DROIT INTERNATIONAL APPLIQUÉ AUX OPÉRATIONS DANS LE CYBERESPACE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES ARMÉES

SOMMAIRE

INTRODUCTION

Un renforcement des menaces dans le cyberespace

Le 12 novembre 2018, à l'initiative de la France, plusieurs centaines d'États, d'entreprises, d'acteurs du secteur privé et de représentants de la société civile ont réaffirmé dans l'Appel de Paris pour la confiance et la sécurité dans le cyberespace leur soutien à un cyberespace ouvert, sûr, stable, accessible et pacifique, ainsi que l'applicabilité du droit international, dont la Charte des Nations unies dans son intégralité, le droit international humanitaire (DIH) et le droit international coutumier, à l'usage des technologies de l'information et de la communication (TIC) par les États.

Cette initiative, en faveur d'une plus grande coopération internationale entre tous les acteurs opérant dans l'espace numérique, s'inscrit en réponse à une décennie d'attaques informatiques toujours plus sophistiquées qui menacent nos sociétés.

L'absence de règles communes clairement établies et appliquées laisse, en effet, libre cours à une compétition entre les acteurs étatiques ou non-étatiques d'autant plus âpre que l'accès et la maîtrise de cet espace revêtent un caractère stratégique. Dans le même temps, la difficulté à contrôler la propagation des attaques, leurs vecteurs et leurs conséquences fait courir des risques systémiques majeurs.

Le dérèglement et la crise qui en résulte contribuent à faire de l'espace numérique un champ de confrontation à part entière comme le souligne la Revue stratégique de défense et de sécurité nationale publiée en octobre 2017, et participent de l'imprévisibilité et de l'instabilité de l'environnement stratégique actuel. Illustrant ce constat, les cyberattaques visant les systèmes d'information du gouvernement et des administrations, les secteurs d'activités d'importance vitale et les industries de défense sont plus nombreuses, plus agressives et plus techniques.

Cette situation précaire est rendue plus critique encore par les postures de certains acteurs étatiques et non-étatiques qui, privilégiant ouvertement les rapports de force, conduisent à une remise en cause du cadre de la régulation du recours à la force établie depuis la fin de la Seconde Guerre mondiale. Aujourd'hui, les violations de principes internationaux auxquels les États adhèrent de longue date se multiplient.

Le respect du droit international est, pour la France, une condition à l'émergence d'une régulation adaptée du cyberespace

Face à une menace d'origine numérique toujours plus présente et durable, et des systèmes rendus plus vulnérables par la numérisation et leur inter-connectivité croissante, la régulation du cyberespace entre États et acteurs privés et publics doit devenir une priorité pour refonder un ordre collectif et multilatéral en vue de préserver la paix et la sécurité internationales.

Dans le prolongement des conclusions de la Revue stratégique de cyberdéfense publiée en février 2018, des propositions françaises lors du dernier cycle de négociations du Groupe des experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale (GGE), ainsi que de l'Appel de Paris, ce document a vocation à préciser la position française concernant l'application du droit international aux opérations cyber [1] afin, notamment, de réduire les risques d'incompréhension ou d'escalade non maîtrisée, et de contribuer à une lecture du corpus juridique cohérente avec la recherche d'un cyberespace pacifique et sûr[2]. Une telle démarche doit, par ailleurs, être de nature à faciliter le développement des coopérations internationales futures.

Dans cette perspective, l'interprétation que la France fait du droit international applicable aux actions menées dans le cyberespace s'inscrit, tout d'abord, dans le respect des conclusions issues des négociations du GGE depuis 2004. Si l'échec du dernier cycle de négociations du GGE 2016-2017 acte une divergence fondamentale de perception entre certains États sur l'architecture internationale de sécurité dans le cyberespace, il ne remet pas en cause les normes et les principes agréés les années précédentes par les experts gouvernementaux. Ces négociations, organisées dans des formats différents (quinze experts gouvernementaux, puis vingt en 2014-2015 et vingt-cinq en 2016-2017) à cinq reprises entre 2004 et 2017, ont ainsi permis de reconnaître dès 2013 l'applicabilité du droit international, dont la Charte des Nations unies, au cyberespace[3]. En 2015, le GGE a insisté sur l'importance du droit international, de la Charte des Nations unies et du principe de souveraineté comme fondements d'une meilleure sécurité dans l'utilisation des technologies de l'information et des communications (TIC) par les États. Tout en convenant de la nécessité d'approfondir la question, le GGE a noté que les États avaient le droit de prendre des mesures conformes au droit international et reconnues par la Charte. Il a également rappelé les principes de DIH reconnus, y compris, lorsqu'ils sont applicables, les principes de distinction et de proportionnalité[4].

1 Dans le présent document, les expressions « opérations dans le domaine cyber », « cyber-opérations » et « opérations cyber » sont considérées comme des synonymes. Pour les définitions associées, voir le glossaire en annexe.

2 L'espionnage informatique, qui n'est pas illicite en droit international bien qu'il puisse méconnaitre ce droit lorsqu'il est associé à un fait internationalement illicite, ne fait pas l'objet d'une analyse ou de développements spécifiques dans le présent document.

3 SGDSN, Revue stratégique de cyberdéfense, février 2018, p. 36. « Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale », A/68/98, 24 juin 2013, § 19.

4 « Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale », Note du Secrétaire général, A/70/174, 22 juillet 2015. L'Assemblée générale des Nations Unies demande à tous les États de s'inspirer, pour ce qui touche à l'utilisation de l'informatique et des technologies des communications, du rapport du GGE de 2015 (voir résolution A/RES/70/237 du 23 décembre 2015).

L'élaboration de cette synthèse tient également compte des réflexions actuellement conduites dans ce domaine par des universitaires et des experts indépendants. Parmi ces dernières, le Manuel de Tallinn 2.0[5] représente le travail le plus exhaustif mené dans ce domaine jusqu'à présent. Si son autorité demeure étroitement tributaire de celle reconnue aux experts à l'origine de sa publication, cette initiative est toutefois de nature à stimuler la réflexion internationale sur le droit international applicable aux cyber-opérations.

Espace d'opportunité favorable au progrès, mais aussi de confrontation, le cyberespace offre de larges possibilités d'action aux acteurs qui l'investissent. Si la France entend prévenir, protéger, anticiper détecter, réagir, et se donner les moyens d'attribuer les cyberattaques, elle se réserve également le droit de répondre à celles qui visent ses intérêts[6]. Dans cette perspective, les normes que la France retient et met en œuvre pour appréhender les opérations cyber menées par les autres États ou les acteurs non-étatiques s'inscrivent dans le respect du droit international, aussi bien en temps de paix (I) qu'en situation de conflit armé (II).

5 Michael Schmitt (dir.), The Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013. Michael Schmitt et Liis Vihul (dir.), The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017.

6 Il s'agit, notamment, des opérations qui visent des secteurs d'activité d'importance vitale, des infrastructures critiques, ou encore le secteur militaire.

