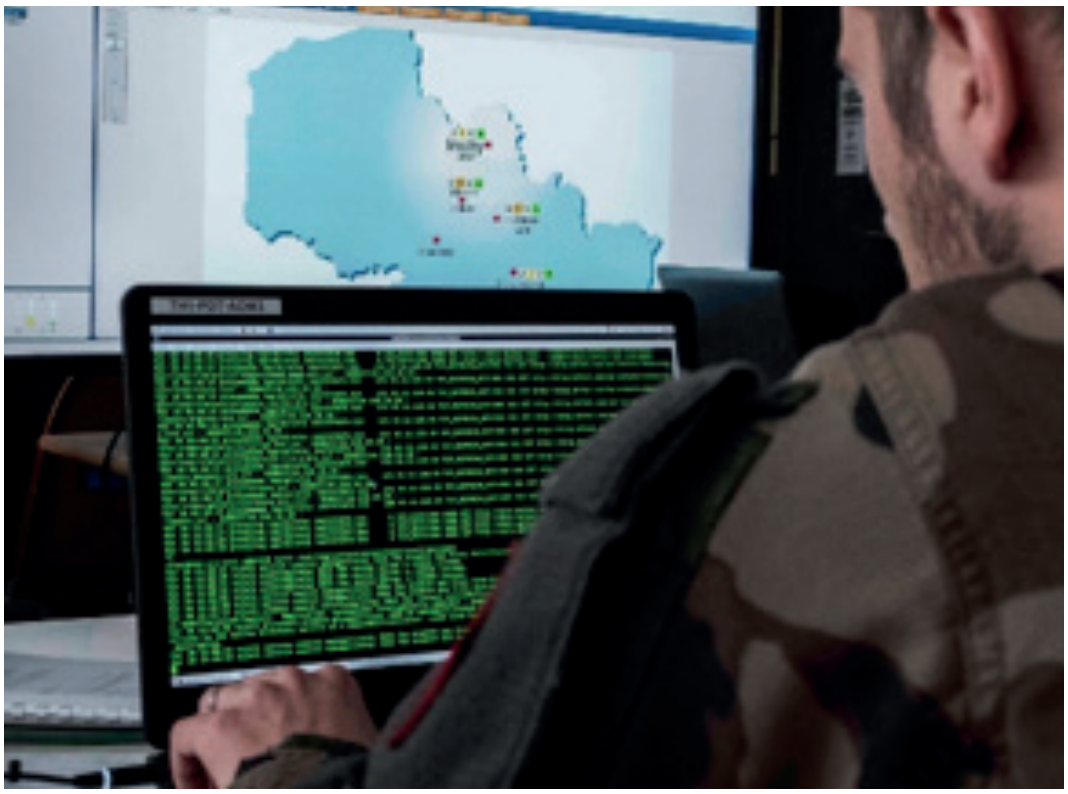
Cette transparence qu'affiche la France au travers de ces documents est le reflet d'un Etat qui se veut responsable. Elle s'inscrit en cohérence avec sa conception d'un cyberespace libre, sûr, ouvert, stable, fondé sur la confiance et les règles du droit international. Dans la continuité de l'Appel de Paris pour la confiance et la sécurité dans le cyberespace, la France entend ainsi porter une conception et une utilisation du cyberespace conformes aux buts des Nations Unies de maintien de la paix et de la sécurité internationales.
L'instruction ministérielle sur la lutte informatique défensive permet de bâtir une défense unifiée, réactive, spécialisée et cohérente de l'ensemble des moyens

numériques du ministère. Autour du Commandant de la cyberdéfense et de la posture permanente de cyberdéfense, elle articule les missions relevant de la protection des installations du ministère face aux menaces cyber, et celles relevant de l'anticipation et de la défense de ces systèmes.
La lutte informatique offensive à des fins militaires élargit la palette des options à la disposition de nos autorités politiques et militaires. Qu'elle soit engagée pour recueillir du renseignement à haute valeur ajoutée, pour mener des opérations de lutte contre la propagande anti-française ou de neutralisation de systèmes adverses, cette nouvelle capacité s'impose graduellement dans les opérations. Pour la première fois, des éléments de cette doctrine de lutte informatique offensive ont été rendus publics. Ils ont pour objectifs de faire partager les grands principes d'emploi de cette composante opérationnelle militaire et d'accompagner l'engagement des armées dans ce champ de confrontation.

Si la France a déjà eu l'occasion de partager publiquement certains éléments de son interprétation de l'application du droit international dans le cyberespace (via différents documents de stratégie et de doctrine, des contributions et initiatives internationales que nous avons portées ces dernières années), **il lui manquait encore un document de référence** abordant de façon transverse les enjeux juridiques et politiques liés à cette question. Un tel document apparait d'autant plus nécessaire au moment où les négociations, qui reprendront en septembre 2019 au sein de l'ONU sur les enjeux de cybersécurité, porteront largement sur la façon dont le droit international trouve à s'appliquer dans le cyberspace.
Lors des précédentes négociations onusiennes, de nombreux Etats ont reconnu l'applicabilité du droit international au cyberespace. En revanche il revient à chaque Etat la responsabilité d'exprimer avec transparence la façon dont il considère que le droit international s'applique dans cet espace ; ce que la France a exprimé, notamment dans sa stratégie nationale de cyberdéfense.

C'est dans ce contexte qu'en juillet 2018, la ministre des Armées a constitué un **groupe de travail (GT) visant à souligner la détermination française à voir appliquer le droit international dans les opérations cyber.**

Ce rapport vient préciser la position de la France, qui considère que le respect du droit international est la condition nécessaire à l'émergence d'une régulation adaptée au cyberespace. Il vient ainsi conforter l'engagement constant de la France en faveur du respect du droit international existant, y compris dans le domaine cyber, et sa volonté de faire preuve d'exemplarité et de transparence dans un contexte international où de nombreux acteurs maintiennent un discours ambigu sur ces sujets.



Sans précédent au niveau international, il met en exergue certaines spécificités de l'approche française, notamment en ce qui concerne les contours du concept de souveraineté dans le cyberespace, le seuil du recours à la force ou d'une agression armée, l'interdiction de faire usage du droit de légitime défense en réaction à la violation par un Etat du principe de diligence due, ou la définition de l'attaque en contexte de conflit armé.

La France espère ainsi ouvrir un débat entre les nations et prolonger l'effort entamé lors de *l'Appel de Paris* pour la confiance et la sécurité dans le cyberespace ; convaincue que c'est ensemble que nous parviendrons à garantir un cyberespace libre, sûr, ouvert, stable, fondé sur la confiance et les règles du droit international.