11 juillet 2018

IRSEM
INSTITUT DE RECHERCHE STRATÉGIQUE
DE L'ÉCOLE MILITAIRE

NOTE DE RECHERCHE – n° 58

# LE DROIT INTERNATIONAL DANS LA « STRATÉGIE NATIONALE DE LA CYBERDÉFENSE »

**François DELERUE**
*Chercheur Cyberdéfense et droit international à l'IRSEM*
**Aude GÉRY**
*Chercheuse associée à la Chaire Castex de Cyberstratégie*

## RÉSUMÉ

Cette note recense et analyse les différents points de droit international présents dans la *Stratégie nationale de la cyberdéfense* rendue publique en février 2018. La *Stratégie nationale de la cyberdéfense* réaffirme la position française déjà exprimée dans le Livre blanc de 2013 : le droit international s'applique aux comportements des États dans le cyberespace. Dans une période où le droit international est remis en cause, la France formule de manière claire et relativement détaillée son attachement aux normes de droit international, piliers de la paix et de la stabilité internationales. La *Stratégie nationale* constitue, de l'avis des auteurs, un des documents les plus complets jamais rendus publics par la France sur son approche du droit international. Elle expose les positions françaises sur certaines obligations internationales, comme la souveraineté, le principe de non-intervention ou encore l'obligation de diligence (*due diligence*) et les réactions possibles à des actes internationalement illicites – mesures de rétorsion, contre-mesures et légitime défense.
Avec la publication d'un document aussi complet sur les questions de cyberdéfense, surtout en ce qui concerne les négociations internationales et le droit international, la France se place comme une nation motrice au niveau européen et mondial. Dans une période troublée pour le droit international applicable au cyberspace à la suite de l'échec du dernier Groupe d'experts gouvernementaux (GGE) et, plus généralement, de remise en cause de l'ordre juridique international, la France énonce avec force sa vision et son attachement à la régulation internationale comme vecteur de la paix et de la sécurité internationales, notamment dans le cyberespace, et à un Internet ouvert, sûr et pacifique.

## SOMMAIRE

Les années 2017/2018 resteront des années charnières pour l'approche et la stratégie française de cyberdéfense[1]. La création du commandement de cyberdéfense (COMCYBER) au sein du ministère des Armées a été suivie de la publication de la *Revue de défense et de sécurité nationale*[2], de la *Stratégie internationale du numérique*[3] et de la *Stratégie nationale de la cyberdéfense*, en attendant l'adoption, prévue à l'été 2018, de la loi de programmation militaire qui contiendra des dispositions relatives à la stratégie française de cyberdéfense.

La *Stratégie nationale de la cyberdéfense* est parue le 29 juin 2018[4]. Elle avait été officiellement présentée et rendue publique sous le titre de « Revue stratégique de cyberdéfense[5] », le 12 février 2018 à la Station F, par Louis Gautier, secrétaire général de la Défense et de la Sécurité nationale, qui l'a qualifiée de véritable « Livre blanc du cyber », la comparant au *Livre blanc sur la défense nationale* de 1972 établissant la doctrine nucléaire de la France. La présente note et les références concernent la *Stratégie nationale de la cyberdéfense* publiée en juin 2018.

La *Stratégie nationale* comporte trois parties. La première, à dimension pédagogique, est consacrée aux « Dangers du monde cyber ». Elle évalue les menaces, leur évolution et les acteurs impliqués. Elle précise également la position française sur le concept de cyberdissuasion, qu'elle réfute en réaffirmant que la dissuasion n'est que nucléaire (p. 46). La deuxième partie, « L'État, responsable de la cyberdéfense de la nation », détaille l'approche française de la cyberdéfense, en posant le principe de séparation des capacités et missions défensives et offensives. Elle présente aussi la stratégie internationale de la France sur les enjeux de cyberdéfense, notamment ses positions sur le droit international. Enfin, la troisième partie, « L'État, garant de la cybersécurité de la société », définit le concept de souveraineté numérique, qu'il faut néanmoins distinguer de la souveraineté au sens juridique du terme.