I. LES CYBER-OPÉRATIONS CONDUITES EN TEMPS DE PAIX CONTRE LA FRANCE

Messages clés

La France exerce sa souveraineté sur les systèmes d'information situés sur son territoire et met en œuvre les moyens nécessaires à la protection de cette souveraineté. En parallèle à un ensemble de mesures de sécurisation et de défense de ses systèmes, elle se réserve le droit de répondre à toute cyberattaque dont elle aurait été victime. Cette identification peut se traduire par une attribution publique décidée en opportunité dans l'exercice de ses prérogatives régaliennes. Il relève de sa souveraineté de décider, ou non, d'une attribution collective en lien avec des partenaires étatiques ou des organisations internationales.

La décision de réponse est politique et réalisée en conformité avec le droit international. Cette réponse peut aller jusqu'à l'utilisation de la force en fonction de la gravité de la cyber attaque[7]. Toute pénétration d'origine étatique non autorisée sur les systèmes français ou toute production d'effets sur le territoire français par un vecteur numérique peut constituer, a minima, une violation de souveraineté. Si celle-ci s'accompagne d'effets constitutifs d'un recours à la force armée au sens de l'article 2 alinéa 4 de la Charte des Nations unies, la France peut adopter des contre-mesures ou saisir le Conseil de Sécurité des Nations unies (CSNU). Par ailleurs, il n'est pas exclu qu'une cyberattaque puisse atteindre le seuil de l'agression armée à laquelle la France peut répondre par la légitime défense en vertu de l'article 51 de la Charte des Nations unies.

La qualification du seuil de violation résulte d'une décision politique formulée au cas par cas à la lumière des critères établis par le droit international. Le Président de la République, chef des armées[8], détermine en dernier ressort la réponse la plus opportune dans le spectre de celles autorisées par le droit international, notamment en fonction de la nature de l'intrusion et de la qualité de l'instigateur.

1.1. La France se réserve le droit de répondre à toute cyberattaque constitutive d'une violation du droit international dont elle serait victime

Dans le prolongement des positions adoptées par le GGE[9], ainsi que les développements sur le sujet au sein de la Revue stratégique de cyberdéfense, **la France réaffirme l'obligation pour les États de respecter le droit international dans le cyberespace**, notamment la Charte des Nations unies, en particulier les principes d'égalité souveraine des États, de règlement des différends internationaux par des moyens pacifiques, ainsi que le fait pour les États de s'abstenir dans leurs relations internationales de recourir à la menace ou à l'emploi de la force contre l'intégrité ou l'indépendance politique de tout État, ou de toute autre manière incompatible avec les buts des Nations unies.

Nombre d'États se dotent de capacités pour préparer et conduire des opérations dans le cyberespace. Lorsqu'elles sont conduites au détriment des droits d'autres États, ces opérations peuvent constituer des violations du droit international. Compte tenu de leur degré d'intrusion ou de leurs effets, elles peuvent porter atteinte aux principes de souveraineté, de non-intervention, voire même d'interdiction de recours à la menace ou à l'emploi de la force[10]. Les États ciblés par de telles cyberattaques ont le droit d'y répondre dans le cadre des possibilités offertes par le droit international. En réponse à une cyberattaque, la France peut envisager des réponses diplomatiques pour certains incidents, des contre-mesures, voire une action de contrainte mise en œuvre par les forces armées pour les atteintes constitutives d'une agression armée.

Au regard du droit international, une cyber-opération n'est pas illicite en soi, mais peut le devenir dès lors qu'elle ou les effets produits entraînent des violations du droit international.

1.1.1. Les cyberattaques peuvent être constitutives d'une violation de souveraineté

Les normes et principes internationaux qui procèdent de la souveraineté étatique s'appliquent à l'utilisation de l'outil informatique par les États, ainsi qu'à leur compétence territoriale en matière d'infrastructure informatique[11].

La France exerce sa souveraineté sur les systèmes d'information situés sur son territoire[12]. Conformément à l'obligation de diligence requise[13], elle veille à ce que son territoire

7 Action volontaire, offensive et malveillante, menée au travers du cyberespace et destinée à provoquer un dommage (en disponibilité, intégrité ou confidentialité) aux informations ou aux systèmes qui les traitent, pouvant ainsi nuire aux activités dont ils sont le support.

8 Article 15 de la Constitution du 4 octobre 1958.

9 « Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale », A/70/174, 22 juillet 2015, §§ 25-26.

10 Article 2 alinéa 4 de la Charte des Nations Unies : « *[L]es Membres de l'Organisation s'abstiennent, dans leurs relations internationales, de recourir à la menace ou à l'emploi de la force, soit contre l'intégrité territoriale ou l'indépendance politique de tout État, soit de toute autre manière incompatible avec les buts des Nations Unies.* »

11 « Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale », A/70/174, 22 juillet 2015, §§ 27-28.

12 Cela comprend les équipements et infrastructures français ou d'intérêts français.

13 Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, rapport de 2015, Note du Secrétaire général, A/70/174, 22 juillet 2015, §13 c).

ne soit pas utilisé pour commettre des faits internationalement illicites à l'aide des TIC. Cette obligation coutumière s'impose aux États qui doivent utiliser le cyberespace dans le respect du droit international, notamment ne pas faire appel à des intermédiaires pour commettre des actes contraires aux droits des autres Etats à l'aide de TIC, et veiller à ce que leur territoire ne soit pas utilisé à de telles fins, notamment par des acteurs non-étatiques.

Toute cyberattaque à l'encontre des systèmes numériques français ou toute production d'effets sur le territoire français via des moyens numériques par un organe étatique, une personne ou une entité exerçant des prérogatives de puissances publiques ou par une personne ou des personnes agissant sur les instructions ou les directives ou sous le contrôle d'un État est constitutive d'une violation de souveraineté.

L'ingérence par le biais d'un vecteur numérique dans les affaires intérieures ou extérieures de la France, c'est-à-dire portant atteinte ou susceptible de porter atteinte au système politique, économique, social et culturel français peut constituer une violation du principe de non-intervention.

Une cyberattaque qui pénètre les systèmes numériques étatiques, qui affecte le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation, ou qui représente une ingérence dans les affaires intérieures ou extérieures de la France, entraînera des opérations de lutte informatique défensive pouvant inclure une neutralisation de l'effet.

Les autorités politiques décident de l'opportunité de répondre à de telles opérations en fonction de la qualité et des caractéristiques de l'intrusion. Cette réponse, choisie parmi le spectre de réponses possibles offertes par le droit international, dépend, sous réserve d'une appréciation en opportunité, du degré de gravité de la violation de souveraineté.

Le principe de souveraineté s'applique au cyberespace. La France exerce sa souveraineté sur les systèmes d'information situés sur son territoire.
L'évaluation de la gravité de cette violation sera soumise à une étude au cas par cas et en cohérence avec la gouvernance de la cyberdéfense française afin de déterminer les réponses possibles dans le respect du droit international.

