Réponse de la France à la résolution 73/27 relative aux « Progrès de l'informatique et des télécommunications et sécurité internationale » et à la résolution 73/266 relative à « Favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale »

RAPPORT

La France salue l'opportunité qui lui est offerte de répondre à la **résolution 73/27** de l'Assemblée générale des Nations Unies intitulée « Progrès de l'informatique et des télécommunications et sécurité internationale » et à la **résolution 73/266** relative à « Favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale ».

1. Appréciation générale des problématiques de cybersécurité

A titre préliminaire, la France souhaite rappeler qu'elle n'emploie pas le terme de « sécurité de l'information » auquel elle préfère le terme de « sécurité des systèmes d'information » ou encore « cybersécurité ». En effet, active dans la promotion de la liberté d'expression en ligne (Résolution A/HRC/38/L.10/Rev.1 du Conseil des droits de l'Homme de 2018), **la France n'estime pas que l'information en tant que telle puisse être un facteur de vulnérabilité** contre lequel il est nécessaire de se protéger, sans préjudice des mesures susceptibles d'être prises de manière proportionnée, transparente et dans les conditions strictement établies par la loi conformément à l'article 19 du Pacte relatif aux droits civils et politiques.

Le terme de « cybersécurité » est ainsi plus précis, en ce qu'il désigne la capacité d'un système d'information de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.

La France considère que l'espace numérique doit rester un espace de liberté, d'échange et de croissance qui conditionne la prospérité et le progrès dans nos sociétés. Comme elle le soulignait déjà dans sa « Stratégie nationale pour la sécurité du numérique[1] » en 2015, la France estime que *« porteur de nouveaux usages et de nouveaux services, le numérique est facteur d'innovation. Il engendre une mutation de la plupart des métiers. Il transforme des*

[1] https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf

secteurs d'activités et des entreprises pour leur apporter plus de souplesses et de compétitivité ». Il offre des opportunités pour les sociétés par l'amélioration de leur quotidien à travers les services en ligne de communication, de commerce, d'information mais aussi économique grâce à l'accentuation de la concurrence ou l'économie collaborative.

Ce cyberespace ouvert, sûr, stable, accessible et pacifique, porteur d'opportunités économiques, politiques, sociales, promu par la France au cours des trois dernières décennies est aujourd'hui menacé par de nouvelles pratiques destructrices qui se développent dans le cyberespace. En effet, les spécificités de l'espace numérique (relatif anonymat, faiblesse des coûts et facilité d'accès aux outils malveillants, mise en œuvre aisée, prolifération des vulnérabilités, etc.) permettent à nombre d'acteurs de développer un arsenal numérique utilisé à des fins **d'espionnage**, de **trafics illicites**, de **déstabilisation** et de **sabotage**. Si certaines menaces de bas niveau ne relèvent pas de la sécurité nationale mais d'une forme de criminalité, l'utilisation de ces **armes cyber** visant des systèmes informatiques d'Etat, des infrastructures critiques ou des grandes entreprises peuvent avoir de graves conséquences.

Les enjeux de cybersécurité font désormais partie intégrante des stratégies de puissance et des rapports de force qui régissent les relations internationales ; il s'agit là d'une priorité et d'un enjeu politique de premier ordre. Comme le souligne, la **Revue stratégique de défense et de sécurité nationale**[2] de 2017, *« la numérisation massive que connaissent nos sociétés depuis une dizaine d'années et l'interconnexion globale des systèmes d'information et de communication suscitent l'émergence de nouvelles menaces comme de nouvelles opportunités. Elles mettent à portée de tous de puissants outils d'expression, d'influence, de propagande et de renseignement, d'immenses volumes de données mais aussi de redoutables vecteurs d'attaque. Elles favorisent la montée en puissance de nouveaux acteurs privés, qui s'imposent sur la scène internationale comme un défi à la souveraineté des Etats mais aussi comme des partenaires parfois essentiels. Elles transforment de fait les rapports de pouvoir entre acteurs étatiques, non étatiques et le secteur privé. ».*

Afin de préserver, développer et promouvoir un cyberespace ouvert, sûr, stable, accessible et pacifique, nous avons tous une part de responsabilité. Face à des menaces communes qui affectent la stabilité et la sécurité internationale, la France mène depuis plusieurs années une politique et une diplomatie active en vue de renforcer la sécurité, la confiance et la stabilité dans le cyberespace.