La *Stratégie nationale de la cyberdéfense* répète la position française déjà exprimée dans le Livre blanc de 2013 : le droit international s'applique aux comportements des États dans le cyberespace (p. 100). Elle note que la « France dispose d'une vision claire, spécifique et précise de l'application du droit international dans le cyberespace ». De manière générale, il convient de souligner que ce texte entre dans un niveau de détails assez poussé quant au droit international applicable. Si le droit international est l'objet principal du titre « V. L'action internationale de la France dans le domaine cyber » (p. 92-112) et de l'Annexe 7 (p. 188-192), la *Stratégie nationale* revient également sur les normes de droit international à plusieurs reprises. L'objectif de la présente note est de décrire les différents points pertinents sur le droit international développés dans la *Stratégie nationale de la cyberdéfense*.

## Applicabilité du droit international aux comportements des États dans le cyberespace

« [L]es principes et règles de droit international s'appliquent aux comportements des États dans le cyberespace » (p. 82). Cette affirmation vient confirmer la position de la France déjà exprimée plusieurs fois, notamment dans :

- Le *Livre blanc sur la défense et la sécurité nationale* de 2013 ;
- Le discours de Jean-Yves Le Drian, ministre de la Défense, lors de la visite de la Direction générale de l'armement-Maîtrise de l'information (DGA-MI), à Bruz (Ille-et-Vilaine), le 12 décembre 2016 ;
- La *Revue stratégique de défense et de sécurité nationale* de 2017 ;
- La *Stratégie internationale de la France pour le numérique* de 2017 et le discours de Jean-Yves Le Drian, ministre de l'Europe et des Affaires étrangères, à Aix-en-Provence (Bouches-du-Rhône), le 15 décembre 2017.

La *Stratégie nationale* mentionne à diverses reprises l'attachement de la France aux travaux du Groupe d'experts gouvernementaux (GGE) chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale des Nations unies, notamment la reconnaissance de l'applicabilité du droit international, et en particulier de la Charte des Nations unies, énoncée dans les rapports de 2013 et 2015 (p. 43, 100, 103 et 105). La *Stratégie nationale* revient sur l'échec du cinquième GGE en juin 2017, soulignant qu'il est « le signe d'une divergence fondamentale de

1. Cette note fait suite à deux publications en anglais : François Delerue et Aude Géry, « France's Cyberdefense Strategic Review and International Law », *Lawfare*, 23 mars 2018, https://www.lawfareblog.com/frances-cyberdefense-strategic-review-and-international-law et « The French Strategic Review of Cyber Defense », ISPI, 2 mai 2018, https://www.ispionline.it/en/pubblicazione/french-strategic-review-cyber-defense-20376
2. https://www.defense.gouv.fr/dgris/presentation/evenements/revue-strategique-de-defense-et-de-securite-nationale-2017
3. https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/strategie-internationale-de-la-france-pour-le-numerique/
4. https://www.economica.fr/livre-strategie-nationale-de-la-cyberdefense-sgdsn,fr,4,9782717869941.cfm
5. http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/

perception, parmi les différents pays, de l'architecture internationale de la sécurité devant régir les relations entre États à l'ère numérique » (p. 44). Elle précise que bien que signant l'arrêt des négociations à l'ONU, cet échec « ne remet nullement en cause les normes et principes agréés au cours des années précédentes » (p. 44), réaffirmant ainsi l'engagement de la France de se conformer aux recommandations adoptées. Enfin, la position de la France au regard des points de discorde du dernier GGE est rappelée : « [l]a France a également eu l'occasion, avec plusieurs de ses partenaires, d'affirmer sa position en faveur de la reconnaissance claire et univoque de la licéité des moyens de réponse à une cyberattaque, qu'ils impliquent un recours à la force (légitime défense) ou non (contre-mesures, mesures de rétorsion, etc.), et de l'applicabilité du droit international humanitaire aux cyberopérations conduites dans le cadre de conflits armés » (p. 103). Ces différentes affirmations peuvent être lues comme un engagement fort de la France en matière d'application du droit international et de sa volonté de maintenir la paix et la sécurité internationales dans le cyberespace, objectif maintes fois énoncé tout au long de la *Stratégie nationale*.