1.1.2. Certaines cyber-opérations peuvent représenter une violation de l'interdiction de recourir à la menace ou à l'emploi de la force

Les violations les plus graves de souveraineté, notamment celles qui portent atteinte à l'intégrité territoriale ou à l'indépendance politique de la France, peuvent constituer une violation du principe d'interdiction de recours à la menace ou à l'emploi de la force[14], lequel s'applique à tout emploi de la force indépendamment de l'arme employée[15].

Dans l'espace numérique, le franchissement du seuil de l'emploi de la force ne dépend pas du moyen numérique employé, mais des effets de la cyber-opération.

Une cyber-opération conduite par un État à l'encontre d'un autre Etat constitue une viol**ation du principe d'interdiction de recourir à la force si ses effets sont similaires à ceux qui résultent de l'utilisation d'armes classiques**.

Toutefois, la France n'exclut pas la possibilité qu'une cyber-opération dénuée d'effets physiques puisse être également qualifiée de recours à la force. En l'absence de dommages physiques, une cyber-opération peut être considérée comme un recours à la force à l'aune de plusieurs critères, notamment les circonstances qui prévalent au moment de l'opération, tels que l'origine de l'opération et la nature de l'instigateur (son caractère militaire ou non), le degré d'intrusion, les effets provoqués ou recherchés par l'opération, ou encore la nature de la cible visée. Ces critères ne sont, bien entendu, pas exhaustifs. À titre d'exemple, le fait de pénétrer des systèmes militaires en vue d'atteindre les capacités de défense françaises, ou de financer, voire d'entraîner des individus afin que ces derniers perpètrent des cyberattaques contre la France pourrait, ainsi, être qualifié de recours à la force.

Tout recours à la force n'est toutefois pas constitutif d'une agression armée au sens de l'article 51 de la Charte des Nations unies[16], notamment si ses effets sont limités, réversibles ou n'atteignent pas une certaine gravité.

Le principe d'interdiction du recours à la force, consacré par la Charte des Nations unies, s'applique dans le cyberespace. Certaines cyber-opérations peuvent constituer un recours à la force armée au sens de l'article 2 alinéa 4 de la Charte des Nations unies.

1.1.3. Le droit international autorise plusieurs réponses en cas de cyberattaque constitutive d'une violation de la souveraineté française ou d'un recours à la force

Face à des adversaires qui multiplient les cyberattaques, la France engage un certain nombre de moyens pour prévenir, anticiper, protéger, détecter et réagir à ces attaques, y compris en neutralisant leurs effets. À cette fin, les services de l'Etat désignés par le Premier ministre mettent en œuvre des opérations de cyberdéfense dans le but d'anticiper, de détecter et de réagir aux cyberattaques en coordination avec leurs partenaires nationaux ou internationaux.

14 « Les Membres de l'Organisation s'abstiennent, dans leurs relations internationales, de recourir à la menace ou à l'emploi de la force, soit contre l'intégrité territoriale ou l'indépendance politique de tout État, soit de toute autre manière incompatible avec les buts des Nations Unies. » L'interdiction du recours à la force armée ne souffre que trois exceptions : la légitime défense en cas d'agression armée prévue par l'article 51 de la Charte des Nations unies, le recours à la force autorisé par le Conseil de sécurité des Nations unies aux termes du Chapitre VII et le consentement de l'État sur le territoire duquel a lieu l'intervention.

15 Licéité de la menace ou de l'emploi d'armes nucléaires, avis consultatif, C.I.J Recueil 1996, p.18, § 39.

16 « Aucune disposition de la présente Charte ne porte atteinte au droit naturel de légitime défense, individuelle ou collective, dans le cas où un Membre des Nations Unies est l'objet d'une agression armée, jusqu'à ce que le Conseil de sécurité ait pris les mesures nécessaires pour maintenir la paix et la sécurité internationales. »

De manière générale, la France peut réagir aux cyberattaques à travers l'adoption de contre-mesures. En réponse à une cyberattaque constitutive d'une violation du droit international (y compris d'un recours à la force), la France peut adopter des contre-mesures afin de faire respecter et protéger ses intérêts et d'amener l'État responsable à s'acquitter de ses obligations[17].

Conformément au droit international, de telles contre-mesures doivent être mises en œuvre par la France en sa qualité d'État victime. Les contre-mesures collectives ne sont ainsi pas autorisées, ce qui exclut la possibilité pour la France d'adopter de telles mesures en réponse à une atteinte aux droits d'un État tiers.

Ces contre-mesures doivent également être exécutées dans le respect du droit international[18], notamment du principe d'interdiction de recourir à la menace ou à l'emploi de la force[19]. Elles s'inscrivent, par conséquent, dans une réponse de nature pacifique et ont pour unique but la cessation de la violation initiale[20], y compris s'il est question de réagir à une cyber-opération constitutive d'un recours à la force armée au sens de l'article 2 alinéa 4 de la Charte des Nations unies. La réponse à une cyber-opération peut se faire par des moyens numériques ou non, à condition que celle-ci soit proportionnelle au préjudice subi, compte tenu de la gravité de la violation initiale et des droits en cause[21].

La mise en œuvre de contre-mesures exige, enfin, de demander à l'État responsable de la cyberattaque de s'acquitter des obligations qui lui incombent. L'État victime peut, dans certaines circonstances, déroger à l'obligation de notifier préalablement l'État responsable de la cyber-opération, lorsqu'il existe une nécessité à protéger ses droits. Cette possibilité d'adopter des contre-mesures urgentes est d'autant plus à propos dans le cyberespace étant donné la prédominance des procédés de dissimulation et les difficultés de traçabilité.

Dans les cas les plus graves constitutifs de menace contre la paix et la sécurité internationales, la France peut également saisir le CSNU au titre du Chapitre VI de la Charte des Nations unies, voire du Chapitre VII en cas de menace contre la paix ou de rupture de la paix.

Par ailleurs, la France n'exclut pas la possibilité d'invoquer l'état de détresse ou l'état de nécessité pour protéger un intérêt essentiel contre une cyberattaque situé en deçà du seuil de l'agression armée constituant un péril grave et imminent. Dans ce cas, les mesures adoptées demeurent de nature pacifique et ne portent pas gravement atteinte à un intérêt essentiel de l'État concerné.

L'adoption de telles mesures en réponse à une cyberattaque visant la France et constitutive d'une violation du droit international n'est pas systématique et relève d'une décision politique adoptée en opportunité.

La France dispose de moyens de prévention, d'anticipation, de protection, de détection et de réaction aux cyberattaques constitutives d'une violation du droit international dont elle serait victime. En cas de cyberattaque visant ses systèmes d'information, les services de l'Etat peuvent conduire des cyber-opérations.
Au cas par cas, et sur décision de la chaîne nationale de cyberdéfense, ces opérations peuvent être menées dans le cadre de contre-mesures.