2. <u>Efforts entrepris pour renforcer la cybersécurité au niveau national et promouvoir la coopération internationale dans ce domaine.</u>

a. Renforcement du dispositif de cybersécurité français

[2] https://www.defense.gouv.fr/dgris/presentation/evenements-archives/revue-strategique-de-defense-et-de-securite-nationale-2017

Les orientations stratégiques prises ces dernières années au plus haut niveau de l'Etat français continuent à consacrer la cybersécurité comme l'une des priorités de l'action gouvernementale.

La France poursuit la montée en puissance et l'approfondissement de la maturité de son dispositif national. Dans la continuité des mesures prises depuis une dizaine d'années (création et montée en puissance de l'Agence nationale de sécurité des systèmes d'information (ANSSI) depuis 2009, élaboration de la première stratégie française de défense et de sécurité des systèmes d'information en février 2011, renforcement des outils juridiques et augmentation substantielle des moyens alloués à la cybersécurité par les dernières lois de programmation militaire, publication en février 2014 du « Pacte Défense Cyber » par le ministère des Armées et développement d'un « Pôle d'excellence Cyber » visant à stimuler le développement de la formation, de la recherche académique et de la base industrielle et technologique en cybersécurité), elle mène également une politique de **transparence** sur sa stratégie tant nationale qu'internationale.

En effet, la France s'est dotée dès 2015 d'une « Stratégie nationale pour la sécurité du numérique[3] » destinée à accompagner la transition numérique de la société française. En matière de sécurité, elle met en avant l'apport d'une réponse forte contre les actes de cybermalveillance et vise à faire de la sécurité numérique un avantage concurrentiel pour les entreprises françaises.

En décembre 2017, la « Stratégie internationale de la France pour le numérique[4] » est venue compléter ce document en précisant les principes et les objectifs poursuivis par la France en matière de numérique au niveau international. Articulée autour de trois grands axes (gouvernance, économie, sécurité), cette stratégie vise à :

- promouvoir un monde numérique ouvert, diversifié et de confiance à l'échelle globale ;
- affirmer un modèle européen d'équilibre entre croissance économique, droits et libertés fondamentaux, et sécurité ;
- renforcer l'influence, l'attractivité, la sécurité et les positions commerciales de la France et des acteurs français dans le monde numérique.

La « Revue stratégique de cyberdéfense[5] » présentée en février 2018 définit une doctrine de gestion de crise cyber et clarifie les objectifs stratégiques nationaux de cyberdéfense. Confirmant la pertinence du modèle français et la responsabilité première de l'Etat en matière de cybersécurité, elle s'articule autour de sept grands principes :

- l'amélioration de la protection des systèmes d'information de notre pays ;
- le découragement des attaques par un ensemble de mesures de nature défensive, de résilience renforcée ainsi que de capacités de réaction et de réponse ;
- l'affirmation et l'exercice d'une souveraineté numérique française ;
- une réponse pénale à la cybercriminalité plus efficace ;

[3] https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf
[4] https://www.diplomatie.gouv.fr/IMG/pdf/strategie_numerique_a4_02_interactif_cle445a6a.pdf
[5] http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf

- la promotion d'une culture partagée de la sécurité informatique ;
- la participation au développement d'une Europe numérique sûre et inspirant la confiance ;
- une action internationale en faveur d'une gouvernance collective et maîtrisée du cyberespace.

La loi de programmation militaire 2019-2025[6] prévoit, dans la continuité des précédentes, une augmentation significative des moyens alloués à la cyberdéfense, en particulier dans le domaine des effectifs avec un objectif de recrutement de 1500 personnes supplémentaires, visant à porter à 4000 le nombre de personnels affectés à ces enjeux au sein du Ministère des Armées à l'horizon 2025.

Les acteurs suivants contribuent à l'efficacité du dispositif technique et opérationnel français :

- **L'Agence nationale de sécurité des systèmes d'information** (ANSSI) est chargée de la prévention (y compris en matière normative) et de la réaction aux incidents informatiques visant l'Etat et les opérateurs d'importance vitale. Elle emploie aujourd'hui 600 personnes et continue de croître. Elle s'est imposée comme référent pour la définition des normes de cybersécurité pertinentes.