La *Stratégie nationale* va plus loin qu'une simple reconnaissance de l'applicabilité du droit international dans le cyberespace. Elle détaille en effet les positions françaises au sujet de certaines obligations internationales et les réactions possibles à des actes internationalement illicites.

## Les obligations internationales des États dans le cyberespace

La *Stratégie nationale* rappelle que la violation d'une obligation internationale par un État, par une action ou une omission, constitue un fait internationalement illicite (p. 101-102). Sans apporter de précision, elle rappelle que la responsabilité de l'État peut être engagée par les actes de ses organes ou ceux « d'acteurs non étatiques […] si l'État exerce une forme de contrôle sur les auteurs de l'attaque » (p. 101). Compte tenu du rôle joué par les proxys dans le cyberespace et des difficultés d'attribution, il aurait cependant été intéressant que la *Stratégie nationale* précise la position française sur le niveau de contrôle que devrait exercer l'État pour que les actes d'un acteur privé lui soient attribuables.

À propos des violations possibles du droit international, elle indique que des cyberopérations pourraient notamment constituer des violations de la souveraineté d'un État, du principe de non-intervention, de l'interdiction du recours à la force ou encore de l'obligation de diligence (*due diligence*) (p. 100-102). Dans cette perspective, elle souligne que « [l]e principe de souveraineté s'applique au cyberespace. À ce titre, la France réaffirme qu'elle exerce sa souveraineté sur les systèmes d'information, les personnes et les activités cyber sur son territoire, dans la limite de ses obligations découlant du droit international » (p. 100). Si cette position, partagée par de nombreux États, s'inscrit dans la continuité de l'interprétation retenue par le GGE en 2015 (§ 29 a, p. 14), on peut néanmoins regretter que la *Stratégie nationale* ne détaille pas sa position quant à l'application du principe de souveraineté sur les données, notamment stratégiques.

En outre, elle revient sur l'obligation de diligence (*due diligence*) à plusieurs reprises (p. 102, 105 et 190). Elle rappelle qu'un État a l'« obligation de ne pas laisser sciemment utiliser son territoire aux fins d'actes contraires aux droits d'autres États » (p. 102) et qu'il s'agit d'une obligation de moyens sur la base de laquelle la responsabilité d'un État pourrait être engagée même s'il n'est pas le commanditaire de l'acte (p. 102). Elle souligne également qu'il convient de « notifier au préalable à l'État que ses infrastructures sont utilisées à des fins malveillantes (critère de connaissance) et de s'assurer que l'État n'a pas rempli son obligation (de moyens) de faire cesser l'attaque » (p. 102).

On aurait pu s'attendre à ce que la *Stratégie nationale* renvoie aux éléments sur la *due diligence* présents dans le rapport du GGE de 2015. En effet, le rapport de 2015 mentionne à deux reprises, sans la citer, l'obligation de diligence, disposant que les États « ne devraient pas permettre sciemment que leur territoire soit utilisé pour commettre des faits internationalement illicites à l'aide des technologies de l'information et des communications » (§ 13 c, p. 9) et « devraient veiller à ce que des acteurs non étatiques n'utilisent pas leur territoire pour commettre de tels actes » (§ 27 e, p. 15). Ce choix différent pourrait sembler surprenant dans la mesure où la *Stratégie nationale* tend à inscrire les positions françaises dans la continuité des rapports du GGE.

Concernant l'application de l'obligation de diligence, la *Stratégie nationale* note que « [d]ans cette optique, la France doit en particulier œuvrer à parvenir à un accord, au niveau international, sur les obligations qui pèsent sur un État dont les infrastructures seraient utilisées à des fins malveillantes » (p. 105). Cette proposition, qui aurait pu être plus détaillée, soulève plusieurs questions : s'agit-il d'un accord contraignant juridiquement, c'est-à-dire d'un traité international, ou plus simplement de prolonger le développement des normes de comportement sur ces questions ? De la