1.2. Une cyberattaque provoquant des dommages d'une ampleur et d'une gravité significatives peut constituer une agression armée ouvrant le droit de faire usage de la légitime défense

Conformément à la jurisprudence de la Cour internationale de justice (CIJ), la France distingue les formes les plus graves d'emploi de la force, qui constituent une agression armée et auxquelles l'État victime peut répondre par la légitime défense individuelle ou collective, d'autres modalités moins brutales[22]. Les cyberattaques peuvent constituer une forme grave d'emploi de la force, à laquelle la France pourrait répondre par la légitime défense.

1.2.1. La qualification d'une cyberattaque comme agression armée

La France réaffirme qu'une cyberattaque peut constituer une agression armée au sens de l'article 51 de la Charte des Nations unies[23], dès lors que ses effets et son ampleur atteignent une certaine gravité et sont comparables à ceux d'un emploi de la force physique[24]. À la lumière de ces critères, la qualification d'une cyberattaque comme constitutive d'une agression armée

17 Article 49 alinéa 1 du Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite de la Commission du droit international (CDI).

18 Article 50 du Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite de la CDI.

19 Article 50 alinéa 1.a du Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite de la CDI.

20 Article 53 du Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite de la CDI.

21 Article 51 du Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite de la CDI.

22 CIJ, Activités militaires et paramilitaires au Nicaragua et contre celui-ci, Nicaragua c. États-Unis d'Amérique, arrêt, C.I.J Recueil 1986, p. 101, § 191 : il faut « distinguer entre les formes les plus graves de l'emploi de la force (celles qui constituent une agression armée) et d'autres modalités moins brutales ».

23 Outre le Livre blanc relatif à la défense et à la sécurité nationale de 2013, cette position figure dans la Revue stratégique de défense et de sécurité nationale (2017) : « [d]ans le cyberespace, certaines attaques, en raison de leur ampleur et de leur gravité, pourraient relever de la qualification d'agression armée : une attaque informatique majeure, par les dommages qu'elle causerait, pourrait ainsi justifier l'invocation de la légitime défense au sens de l'article 51 de la Charte des Nations unies » (p. 35), ainsi que dans la Revue stratégique de cyberdéfense (2018) « [u]ne attaque informatique majeure visant la France, eu égard aux graves dommages qu'elle causerait, pourrait constituer une « agression armée », au sens de l'article 51 de la Charte des Nations unies, et justifier l'invocation de la légitime défense » (p. 82).@

24 Activités militaires et paramilitaires au Nicaragua et contre celui-ci, Nicaragua c. États-Unis d'Amérique, arrêt, C.I.J Recueil 1986, p.93, § 195. Article 2 de la résolution 3314 (1974) de l'AGNU : « l'emploi de la force armée en violation de la Charte par un État agissant le premier constitue la preuve suffisante à première vue d'un acte d'agression », pour peu que les actes en cause ou leurs conséquences atteignent une gravité suffisante. »

sera examinée au cas par cas au regard des circonstances de l'espèce.

Une cyberattaque pourrait être qualifiée d'agression armée dès lors qu'elle provoquerait des pertes humaines substantielles, ou des dommages physiques ou économiques considérables. Cela serait le cas d'une opération dans le cyberespace provoquant une déficience des infrastructures critique[25] avec des conséquences significatives, ou susceptibles de paralyser des pans entiers de l'activité du pays, de déclencher des catastrophes technologiques ou écologiques et de faire de nombreuses victimes[26]. Dans une telle hypothèse, les effets de cette opération seraient similaires à ceux qui résulteraient de l'utilisation d'armes classiques[27].

Pour être qualifiée d'agression armée, la cyberattaque doit également avoir été perpétrée, directement ou indirectement, par un État. En dehors des actes commis par des personnes appartenant aux organes étatiques ou exerçant des prérogatives de puissance publique, un État est responsable des actes perpétrés par des acteurs non-étatiques uniquement si ces derniers agissent en fait sur ses instructions ou ses directives ou sous son contrôle conformément aux règle sur la responsabilité de l'État pour fait internationalement illicite et à la jurisprudence de la CIJ. À l'heure actuelle, aucun État n'a qualifié une cyberattaque menée à son encontre d'agression armée.

Conformément à la jurisprudence de la CIJ, la France ne reconnaît pas l'extension du droit de légitime défense à des actes perpétrés par des acteurs non-étatiques dont l'action ne serait pas attribuable, directement ou indirectement, à l'État.

La France a pu invoquer exceptionnellement la légitime défense à l'encontre d'une agression armée perpétrée par un acteur présentant les caractéristiques d'un « quasi-État » comme elle l'a fait pour son intervention en Syrie face au groupe terroriste Daech[28]. Toutefois, ce cas exceptionnel ne saurait constituer l'expression définitive d'une reconnaissance de l'étirement du concept de légitime défense à des actes perpétrés par des acteurs non-étatiques intervenant sans le soutien direct ou indirect d'un État.

Il n'en demeure pas moins qu'il ne peut être exclu que la pratique générale évolue dans le sens d'une interprétation du droit de la légitime défense comme autorisé en réponse à une agression armée perpétrée par des acteurs non-étatiques dont les actes ne sont pas imputables à un État. Toutefois, une telle évolution devra être engagée en ayant à l'esprit le Statut de Rome de la Cour pénale internationale (CPI), tel qu'amendé en 2010 pour y ajouter le crime d'agression[29], et la jurisprudence que la CPI aura alors pu adopter en ce domaine[30].

1.2.2. L'usage du droit de légitime défense à l'encontre d'une agression armée numérique

En vertu de l'article 51 de la Charte des Nations unies, une agression armée ouvre le droit de l'État victime à faire usage de la légitime défense individuelle ou collective. La légitime défense en réponse à une agression armée conduite dans le cyberespace peut être mise en œuvre par des moyens numériques ou classiques dans le respect des principes de nécessité et de proportionnalité[31]. Sur décision du Président de la République d'engager les forces armées françaises, le ministère des armées peut mener des cyber-opérations[32] à des fins militaires dans le cyberespace.

Des cyberattaques qui, isolément, n'atteignent pas le seuil de l'agression armée pourraient être qualifiées comme telle si l'accumulation de leurs effets atteint un seuil de gravité suffisant[33], ou si elles sont réalisées de manière concourante à des opérations menées dans le champ d'action physique constitutives d'une agression armée, dès lors que ces attaques sont coordonnées et émanent de la même entité ou de différentes entités agissant de concert.

Dans des circonstances exceptionnelles, la France s'autorise à recourir à la légitime défense préemptive en réponse à une cyberattaque « 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 »[34]. Toutefois, elle ne reconnaît pas la légalité du recours à la force sur le fondement de la légitime défense préventive[35].

25 SGDSN, Revue stratégique de cyberdéfense, 2018, p. 61.

26 *Livre Blanc de la Défense et de la Sécurité nationale*, 2013, p. 49.

27 SGDSN, Revue stratégique de cyberdéfense, février 2018, p. 82

28 La France a fondé la légalité de son intervention contre Daech en Syrie, tout d'abord, sur le principe de la légitime défense collective au profit de l'Irak, puis, après les attentats du 13 novembre 2015, sur le fondement de la légitime défense individuelle.