- Le **ministère des Armées** a la double mission d'assurer la protection des réseaux qui garantissent son action et d'intégrer les opérations dans le cyberespace au cœur de l'action militaire. Afin de consolider l'action du ministère dans ce domaine, un officier général **commandant de la cyberdéfense** (COMCYBER), placé sous les ordres du chef d'État-major des Armées, a été nommé en septembre 2017. À ce titre, le ministère des Armées a publié, début 2019, une politique de lutte informatique défensive ; en même temps qu'une première expression publique de doctrine de lutte informatique offensive des opérations militaires était présentée par le chef d'état-major des armées.

- Le **ministère de l'Intérieur** et le **ministère de la Justice** ont 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.

b. Promotion de la coopération internationale pour la stabilité et la sécurité du cyberespace

Le renforcement de la stabilité stratégique et de la sécurité internationale dans le cyberespace est l'un des objectifs prioritaires de la France. Selon la Revue stratégique de cyberdéfense, *« la coopération de la communauté internationale dans le cyberespace est un*

[6] https://www.legifrance.gouv.fr/eli/loi/2018/7/13/ARMX1800503L/jo/texte

moyen efficace d'en renforcer la stabilité par une connaissance mutuelle, voire une confiance, approfondie entre les acteurs et par l'établissement de mécanismes de gestion commune des crises, de communication et de désescalade. ». L'action de la France en matière de promotion de la coopération internationale sur les enjeux de cybersécurité se décline dans un cadre européen et international.

- *Prévenir les crises par le renforcement des coopérations et le développement des capacités*

La France considère que le premier objectif poursuivi par son action dans l'espace numérique est la prévention des crises. Ainsi, comme le souligne la Revue stratégique de cyberdéfense, *« le renforcement de la protection, de la résilience et de la coopération de l'ensemble des acteurs du cyberespace participe de manière directe au renforcement de notre sécurité nationale »*. Atteindre cet objectif passe par le renforcement de la coopération technique, opérationnelle et structurelle avec les partenaires étatiques et avec les organisations internationales en vue de développer les capacités respectives de ces différents acteurs et la résilience globale du cyberespace.

En effet, en raison de la grande interconnexion des réseaux et sociétés, la France estime que la cybersécurité de tous ne sera assurée que lorsque chaque Etat se sera doté de capacités suffisantes pour sécuriser ses propres systèmes d'information. Dès lors, elle s'investit pour renforcer les capacités de cybersécurité de ses partenaires, à titre bilatéral ou dans le cadre d'initiatives multilatérales. Un tel investissement dans la coopération est, du reste, bénéfique pour toutes les parties : il permet notre maintien à l'état de l'art en se confrontant à nos pairs et en apprenant d'eux, un enrichissement mutuel des savoir et savoir-faire et le développement de la confiance entre les acteurs concernés.

Sur le plan technique, l'ANSSI poursuit l'établissement de partenariat avec ses homologues de nombreux pays afin de favoriser le partage des données essentielles, comme, par exemple, les informations concernant les vulnérabilités ou les failles des produits et services. Par ailleurs le CERT-FR (Computer Emergency Response Team – France) au sein de l'ANSSI est actif dans **plusieurs réseaux multilatéraux** (FIRST, TF-CSIRT, EGC, CSIRT Network de l'Union européenne) grâce auxquels il entretient des contacts avec des CERTs du monde entier.

En matière de coopération opérationnelle et structurelle, la France mène une politique volontariste. Au cours des dernières années, la France a déployé au sein des forces de sécurité intérieure de pays partenaires des experts techniques internationaux en cybersécurité. La France poursuit également avec le Sénégal le lancement des activités de l'école nationale à vocation régionale de cybersécurité de Dakar inaugurée fin 2018. Ce projet vise à fournir des formations courtes et adaptables pour des professionnels de la cybersécurité et des hauts fonctionnaires issus de l'Afrique de l'Ouest en priorité.

Au niveau de l'Union européenne, dans le but de renforcer la cyber-résilience de l'espace européen, la France contribue au développement d'un cadre volontaire de coopération pour la prévention et la résolution des incidents. Il repose en particulier sur le développement de standards opérationnels communs et de procédures de coopération entre partenaires, qui sont testés lors d'exercices paneuropéens. La France a également participé à l'élaboration d'une « **boîte à outil cyber** » offrant un cadre européen de réponse diplomatique conjointe à une attaque informatique, *via* l'utilisation de mesures de prévention, de coopération et de stabilisation.