même manière, s'agit-il d'obligations juridiquement contraignantes ou de *soft law* ? Le paragraphe suivant reprenant les recommandations du GGE et proposant de les prolonger dans d'autres cadres, il paraît probable qu'il s'agisse d'un accord non-juridiquement contraignant sur des normes de comportement, et non d'un traité international codifiant l'obligation de diligence appliquée au domaine cyber. Par ailleurs, la *Stratégie nationale* semble préciser le contenu d'une de ces obligations en suggérant la « mise en place d'une chaîne de responsabilité permettant à l'État victime de bénéficier de l'assistance des États par lesquels transite l'attaque » (Annexe 7, p. 189). Cette proposition découlerait, selon la *Stratégie nationale*, de la norme adoptée en 2015 par le GGE selon laquelle « [l]es États devraient répondre aux demandes d'aide appropriées formulées par un autre État dont une infrastructure essentielle est exposée à des actes de malveillance informatique ; ils devraient aussi répondre aux demandes appropriées visant à atténuer les conséquences d'activités informatiques malveillantes dirigées contre une infrastructure essentielle d'un autre État et exercées depuis leur territoire, en tenant dûment compte de la souveraineté » (§ 13 h, p. 9-10). On aurait pu s'attendre à ce que cette proposition intéressante soit détaillée davantage.

## Les réponses possibles en droit international

La *Stratégie nationale de la cyberdéfense* se concentre principalement sur les formes possibles de réponse conformes au droit international (p. 97-103 et 189-192). Elle adopte une approche conforme au droit international et s'inscrit dans la continuité des réponses reconnues dans le rapport de 2015 du GGE (§ 29 c, p. 15) qui ont néanmoins été remises en cause par certains États lors du dernier GGE. Elle rappelle que « [la] France doit tout d'abord s'efforcer d'avoir recours à des mécanismes de coopération internationale et de règlement pacifique des différends » (p. 100). La *Stratégie nationale* souligne ensuite que « si la situation le nécessitait, il serait alors possible de prendre des mesures de rétorsion, de recourir à des mécanismes exceptionnels d'autoprotection et/ou d'adopter des contre-mesures pacifiques. Les cas les plus graves pourraient nécessiter une réponse constitutive d'un recours à la force » (p. 103). La notion de « mécanismes exceptionnels d'autoprotection » semble ici faire référence aux circonstances excluant l'illicéité, et plus précisément à l'état de nécessité. La *Stratégie nationale* détaille expressément les trois formes de mesures unilatérales que pourrait adopter la France en réponse à une cyberopération conformément au droit international : les mesures de rétorsion, les contre-mesures et la légitime défense (p. 100-102).

Il convient de souligner que cette analyse des modalités de réponse s'inscrit dans la continuité des récentes évolutions du droit national, notamment à la suite de l'adoption de l'article 21 de la loi de programmation militaire de 2013[6], codifié dans l'article L2321-2 du Code de la défense, qui précise que « [p]our répondre à une attaque informatique qui vise les systèmes d'information affectant le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation, les services de l'État peuvent, dans les conditions fixées par le Premier ministre, procéder aux opérations techniques nécessaires à la caractérisation de l'attaque et à la neutralisation de ses effets en accédant aux systèmes d'information qui sont à l'origine de l'attaque ». La *Stratégie nationale* semble reprendre le contenu de cet article, tout en rappelant que sa mise en œuvre doit s'inscrire dans les limites du droit international : « la possibilité pour un État victime d'une cyberattaque ayant atteint une infrastructure critique de prendre les mesures techniques nécessaires et proportionnées afin de neutraliser les effets de cette attaque, dans le respect de ses obligations en matière de droit international ».

La *Stratégie nationale de la cyberdéfense* s'attarde tout particulièrement sur les conditions et modalités de mise en œuvre de la légitime défense. Si elle fait référence à l'article 51 de la Charte des Nations unies, elle ne mentionne aucunement le droit coutumier international. Elle souligne qu'une agression armée se définit par sa gravité et ses effets, reprenant ainsi implicitement les deux critères cumulatifs définis par la Cour internationale de justice dans l'affaire *Nicaragua* (p. 101, § 191). Elle signale par ailleurs qu'une attaque informatique pourrait être qualifiée d'agression armée « en raison de pertes en vies humaines substantielles ou de dommages physiques aux biens considérables. Dans une telle hypothèse, l'État serait victime d'une attaque informatique causant des dégâts et/ou des victimes similaires à ceux qui résulteraient de l'utilisation d'armes classiques » (p. 100).