29 L'article 8 bis du Statut de Rome définit le crime d'agression comme un acte perpétré par « une personne effectivement en mesure de contrôler ou de diriger l'action politique ou militaire d'un État » qui par sa nature, sa gravité et son ampleur, donc indépendamment des moyens employés, constitue une violation manifeste de la Charte des Nations unies

30 La CPI est compétente pour juger du crime d'agression depuis juillet 2018.

31 « Les Parties sont en outre d'accord pour admettre que la licéité de la riposte à l'agression dépend du respect des critères de nécessité et de proportionnalité des mesures prises au nom de la légitime défense (…). Les mesures ne doivent pas simplement tendre à protéger les intérêts vitaux de sécurité de la partie qui les adopte ; elles doivent être « nécessaires » », Activités militaires et paramilitaires au Nicaragua et contre celui-ci, Nicaragua c. États-Unis d'Amérique, arrêt, C.I.J Recueil 1986, §194 et §282. « [I]l existe une « règle spécifique (…) bien établie en droit international coutumier » selon laquelle « la légitime défense ne justifierait que des mesures proportionnées à l'agression armée subie, et nécessaires pour y riposter », Licéité de la menace ou de l'emploi d'armes nucléaires, avis consultatif, C.I.J Recueil 1996, § 41.

32 Il s'agit, plus particulièrement, d'opérations de lutte informatique offensive (LIO).

33 SGDSN, *Revue stratégique de cyberdéfense*, février 2018, p. 82. Dans l'Affaire des plateformes pétrolières, République Islamique d'Iran c. États-Unis, la CIJ n'écarte pas l'approche consistant à évaluer si une série d'attaques contre les États-Unis est susceptible de constituer une agression armée (arrêt, C.I.J Recueil, 2003, § 64).

34 SGDSN, Revue stratégique de cyber défense, février 2018, p. 84.

35 La légitime défense préventive s'exerce en réponse à une potentielle agression armée, c'est-à-dire latente et plus ou moins susceptible de se produire dans le futur.

Les États qui décident, dans la conduite d'une cyber-opération ou dans leur réaction à une cyberattaque, de s'appuyer sur des acteurs non-étatiques, par exemple des entreprises fournissant des services informatiques offensifs ou des groupes de hackeurs, sont responsables des actions menées par ces acteurs. Face au risque d'instabilité systémique que fait peser l'utilisation de capacités offensives par le secteur privé, la France, dans le prolongement de l'Appel de Paris, est favorable à leur encadrement strict et à l'interdiction pour ces acteurs non-étatiques de conduire des activités offensives dans le cyberespace pour eux-mêmes ou pour le compte d'autres acteurs non-étatiques[36].

Enfin, toute réaction sur le fondement de la légitime défense reste provisoire et subsidiaire. Elle doit faire l'objet d'une notification sans délai au CSNU[37] et être suspendue dès lors que le Conseil se saisit de la question, substitue des mesures collectives à des actions unilatérales ou, à défaut, dès lors qu'elle atteint son but, c'est-à-dire repousse l'agression armée ou met fin à celle-ci. Le choix d'autres mesures, notamment des contre-mesures ou une saisine du CSNU, peut être privilégié si ces dernières s'avèrent plus opportunes.

Les particularités du cyberespace ne remettent pas en cause la position française quant au droit de légitime défense en réponse à des cyberattaques qui atteignent le seuil de l'agression armée au sens de l'article 51 de la Charte des Nations unies.

En réponse à une agression armée conduite par un vecteur numérique, l'usage de la force par des moyens numériques ou classiques doit répondre aux critères de nécessité et de proportionnalité.

1.2.3. Le non-respect de l'obligation de diligence requise par un État tiers ne suffit pas à fonder le droit de recourir à la force à son encontre dans le cadre de cyber attaques perpétrées depuis son territoire

En vertu du principe de diligence requise, les États ne doivent 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 »[38], notamment des actes qui porteraient atteinte à l'intégrité territoriale ou à la souveraineté d'État tiers[39]. En outre, les États doivent veiller à ce que les acteurs non-étatiques n'utilisent pas leur territoire pour commettre de telles activités, et ne pas faire appel à des intermédiaires pour commettre des actes contraires aux droits des autres Etats à l'aide de TIC[40]. La violation par un État de son obligation de diligence requise peut justifier l'activation de mécanismes au niveau politico-diplomatique[41] pouvant aller jusqu'à la mise en œuvre de contre-mesures, voire d'une saisine du CSNU.

Le fait pour un État de ne pas prendre toutes les mesures raisonnables pour faire cesser des actes illicites à l'encontre d'États tiers perpétrés depuis son territoire par des acteurs non-étatiques, ou d'être incapable de les prévenir ne saurait constituer une exception au principe d'interdiction de recours à la force[42].

Dans ces conditions, la France ne reconnaît pas l'approche extensive de la légitime défense exprimée par une majorité des experts du *Manuel de Tallinn*[43] qui autorise un État victime d'une cyberattaque de grande ampleur perpétrée depuis le territoire d'un État tiers par des acteurs non-étatiques à faire usage de la légitime défense à l'encontre de cet État, y compris si cette réponse est réalisée dans le respect du principe de nécessité, s'il s'agit de l'unique moyen de faire face à l'agression armée et si l'État territorial ne veut pas ou n'est pas en mesure d'empêcher la perpétration de telles activités.

En vertu de l'obligation de diligence requise, les États veillent à ce que leur domaine de souveraineté dans le cyberespace ne soit pas utilisé pour commettre des faits internationalement illicites.
Le non-respect de cette obligation par un État ne constitue pas un motif d'exception au principe d'interdiction de recours à la force, contrairement à l'avis de la majorité des experts du *Manuel de Tallinn*.

1.3. L'attribution d'une cyberattaque d'origine étatique relève d'une décision politique nationale

Les cyberattaques auxquelles les États et les acteurs privés sont confrontés sont, par nature, difficiles à caractériser dans le cyberespace. Les moyens numériques sont utilisés à des fins d'espionnage, cybercriminelles, de déstabilisation, voire de sabotage. Les caractéristiques inhérentes à ce milieu, la difficulté à tracer et à maîtriser les activités, l'intervention toujours plus importante d'acteurs non-étatiques, ainsi que des possibilités

36 SGDSN, Revue stratégique de cyberdéfense, février 2018, p.88.

37 Article 51 de la Charte des Nations unies: « [l]es mesures prises par des Membres dans l'exercice de ce droit de légitime défense sont immédiatement portées à la connaissance du Conseil de sécurité ».

38 Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, rapport de 2015, Note du Secrétaire général, A/70/174, 22 juillet 2015, §13 c).

39 Affaire relative au personnel diplomatique et consulaire des États-Unis à Téhéran, États-Unis d'Amérique c. Iran, arrêt, C.I.J Recueil 1980, §§ 61-8.