La France s'est investie également pour l'adoption d'une réglementation européenne prenant en compte les exigences de compétitivité et les potentialités du numérique tout en restant protectrice des citoyens, des entreprises, des États membres (droit à la vie privée et protection des données à caractère personnel, protection des infrastructures critiques, lutte contre les contenus terroristes en ligne). Cela s'est illustré par les adoptions du **règlement général sur la protection des données** n°2016/679 (RGPD), de la **directive sur la sécurité des réseaux et des systèmes d'information** n°2016/1148 (directive NIS) en 2016 ainsi que par la prochaine entrée en vigueur du règlement relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et par la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité). La France soutient également activement l'adoption d'un règlement européen visant à empêcher la diffusion de contenus terroristes en ligne et à imposer des obligations uniformes aux opérateurs de l'Internet. Enfin, la France œuvre pour que **la politique industrielle de l'Union européenne** soutienne les capacités de recherche et de développement de pointe afin de favoriser le déploiement de technologie et de service numérique de sécurité fiable et évalué.

Au sein de l'OTAN, la France a été à l'initiative dans l'adoption par les Alliés d'un Engagement pour la cyberdéfense, le « **Cyberdefence Pledge** », lors du Sommet de Varsovie en juin 2016. Cet engagement permet de s'assurer que chaque Etat membre de l'Alliance consacre une part appropriée de ses ressources au renforcement de ses capacités de cyberdéfense, permettant ainsi d'élever le niveau de sécurité général de tous. En mai 2018, la France a accueilli la toute première conférence dédiée au Cyberdefence Pledge. Les Alliés ont par ailleurs 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.

- *Prévenir les crises par le développement de normes régulant le comportement des acteurs dans le cyberespace*

La France considère que l'émergence d'un cadre de cybersécurité collective, ne pourra reposer que sur les équilibres définis par le droit international. La « Stratégie internationale de la France pour le numérique » souligne en outre l'importance pour la France de poursuivre « *un dialogue coopératif avec l'ensemble des acteurs privés et publics concernés, et l'ensemble des partenaires internationaux qui y sont prêts, sur le plan bilatéral comme multilatéral* ».

La France a pris une part active aux négociations au sein de l'ONU conduites dans le cadre des cinq derniers groupes d'experts gouvernementaux sur la cybersécurité**. Elle poursuivra son engagement dans la reprise des discussions** aussi bien dans le groupe d'experts gouvernementaux que dans le groupe de travail à composition non limitée pour y porter sa vision d'un espace numérique de liberté, d'échange et de croissance qui conditionne la prospérité et le progrès dans nos sociétés. Elle est également engagée dans d'autres enceintes internationales où sont abordées ces questions de sécurité de l'espace numérique.

La France a ratifié la **Convention de Budapest en 2006** qui offre une base juridique pour établir les différentes infractions en matière de lutte contre la cybercriminalité et prévoit des moyens flexibles et modernes de coopération internationale dans ce domaine (ex : mise en place d'un réseau 24/7 pour accélérer les procédures d'assistance entre Etats parties). La France plaide aujourd'hui pour une **universalisation de la Convention de** Budapest qui compte aujourd'hui **63 Etats parties représentant tous les continents**. Elle **participe activement à la négociation de son deuxième protocole additionnel** qui vise à renforcer encore davantage la coopération internationale dans ce domaine, en développant la coopération policière et l'entraide pénale, notamment en matière d'accès à la preuve électronique. La France soutient par ailleurs les **travaux du groupe intergouvernemental à composition non limitée** (IEG), chargé de réaliser une étude approfondie sur le problème de la cybercriminalité qui confirment le rôle central de l'ONUDC dans ce domaine.

Présenté par le président de la République, à l'UNESCO, à l'occasion du forum sur la gouvernance de l'internet, le 12 novembre 2018, « **l'Appel de Paris pour la confiance et la sécurité dans le cyberespace**[7] » témoigne du rôle actif joué par la France dans la promotion d'un cyberespace sûr, stable et ouvert. Soutenu à ce jour par 66 pays et près de 500 entités non-étatiques, ce texte vise à promouvoir certains principes fondamentaux de la régulation de l'espace numérique comme l'application du droit international et des droits de l'Homme dans le cyberespace, le comportement responsable des Etats, le monopole étatique de la violence légitime, la reconnaissance des responsabilités spécifiques des acteurs privés, etc.

La France s'est investie également au sein de **l'Organisation de coopération et de développement économiques.** Elle a œuvré à l'organisation d'une première réunion du « Forum mondial de l'OCDE sur la sécurité numérique pour la prospérité économique et sociale » en décembre 2018, sur le thème de **la responsabilité des acteurs privés** dans la sécurité du numérique.