Elle va plus loin dans la définition de l'agression armée en se référant à la théorie de l'accumulation des effets, et reconnaît ainsi qu'une agression armée peut être constituée de plusieurs actes qui, si analysés séparément, n'atteindraient

6. Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.

pas le seuil de l'agression armée (p. 101). En outre, elle indique, au sujet de la qualification d'une agression armée, qu'« [u]ne seconde hypothèse pourrait être celle d'une attaque informatique visant un État, qui semblerait constituer la première étape d'une intervention militaire massive plus classique » (p. 100).

La *Stratégie nationale* confirme la position française en faveur de la légitime défense préemptive : « [c]ompte tenu des spécificités du vecteur cyber (une attaque peut se préparer clandestinement et être mise en œuvre très rapidement ; les dégâts peuvent être considérables sur tous les plans, humains, financiers, organisationnels), la France ne peut exclure de recourir, dans des circonstances exceptionnelles, à la légitime défense contre une agression armée non encore déclenchée mais sur le point de l'être, de façon imminente et certaine, pourvu que l'impact potentiel de cette agression soit suffisamment grave » (p. 102). Cette position n'est pas nouvelle et avait déjà été exprimée dans la Loi de programmation militaire de 2003 : « la possibilité d'une action préemptive pourrait être considérée, dès lors qu'une situation de menace explicite et avérée serait reconnue[7] ». Néanmoins, c'est la première fois qu'elle est formulée aussi explicitement.

Il convient de souligner qu'avec la légitime défense préemptive et la théorie de l'accumulation des effets, l'approche française rejoint celle d'un certain nombre d'autres États et s'écarte de l'approche traditionnelle du droit international.

Les modalités de mise en œuvre de la légitime défense en réponse à une cyberopération peuvent aussi être analysées à la lumière d'autres points développés dans la *Stratégie nationale*. Premièrement, la *Stratégie nationale* propose la création d'une catégorie d'infrastructures qualifiées de « supercritiques » (p. 76-77). Selon l'approche générale de la doctrine, la qualification d'une agression armée dépend généralement de la gravité et des effets de la cyberopération. Cependant, la nature de la cible peut aussi constituer un facteur aggravant. Il convient donc de s'interroger, en cas de cyberopération contre une infrastructure supercritique, de l'impact de cette qualification sur la détermination de savoir s'il s'agit ou non d'une agression armée. Deuxièmement, la *Stratégie nationale* propose un schéma de classement des attaques informatiques, faisant un parallèle avec celui adopté par les États-Unis qui « n'est pas directement transposable » dans le contexte français, et note qu'il est essentiellement fondé sur les effets induits par l'incident (p. 97-99). Il est probable que ce schéma servira de base pour déterminer si une cyberopération constitue une agression armée, et plus largement dans l'évaluation des réponses possibles à toute forme de cyberopération. Troisièmement, tout en rappelant son opposition aux *hack-back* par le secteur privé, elle indique que « [l]a question d'une potentielle exception à l'interdiction générale de recours à des actions cyberoffensives par des entreprises privées en cas de légitime défense devra être posée au niveau international » (p. 108). Ouvrant ainsi la possibilité pour un État de demander l'assistance d'acteurs non étatiques dans la mise en œuvre de mesures de légitime défense, ces acteurs non étatiques pourraient alors mener des cyberopérations dépassant le seuil du recours à la force qui seraient imputables à cet État.

La *Stratégie nationale* rappelle qu'en dessous du seuil de l'agression armée, même en cas de recours à la force, il n'est pas possible d'invoquer la légitime défense (p. 101), et que seules les mesures de rétorsion et les contre-mesures seraient envisageables sous certaines conditions. Elle rappelle que les contre-mesures ne peuvent être prises qu'en réponse à un fait internationalement illicite, et doivent être nécessaires, proportionnées et pacifiques (p. 101 et 191-192). De la même manière, elle définit les mesures de rétorsion (p. 191).

La *Stratégie nationale* insiste tout particulièrement sur l'importance de la coopération internationale et sur les possibilités de réponses multilatérales, renvoyant notamment à la possibilité de saisir le Conseil de sécurité des Nations unies (p. 100, 105, 190 et 192) et à la *cyber tool box* récemment adoptée par les États européens pour coordonner leurs réponses en cas de cyberopération (p. 191).