40 « Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale », Note du Secrétaire général, A/70/174, 22 juillet 2015, § 28.

41 SGDSN, Revue stratégique de cyberdéfense, février 2018, annexe 7 relative aux options de réponse aux attaques informatiques, p. 159.

42 L'interdiction du recours à la force ne souffre que de trois exceptions : la légitime défense en cas d'agression armée prévue par l'article 51 de la Charte des Nations unies, le recours à la force autorisé par le CSNU aux termes du Chapitre VII et le consentement de l'État sur le territoire duquel a lieu l'intervention.

43 "Self-defence against a cyber armed attack (…) is permissible when it complies with the principle of necessity (Rule 72), is the only effective means of defence against the armed attack, and the territorial State is unable (e.g. because its lacks the expertise or technology) or unwilling to take effective actions to repress the relevant elements of the cyber armed attack. In particular, these Experts emphasised that States have a duty to ensure their territory is not used for acts contrary to international law (Rule 6)", Michael Schmitt et Liis Vihul (dir.), The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017, règle 71, p. 339.

ouvertes aux États d'utiliser ces acteurs privés comme des intermédiaires pour développer des activités malveillantes, rendent particulièrement complexes l'identification des auteurs et des commanditaires de ces attaques.

Lorsqu'une cyberattaque est détectée, la France met en œuvre les opérations nécessaires à la caractérisation pouvant aller jusqu'à la neutralisation de ses effets. La détermination de l'instigateur repose principalement, mais non exclusivement, sur des éléments techniques recueillis lors des investigations menées sur la cyberattaque, notamment la détermination de l'infrastructure d'attaque et de transit de la cyber-opération et leur localisation, l'identification des modes opératoires adverses (MOA), la chronologie générale des activités de l'auteur, de l'ampleur et de la gravité de l'incident et du périmètre compromis, ou encore des effets recherchés par l'attaquant[44]. Ces éléments pourront permettre de déterminer l'existence, ou non, d'un lien entre les instigateurs et un État.

Une cyberattaque est considérée comme étant le fait d'un État si celle-ci a été perpétrée par un organe étatique[45], une personne ou une entité exerçant des prérogatives de puissance publique[46], ou encore une personne ou un groupe de personnes agissant sur les instructions ou les directives ou sous le contrôle de cet État[47].

L'identification d'un État comme responsable d'une cyberattaque constitutive d'un fait internationalement illicite n'oblige en rien l'État lésé à procéder à une attribution publique. En effet, cette attribution relève d'un choix en opportunité réalisé, notamment, en fonction de la nature et de l'origine de l'opération, des circonstances de l'espèce, ou encore du contexte international. Cette décision est de nature régalienne en ce que la France se réserve le droit d'attribuer publiquement, ou non, une cyberattaque dont elle aurait été victime, et de porter cette information à la connaissance de sa population, d'États tiers ou de la communauté internationale. Si cette démarche n'exclut pas une coordination étroite, pouvant aller jusqu'à une décision d'attribuer de façon collective une attaque informatique, avec les alliés et les États partenaires de la France, y compris des organisations internationales ou régionales, notamment l'Union européenne (UE) ou l'Organisation du traité de l'Atlantique Nord (OTAN), elle relève de la compétence exclusive de la France. Par ailleurs, le droit internationl ne contraint pas les États à communiquer les éléments de preuve sur lesquels ils se fondent pour attribuer publiquement une cyberattaque. Ces éléments permettent, néanmoins, de légitimer le bien-fondé de cette attribution.

En tout état de cause, le défaut d'attribution publique ne constitue pas un obstacle définitif à l'application du droit international, notamment à la mise en œuvre du droit de réponse offert aux États[48].

Les capacités du ministère des armées participent au processus de caractérisation des cyberattaques menées contre l'État français.

L'attribution publique d'une cyberattaque dont la France est victime relève d'une décision politique nationale. Si cette compétence peut s'exercer en coordination avec d'autres États ou des organisations internationales, elle constitue, prima facie, une prérogative régalienne.

44 Instruction n° 101000/ARM/CAB relative à la politique de lutte informatique et défensive du ministère des armées du 7 février 2019.

45 Article 4 alinéa 1 du projet d'articles sur la responsabilité de l'État pour fait internationalement illicite de la CDI.

46 Article 5 du projet d'articles sur la responsabilité de l'État pour fait internationalement illicite de la CDI.

47 Article 8 du projet d'articles sur la responsabilité de l'État pour fait internationalement illicite de la CDI

48 « Le défaut d'attribution ne saurait constituer un obstacle définitif à l'application du droit international existant, d'autant que ce dernier offre des moyens d'action neutres quant à celle-ci », SGDSN, Revue stratégique de cyberdéfense, février 2018, p. 82.

II. LE DROIT INTERNATIONAL APPLICABLE AUX CYBER-OPÉRATIONS EN CONTEXTE DE CONFLIT ARMÉ

Messages clés

En situation de conflit armé, le cyberespace est un espace de confrontation à part entière qui s'articule avec les autres champs de confrontation. La capacité informatique offensive mise en œuvre sur les théâtres d'engagement des forces armées françaises est maîtrisée à travers une doctrine et un cadre d'emploi qui la soumettent au respect du Droit International Humanitaire (DIH).

Une cyber-arme[49] est, en premier lieu, un moyen de combinaison étant donné sa capacité à agir au profit des armes employées dans les autres milieux. À cet égard, elle produit les mêmes effets de renseignement, de neutralisation et de déception[50] que les moyens classiques qui sont soumis à des procédures de ciblage déjà mises en œuvre par les forces armées françaises et respectueuses du DIH. **Ces opérations peuvent constituer des attaques** au sens de l'article 49 du Protocole additionnel I aux Conventions de Genève (PA I), **dès lors qu'elles produisent des dommages physiques, ou qu'elles rendent un système inopérant. Toutefois, certaines opérations militaires, telles que le recueil général d'informations ou l'altération des capacités d'influence de l'adversaire, ne relèvent pas de l'attaque. Elles restent, néanmoins, soumises aux dispositions pertinentes du DIH.**

La France intègre les principes de distinction, de proportionnalité et de précaution à toute opération de lutte informatique offensive menée en contexte de conflit armé. Les cyber-opérations visent exclusivement des infrastructures numériques identifiées comme objectifs militaires. En outre, l'identification de dommages civils excessifs par rapport à l'avantage militaire direct et concret attendu encadre les possibilités d'actions numériques, tout comme l'adaptation de l'arme employée à l'effet recherché, contribue au respect du principe de précaution.

En situation de conflit armé, le cyberespace est un espace de confrontation à part entière comme le sont les espaces terrestre, maritime, aérien ou l'espace extra-atmosphérique[51].

Afin de répondre à cette nouvelle forme de conflictualité, le ministère des armées intègre pleinement la dimension numérique à ses opérations militaires. Si la lutte informatique offensive (LIO) est une capacité de niveau stratégique, elle est aussi, au niveau tactique, une arme dont les effets se combinent à ceux des armes classiques.