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, dite « **déclaration de Lucca** », concernant les normes de comportement responsable des États dans le cyberespace. En mars 2019, dans le cadre de sa présidence, la France a proposé le lancement d'un **mécanisme de suivi de la mise**

[7] https://www.diplomatie.gouv.fr/IMG/pdf/texte_appel_de_paris_-_fr_cle0d3c69.pdf

en œuvre des normes et recommandations agréées au niveau de l'ONU, acté par la « Déclaration de Dinard sur l'initiative pour les normes cyber[8] ».

Au sein du G20, la France œuvre pour que les travaux du G20 portent sur les questions fondamentales de la concurrence dans l'économie numérique, des nouveaux modes de régulation et de gouvernance comme de la sécurité numérique dans la lignée de « l'Appel de Paris ».

Participant activement au groupe de travail informel de **l'Organisation pour la sécurité et la coopération en Europe** sur la cybersécurité, la France continue de promouvoir l'opérationnalisation des 16 mesures de confiance développées par l'OSCE sur les enjeux cyber. Elle y pilote notamment la mise en œuvre d'une mesure de confiance sur la protection des infrastructures critiques (CBM 15).

En vue de renforcer la lutte contre la prolifération d'outils et techniques malveillants, la France a soutenu l'inscription des logiciels d'intrusion sur la liste des biens à double usage de l'Arrangement de Wassenaar. La France estime que l'effort de régulation doit être poursuivi dans ce sens en inscrivant certains outils cyber, déterminés en fonction de la gravité de leurs effets, sur la liste des matériels de guerre.

La France considère que de nombreux enjeux liés à la cybersécurité méritent d'être abordés selon une approche multi-acteurs ou multi-parties-prenantes, afin de prendre en compte le rôle et les responsabilités spécifiques d'acteurs non-étatiques. Dans cette logique, la France a soutenu les activités de la **Global Commission on the Stability of Cyberspace** (GCSC). Cette commission vise élaborer des propositions de normes et de politiques destinées à renforcer la sécurité et la stabilité internationales et à orienter le comportement responsable des États dans le cyberespace.

3. Concept internationaux pertinents visant à renforcer la cybersécurité globale

a. Concepts permettant la préservation de la paix et de la sécurité internationale

Afin de garantir un cyberespace ouvert, sûr, stable, accessible et pacifique, la France réaffirme son attachement à l'applicabilité du droit international, dont la Charte des Nations Unies dans son intégralité, le droit international humanitaire, et le droit international de droits de l'Homme, à l'usage des technologies de l'information et de la communication (TIC) par les États.

- *Droit international public*

Ainsi que le groupe des experts gouvernementaux de l'ONU (GGE) a pu le conclure dans son rapport publié en 2013, les principes et règles de droit international s'appliquent aux comportements des Etats dans le cyberespace. Si le cyberespace présente

[8] https://www.diplomatie.gouv.fr/IMG/pdf/g7_-_declaration_de_dinard_sur_l_initative_pour_des_normes_dans_le_cyberespace_cle8a8313.pdf

des spécificités propres (anonymat, rôle des acteurs privés), le droit international offre toutefois les moyens nécessaires pour encadrer de manière responsable le comportement des Etats dans cet environnement. A cet égard, le défaut d'attribution ne saurait constituer un obstacle définitif à l'application du droit international existant.

Le principe de souveraineté s'applique au cyberespace. A 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 les limites de ses obligations découlant du droit international. La pénétration non-autorisée de systèmes français ou la production d'effets sur le territoire français *via* des moyens cyber par une entité étatique, ou des acteurs non-étatiques agissant sous les instructions ou le contrôle d'un Etat, est susceptible de constituer une violation de souveraineté.