La *Stratégie nationale* réaffirme enfin l'applicabilité du *jus in bello* (p. 102) et rappelle que « [l]es grands principes de ce droit sont la nécessité, la proportionnalité, la distinction et l'humanité » et que « les armes cyber doivent pouvoir être utilisées de manière discriminante ». En matière de neutralité, elle distingue le transit d'une cyberopération et l'utilisation des infrastructures, le premier étant tolérable et pas le second.

7. Loi n° 2003-73 du 27 janvier 2003 relative à la programmation militaire pour les années 2003 à 2008.

## Conclusion

La *Stratégie nationale de la cyberdéfense* publiée en juin 2018, reprenant la « Revue stratégique de cyberdéfense » présentée en février 2018, est un document important qui fera date concernant la stratégie française de cyberdéfense et l'approche française du droit international.

Dans une période où le droit international est remis en cause, la France réaffirme de manière claire et relativement détaillée son attachement aux normes de droit international, piliers de la paix et de la stabilité internationales. La *Stratégie nationale* constitue, de l'avis des auteurs, un des documents les plus complets jamais rendus publics par la France sur son approche du droit international.

La *Stratégie nationale* consacre également de longs développements aux mesures relevant de la *soft law*, en particulier les normes de comportement responsable et les mesures de confiance, qu'elles s'appliquent aux États ou à d'autres acteurs, ainsi qu'à la coopération internationale et aux forums au sein desquels les discussions prennent et pourraient prendre place à l'avenir.

Avec la publication d'un document aussi complet sur les questions de cyberdéfense, notamment en ce qui concerne les négociations internationales et le droit international, la France se place comme une nation motrice dans ce domaine au niveau européen et mondial. Dans une période troublée pour le droit international applicable au cyberspace à la suite de l'échec du dernier GGE et, plus généralement, de remise en cause de l'ordre juridique international, la France affirme avec force sa vision et son attachement à la régulation internationale comme vecteur de la paix et de la sécurité internationales, notamment dans le cyberespace, et à un Internet ouvert, sûr et pacifique.

**François Delerue est chercheur cyberdéfense et droit international à l'IRSEM, chercheur associé à la Chaire Castex de Cyberstratégie et enseignant à Sciences Po Paris. Il mène des recherches portant sur le droit international, notamment sur l'impact des nouvelles technologies (conquête spatiale, robotique, intelligence artificielle, etc.), sur les normes et la coopération internationale, et sur les questions de cyberdéfense et de cybersécurité tant sous l'angle juridique, stratégique que politique. Il intervient régulièrement à l'Institut international de Droit humanitaire (IIDH) de Sanremo, ainsi que dans diverses autres institutions. Il a enseigné à l'IUE et à l'Université de Florence (Università degli Studi di Firenze). Il a soutenu son doctorat intitulé *State-Sponsored Cyber Operations and International Law* en novembre 2016 à l'Institut universitaire européen (IUE - Florence, Italie), sous la direction du Professeur Nehal Bhuta. Il a été chercheur invité à l'Université de Columbia à New York (2014) et auditeur de la 62e session jeune de l'IHEDN (2009) et du séminaire « International Law and Cyber Operations » de l'École de l'OTAN à Oberammergau (2013). Il est titulaire d'un Master recherche en droit international et organisations internationales de l'Université de Paris 1 Panthéon-Sorbonne (2011) et d'un *LL.M. in Comparative, European and International Laws de l'IUE* (2013).**

**Aude Géry est doctorante à l'Université de Rouen. Sa thèse porte sur le droit international face à la prolifération des armes numériques. Elle est également chercheuse associée à la Chaire Castex de Cyberstratégie. Ses recherches portent sur les enjeux de la régulation internationale de l'espace numérique, tant aux plans juridiques que stratégiques. Elle a travaillé pour le ministère des Armées et pour CEIS, et intervient régulièrement sur les questions de lutte contre la prolifération des armes numériques et droit international. Elle est également officier de réserve au sein de l'Armée de Terre.**

**Contacts :** francois.delerue@sciencespo.fr **;** gery.aude@gmail.com