La complexité liée à l'emploi de la cyber-arme exige d'en maîtriser l'ensemble des effets, dans un cadre qui respecte le DIH. Tout emploi des moyens de lutte informatique offensive par les forces armées françaises est réalisé dans le respect des principes régissant la conduite des hostilités, au même titre que les opérations planifiées et conduites exclusivement dans le champ d'action physique.

2.1. Des cyber-opérations peuvent caractériser l'existence d'un conflit armé

Des cyber-opérations constitutives d'hostilités entre deux ou plusieurs États peuvent caractériser l'existence d'un conflit armé international (CAI)[52]. De même, des cyber-opérations prolongées opposant des forces armées gouvernementales aux forces d'un ou de plusieurs groupes armés, ou opposant plusieurs groupes armés entre eux peuvent constituer un conflit armé non international (CANI), dès lors que ces groupes font preuve d'un minimum d'organisation et que les effets de ces opérations atteignent un degré de violence suffisant[53].

Il s'agit généralement d'opérations militaires concourantes à des opérations militaires conventionnelles, d'où l'absence de difficulté à qualifier la situation de conflit armé. Si l'hypothèse d'un conflit armé constitué exclusivement d'activités numériques ne peut être exclue par principe, elle repose toutefois sur la capacité des cyber-opérations autonomes à atteindre le seuil de violence requis pour une telle qualification.

Bien que dématérialisées, les cyber-opérations restent soumises au champ d'application géographique du DIH, dans la mesure où leurs effets doivent se produire sur le territoire des États parties au CAI et sur le territoire sur lequel se déroulent les hostilités en CANI.

49 Le terme « arme » est utilisé, ici, dans un sens générique. Une « cyber-arme » renvoie à l'ensemble des moyens numériques utilisés en contexte de conflit armé et en lien avec celui-ci, c'est-à-dire aux armes, moyens et méthodes de guerre au sens de l'article 35 du PA I, mais également aux moyens numériques qui ne produisent pas de dommages (utilisés à des fins, par exemple, de renseignement).

50 La déception comprend la dissimulation, la diversion et la manipulation de l'information à fins de tromper l'adversaire sur ses intentions.

51 Livre blanc sur la défense et la sécurité nationale, 2013 : « [l]es systèmes d'information sont désormais une donnée constitutive de nos sociétés ». La Revue stratégique de défense et de sécurité nationale de 2017 indique que l'espace numérique est « désormais considéré comme un champ de confrontation à part entière [et qu'il] fait l'objet d'une compétition stratégique intense ».

52 Article 2 commun aux Conventions de Genève (1949) et article 1 alinéa 3 du PA I.

53 Dans le cas d'un affrontement armé prolongé atteignant un certain seuil d'intensité entre deux parties incluant au moins une partie non-étatique, le DIH distingue entre le CANI de basse intensité soumis à l'article 3 commun aux Conventions de Genève (le ou les groupe(s) armé(s) fait ou font preuve d'un minimum d'organisation) et le CANI de haute intensité soumis à l'article 3 commun, ainsi qu'au Protocole additionnel II (PAII) (le degré d'organisation exigé du ou des groupe(s) armé(s) est particulièrement élevé : commandement responsable, exercice sur une partie du territoire d'un contrôle tel qu'il permet de mener des opérations militaires continues et concertées). Par ailleurs, un CANI peut être exporté lorsque les parties à un CANI initial prolongent leurs hostilités sur le territoire d'un ou de plusieurs États voisins avec le consentement du ou des États concernés. Les critères applicables au CANI exporté sont les mêmes que ceux applicables au CANI d'origine (identité des parties et intensité des violences). Ainsi, des opérations dans le cyberespace, seules ou en lien avec des opérations conventionnelles, qui obéissent à ces règles peuvent relever du CANI exporté.

Les cyber-opérations dédiées à l'engagement des forces armées en contexte de conflit armé sont soumises au DIH.

Une cyber-opération constitutive d'un affrontement entre États peut caractériser l'existence d'un CAI. L'état de la technologie semble exclure pour le moment que des cyber-opérations seules puissent atteindre le seuil de violence requis pour caractériser une situation de CANI.

Les moyens cyber sont, tout d'abord, des moyens de combinaison et de soutien des effets conventionnels. Malgré la nature dématérialisée du cyberespace, ces opérations restent soumises au cadre géographique du conflit dans lesquelles elles interviennent.

2.2. Le DIH s'applique à l'ensemble des cyber-opérations menées en contexte de conflit armé et en lien avec ce conflit

Dans le cadre d'un conflit armé, l'emploi de la cyber-armée est assujetti aux principes régissant la conduite des hostilités. La cyber-arme, qui s'inscrit dans le cadre de la LIO, peut être mise en œuvre en combinaison des moyens militaires conventionnels, ou de manière autonome. En appui des moyens conventionnels, elle produit les mêmes effets de renseignement, de neutralisation et de déception que ces moyens classiques soumis de longue date aux procédures de ciblage mises en œuvre dans le respect du DIH par les forces armées françaises.

La spécificité et la complexité des moyens de LIO exigent un dispositif de maîtrise des risques tout aussi important que celui qui est appliqué aux opérations conventionnelles en tenant compte des caractéristiques inhérentes à la conduite des opérations dans le cyberespace. En pratique, les risques liés à l'emploi d'une cyber-arme, notamment l'immédiateté de l'action, la dualité des cibles et l'hyperconnectivité des réseaux, exigent un processus de ciblage numérique spécifique encadrant l'ensemble des phases de la cyber-opération, ceci afin de les soumettre aux principes de distinction, de précaution et de proportionnalité, notamment en vue de minimiser les dommages et les pertes civils potentiels. Ce processus relève d'une planification longue et spécifique conduite en coordination étroite avec la planification des opérations dans le champ physique.

2.2.1. Une cyber-opération peut constituer une attaque au sens du droit international humanitaire

Toute cyber-opération menée en contexte de conflit armé, en lien avec celui-ci et constitutif d'un acte de violence, offensif ou défensif, contre une autre partie au conflit est une attaque au sens de l'article 49 du PA I aux Conventions de Genève[54].

En contexte de conflit armé, les cyber-armes visent principalement à produire des effets à l'encontre d'un système adverse pour en altérer la disponibilité, l'intégrité ou la confidentialité des données. Leurs effets peuvent être d'ordre matériel (cela est le cas de la neutralisation d'un système d'arme) ou immatériel (comme la collecte de renseignements), temporaires, réversibles ou définitifs[55].

À titre d'illustration, la destruction des capacités informatiques offensives ou conventionnelles militaires adverses par la perturbation, ou la création de dommages majeurs, est une attaque au sens du DIH. Cela est également le cas des actions de neutralisation qui endommagent les capacités militaires informatiques ou conventionnelles adverses par la destruction d'équipements ou de systèmes informatiques, ou de l'altération ou de la suppression de données numériques et/ou de flux d'échanges qui rendent inactif un service essentiel au fonctionnement de ces capacités.