Le champ des mesures que les Etats peuvent adopter pour réagir à une attaque informatique dont ils seraient victimes est fonction de la gravité de celle-ci. Plus la cyberattaque sera grave, plus le champ des mesures sera large. Une opération cyber peut être considérée comme un recours à la force prohibé au titre de l'article 2.4 de la Charte des Nations unies. Le franchissement du seuil de l'emploi de la force n'est pas fonction du moyen cyber employé, mais des effets de la cyber-opération. Si ces derniers sont similaires à ceux qui résultent d'armes classiques, l'opération cyber peut constituer un recours à la force. La France considère qu'une attaque informatique majeure, perpétrée par un Etat ou des acteurs non-étatiques agissant sous le contrôle ou les instructions d'un Etat, si elle atteignait par son ampleur ou ses effets un seuil de gravité suffisant (exemples : pertes humaines substantielles, dommages physiques considérables, déficience des infrastructures critiques avec des conséquences significatives) et était attribuable à un Etat, pourrait constituer une « agression armée », au sens de l'article 51 de la Charte des Nations Unies, et justifier ainsi l'invocation de la légitime défense. Cette légitime défense peut être mise en œuvre par des moyens conventionnels ou cybernétiques pour peu que soient respectés les principes de nécessité et de proportionnalité. La caractérisation d'une attaque informatique en tant qu'« agression armée », au sens de l'article 51 de la Charte des Nations Unies, relève d'une décision politique au cas par cas à la lumière des critères établis par le droit international.

La France estime que la création d'un nouvel instrument international juridiquement contraignant spécifique aux enjeux de cybersécurité n'est pas nécessaire, à ce stade. Dans le cyberespace, comme dans les autres domaines, le droit international existant s'applique et doit être respecté.

- *Droit international humanitaire*

La France soutient l'applicabilité du droit international humanitaire aux cyberopérations qui sont conduites dans le cadre de conflits armés et en lien avec ceux-ci.

A l'heure actuelle, les opérations de lutte informatique offensive sont concourantes aux opérations militaires conventionnelles. L'hypothèse d'un conflit armé constitué exclusivement d'activités numériques ne peut être exclue par principe, mais repose sur la capacité des

opérations cyber à atteindre le seuil de violence requis pour qualifier l'existence d'un conflit armé international ou non-international.

Malgré leur caractère dématérialisé, ces opérations restent soumises au champ d'application géographique du DIH, c'est-à-dire que leurs effets sont limités au territoire des Etats parties en conflit armé international ou sur le territoire sur lequel se déroulent les hostilités dans le cadre d'un conflit armé non-international.

Les opérations de lutte informatique offensive mises en œuvre par les forces armées françaises sont soumises au respect des principes du DIH dont :

- le **principe de distinction** entre biens civils et objectifs militaires. A ce titre, les attaques cyber qui ne sont pas dirigées contre un objectif militaire déterminé ou qui sont mises en œuvre par des armes cyber qui ne peuvent pas être dirigées contre un objectif militaire déterminé sont prohibées. A cet égard certaines données de contenu, bien que de nature intangibles, peuvent constituer des biens civils protégés au titre du DIH ;

- le **principe d'humanité**. Elles ne doivent pas non plus viser la population civile en tant que telle ni les personnes civiles, sauf si celles-ci participent directement aux hostilités et durant le temps de cette participation. En contexte de conflit armé, tout cyber combattant membre des forces armées, tout membre d'un groupe armé organisé commettant des cyber attaques au détriment d'une partie adverse, ou tout civil participant directement aux hostilités *via* des moyens cyber peuvent faire l'objet d'une attaque par des moyens conventionnels ou cyber ;

- le **principe de proportionnalité**. Elles doivent être conduites en veillant constamment à protéger les personnes et les biens civils des effets des hostilités. Les dommages collatéraux ne sauraient excéder l'avantage militaire direct et concret attendu. Le respect du principe de proportionnalité dans le cyberespace exige de prendre en compte l'ensemble des effets prévisibles de l'arme, que ces derniers soient directs (dommages sur le système visé, interruption du service etc.), mais également indirects (effets sur l'infrastructure contrôlé par le système attaqué, mais également sur les personnes affectés par le dysfonctionnement ou la destruction des systèmes, ou par l'altération et la corruption de données de contenu) pour peu que ceux-ci entretiennent un lien de causalité suffisant avec l'attaque. Ce principe prohibe également le recours à des armes cyber qui ne peuvent être contrôlés (notamment dans le temps et dans l'espace), autrement dit susceptibles de provoquer des dommages irréversibles sur des infrastructures, des systèmes ou des données de contenu civiles.

Ces éléments sont notamment rappelés dans les éléments publics de doctrine militaire française de lutte informatique offensive présentés début 2019.

- *Droits de l'Homme*

La France soutient que les droits dont les personnes jouissent hors ligne doivent également être protégés en ligne et que le droit international des droits de l'Homme s'applique au cyberespace. Ces valeurs sont notamment mises à mal par la propagation en ligne de contenus illégaux (terroristes, haineux, antisémites). La France considère qu'il est

particulièrement nécessaire d'impliquer les acteurs privés du numérique dans la lutte contre les contenus illicites et de clarifier leur rôle et responsabilités au niveau international pour lutter contre ces contenus illicites et garantir la protection des droits de l'Homme et des libertés fondamentales en ligne.

- *Principe de due diligence*

La France considère comme essentiel de parvenir à une compréhension partagée, au niveau international, sur les obligations qui pèsent sur un Etat dont les infrastructures seraient utilisées à des fins malveillantes, contre les intérêts d'un autre Etat. L'objectif est de clarifier l'application, dans le domaine cyber, du **principe de due diligence** qui prévoit que tout Etat a l'obligation « de ne pas laisser utiliser son territoire aux fins d'actes contraires aux droits d'autres Etats »[9]. A ce titre, les Etats ne doivent pas permettre sciemment que leur territoire soit utilisé pour commettre des faits internationalement illicites à l'aide de moyens cybernétiques et ne pas utiliser d'intermédiaire non-étatique (proxys) pour commettre des violations du droit international. Une meilleure compréhension de l'application de ce principe aux enjeux cyber permettrait de renforcer la coopération entre les Etats en vue de protéger certaines infrastructures critiques mais aussi pour faire cesser des cyberattaques majeures qui transiteraient *via* un Etats tiers.

b. Concept permettant de renforcer la coopération et la confiance entre les Etats

- *Normes de comportement*

Les différents cycles de négociation conduits dans le cadre du GGE de l'ONU sur la cybersécurité ont permis des avancées sensibles en matière de régulation internationale du cyberespace. Le rapport de 2015 identifie notamment 11 normes de comportement responsable des Etats dans le cyberespace. La France considère que chaque Etat est tenu de respecter ces normes et de développer des mécanismes permettant de les mettre en œuvre. D'autres normes, applicables au comportement des Etats ou à celui d'autres acteurs dans le cyberespace, pourraient également être développées à l'avenir.

- *Mesures de confiance*

Les travaux menés dans diverses enceintes et organisations régionales en vue de développer des mesures de confiance spécifiques aux enjeux de cybersécurité doivent être approfondis. La France continuera à encourager ses partenaires à se doter de procédures interministérielles qui puissent être mobilisées afin d'assurer la bonne communication entre Etats en temps de crise. Le développement de tels procédures et mécanismes, reposant sur la transparence et la communication, s'avère indispensable à la prévention des conflits dans le cyberespace.

- *Développement capacitaire*

[9] *Affaire du Détroit de Corfou*, Arrêt du 9 avril 1949 : C.I.J., Recueil 1949, p. 4

La France soutient l'objectif de renforcement international des capacités en matière de cybersécurité. De tels efforts participent de façon très directe au renforcement de la sécurité de tous et de la stabilité du cyberespace. La France entend prendre toute sa part à ces efforts, *via* des actions de renforcement des capacités menées au niveau bilatéral, régional ou multilatéral.

c. Rôle et responsabilité des acteurs non-étatiques

- *Approche multi partie prenante*

Avec l'Appel de Paris, la France a souligné « la nécessité d'une approche multi-acteurs renforcée ». La France considère en effet que la société civile, le monde académique, le secteur privé et la communauté technique disposent de compétences et de ressources utiles à la définition de certains aspects des politiques pertinentes en matière de cybersécurité.

- *Responsabilité de sécurité des acteurs privés dans la conception et la maintenance des produits numériques*

L'essor du numérique comme nouvel outil et espace de confrontation confère au secteur privé, notamment à un certain nombre d'acteurs systémiques, un rôle critique et une responsabilité inédite dans la préservation de la paix et de la sécurité internationale. L'Appel de Paris reconnait ainsi « les responsabilités des principaux acteurs du secteur privé pour développer la confiance, la sécurité et la stabilité dans le cyberespace » et encourage « les initiatives qui visent à accroître la sécurité des processus, produits et services numériques. ».

La France considère pertinent de poser au niveau international un principe de responsabilité de sécurité des acteurs privés systémiques dans la conception, l'intégration, le déploiement et la maintenance de leurs produits, processus et services numériques, tout au long de leur cycle de vie et d'un bout à l'autre de la chaine d'approvisionnement.

- *Responsabilité des plateformes numériques en matière de lutte contre le terrorisme*

La France œuvre également en faveur d'une responsabilisation des acteurs privés du numérique en matière de lutte contre l'utilisation abusive de leurs services à des fins terroristes. Elle porte notamment cette thématique au sein du **G7** et de **l'UE**, où elle soutient activement l'adoption d'un **projet de règlement européen** permettant d'encadrer l'action des opérateurs de l'internet en matière de lutte contre les contenus terroristes en ligne. Ce texte impose le retrait d'un contenu terroriste dans l'heure à la demande d'un Etat membre, l'adoption de mesures proactives pour les plateformes exposées aux contenus terroristes, l'obligation de désigner un point de contact disponible 24h/24 pour traiter les signalements et les demandes de retrait, et des sanctions en cas de non-coopération systématique.

- *Prévention des activités offensives des acteurs privés*

La France estime que les Etats doivent conserver le monopole de la violence physique légitime, dans le cyberespace comme dans les autres domaines. Elle soutient en ce sens l'interdiction faite aux acteurs non-étatiques, y compris au secteur privé, de conduire des activités offensives dans le cyberespace pour eux-mêmes et pour le compte d'autres acteurs non-étatiques. Ces pratiques, basées sur le principe d'une légitime défense privée (*hack-back*), sont potentiellement déstabilisatrices par leurs conséquences défavorables sur une tierce partie et pourraient alimenter une possible escalade entre Etats. A ce titre, la France considère qu'il est nécessaire de réussir à clarifier la marge de manœuvre dont disposent les acteurs privés en matière de réponse à incident.

4. Mesures qui pourraient être prises par la communauté internationale pour renforcer la cybersécurité au niveau global

Face aux nouvelles menaces issues de la révolution numérique, la France estime que la coopération et le droit sont nécessaires pour que le cyberespace ne devienne pas une zone de conflit et permanente. A l'instar des autres domaines, les Etats sont tenus de respecter le droit international dans l'espace numérique. En outre, un corpus normatif encadrant le comportement responsable des Etats dans le cyberespace a émergé ces dernières années, qu'il convient encore de consolider. La France estime que les mesures suivantes pourraient être prises pour renforcer la cybersécurité au niveau international :

- **Approfondir le travail des précédents GGE** : sans remettre en cause les normes et recommandations ayant fait l'objet de consensus lors des cycles de négociation précédents, il pourrait être utile de préciser la façon dont ces normes et recommandations peuvent être mises en œuvre et de développer une meilleure compréhension, au niveau international, des bonnes pratiques en la matière ;

- **S'appuyer sur l' « Appel de Paris pour la confiance et la sécurité dans le cyberespace » lors des discussions à venir sur les enjeux de cybersécurité à l'ONU** : cette déclaration rassemble en effet à ce jour plus du tiers des Etats membres des Nations Unies, et plusieurs centaines d'acteurs non-étatiques de premier ordre, sur une vision commune des principes devant sous-tendre les comportements des différents acteurs dans le cyberespace ;

- **Universaliser la convention de Budapest de lutte contre la cybercriminalité** : adoptée en novembre 2001 pour renforcer la coopération internationale en matière, cet instrument est aujourd'hui ratifié par 63 Etats et a influencé les législations nationales de plus des deux tiers des Etats membres des Nations Unies ;

- **Encourager les Etats à faire preuve de transparence** : notamment en ce qui concerne leur stratégie de cybersécurité, leur doctrine de gestion des crises cyber et de

réponse à une attaque informatique et de leur interprétation de l'application du droit international au cyberespace ;

- **Opérationnaliser dans les cadres régionaux ou internationaux pertinents les mesures de confiance spécifiques aux enjeux cyber qui ont pu y être développées** ;

- **Renforcer les initiatives et mécanismes permettant l'échange de bonnes pratiques et le renforcement des capacités** : de tels mécanismes devraient viser à doter tous les Etats d'un dispositif performant de cybersécurité, passant notamment par la :

    - mise en place d'une stratégie de cybersécurité ;
    - définition d'un cadre législatif pour promouvoir la cybersécurité et la lutte contre la cybercriminalité ;
    - création d'un CERT ;
    - mise en place de procédures pour coopérer avec le secteur privé notamment les grandes entreprises du numérique ;
    - définition d'un cadre de protection des infrastructures critiques dans le cyberespace.

- **Reconnaitre au niveau international un principe de responsabilité de sécurité des acteurs privés systémiques** dans la conception, l'intégration, le déploiement et la maintenance de leurs produits, processus et services numériques, tout au long de leur cycle de vie et d'un bout à l'autre de la chaine d'approvisionnement./.