Contrairement à la définition adoptée par les experts du *Manuel de Tallinn*[56], la France ne retient pas uniquement l'existence de critères matériels pour qualifier une cyber-opération d'attaque. En effet, elle considère qu'**une cyber-opération constitue une attaque dès lors que les équipements ou les systèmes visés ne rendent plus le service pour lesquels ils ont été mis en place, que cela soit de manière temporaire ou définitive, réversible ou non.** Dans le cas **d'effets temporaires et/ou réversibles, l'attaque est caractérisée dès lors qu'une intervention de l'adversaire est nécessaire pour rendre l'infrastructure ou le système de nouveau opérant** (réparation des équipements, remplacement d'une pièce, réinstallation du réseau, etc.).

La majeure partie des cyber-opérations menées par les forces armées françaises en contexte de conflit armé (essentiellement de la collecte d'informations) ne répond pas à la définition de l'attaque. Ainsi, l'altération des capacités de propagande de l'adversaire, notamment le fait de rendre indisponible un site d'influence par saturation ou déni de service, non prohibée par le DIH par analogie aux actions classiques de brouillage des communications radio ou d'émissions de télévision, ne saurait être caractérisée comme une attaque. Toutefois, ces opérations – au même titre que le recueil général d'informations dans le but d'évaluer les capacités militaires adverses, ou de l'intrusion dans un système afin de recueillir des données – restent soumises aux dispositions du DIH applicables à toute opération militaire menée en contexte de conflit armé.

Contrairement au Manuel de Tallinn, la France considère qu'une attaque au sens de l'article 49 du PA I peut être caractérisée en l'absence de blessures ou de pertes humaines, ou de dommages physiques à l'encontre de biens. Ainsi, une cyber-opération constitue une attaque si les équipements ou les systèmes visés ne rendent plus le service pour lesquels ils

54 Article 49 du PA I : « [L]'expression « attaques » s'entend des actes de violence contre l'adversaire, que ces actes soient offensifs ou défensifs ».

55 Éléments publics de doctrine militaire de lutte informatique offensive, 2019.

56 "Definition of cyber attack. A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects", Michael Schmitt et Liis Vihul (dir.), The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017, règle 92, p. 415.

ont été mis en place, ceci y compris de manière temporaire et réversible, dès lors qu'une intervention de l'adversaire est nécessaire pour rendre l'infrastructure ou le système de nouveau opérant.

La majeure partie des cyber-opérations, en particulier celles de LIO menées par la France en contexte de conflit armé, se situe en deçà du seuil de l'attaque, puisqu'il s'agit principalement de collecte d'informations et de brouillage des capacités d'influence adverse. Ces opérations restent, néanmoins, soumises aux principes généraux du DIH.

2.2.2. L'application des principes régissant la conduite des hostilités

Dans un environnement militaire marqué par une conflictualité en évolution, l'absence de ligne de front clairement définie et l'intervention d'adversaires qui se fondent dans la population civile, ou qui opèrent selon des modes d'actions variés et asymétriques, les règles applicables à la conduite des hostilités sont particulièrement complexes à mettre en œuvre. Cette complexité est accrue dans le cyberespace où l'immédiateté de l'action, la dualité des cibles et l'hyperconnectivité des systèmes d'information et des réseaux peuvent rendre les effets d'une cyber-opération fulgurants.

Afin de veiller à l'application des principes régissant la conduite des hostilités (distinction, proportionnalité et précaution, interdiction des maux superflus et des souffrances inutiles[57]), les cyber-opérations répondent à un processus de ciblage numérique spécifique placé sous la responsabilité du chef d'état-major des armées qui bénéficie, notamment, du soutien des opérationnels et de conseillers juridiques opérationnels spécialisés.

Il n'est pas exclut que la violation grave de ces principes du fait d'une cyber-opération pourrait constituer un crime de guerre au sens du Statut de Rome[58].

• Le principe de distinction

En vertu du principe de distinction, les parties à un conflit armé doivent en tout temps faire la distinction entre la population civile et les combattants, ainsi qu'entre les biens de caractère civil et les objectifs militaires[59]. À ce titre, les cyberattaques réalisées dans un contexte de conflit armé qui ne sont pas dirigées contre un objectif militaire déterminé, ou dont les effets ne peuvent pas être limités sont interdites[60]. En cas de doute sur la qualité belligérante d'un individu, celui-ci doit être considéré comme civil[61]. De manière identique, en cas de doute, un bien normalement affecté à un usage civil est présumé ne pas être utilisé en vue d'apporter une contribution effective à l'action militaire[62] La France s'oppose en cela au Manuel de Tallinn[63] qui considère qu'en cas de doute sur l'usage d'un tel bien à des fins militaires, il convient de conclure à un tel usage uniquement à l'issue d'un examen minutieux.

Dans cette perspective et sous l'autorité du chef d'état-major des armées, des opérations de LIO sont planifiées et coordonnées en prenant toutes les mesures pratiquement possibles pour vérifier que les objectifs ciblés ne sont pas des personnes civiles, ou des biens de caractère civil. Le commandement veille ainsi à réunir les renseignements nécessaires à l'identification de l'objectif et à choisir le moyen le plus adapté pour mettre en œuvre le principe de distinction. Même si la cyber-arme peut revêtir des effets immédiats, son intégration dans la manœuvre opérationnelle repose sur une planification souvent longue et spécifique qui permet de recueillir l'information nécessaire à l'identification de la nature du système visé (par une cartographie du réseau ennemi, par exemple) afin de veiller au respect du DIH. Ainsi, une cyber-opération est annulée s'il est constaté que la cible examinée s'avère ne pas être un objectif militaire.

– La distinction entre objectifs militaires et biens civils[64].

Dans le cyberespace, des équipements ou des systèmes informatiques, des données, des processus ou des flux d'échanges qui composent un service peuvent constituer un objectif militaire si, d'une part, ils contribuent à l'action militaire par leur nature (postes informatiques des forces armées, réseaux de commandement militaire, de localisation, de surveillance etc.), leur emplacement (lieux depuis lesquels sont menées les cyberattaques), leur destination (usage prévisible des réseaux informatiques à des fins militaires), ou leur utilisation (usage d'un pan du réseau à des fins militaires) ; et si d'autre part, leur destruction totale ou partielle, leur capture ou neutralisation confèrent un avantage militaire précis. Dès lors, un centre de propagande peut constituer un objectif militaire licite et faire

57 Ce principe interdit de causer des maux et des souffrances aux civils, mais également aux combattants ou membres de GAO qui ne sont pas nécessaires pour atteindre des buts strictement militaires. A ce titre, il est interdit d'employer des armes, des projectiles et des matières, ainsi que des méthodes de guerre de nature à causer de telles souffrances, que celles-ci soient physiques ou morales. Au regard de la nature des opérations menées par la France dans le cyberespace (à l'encontre d'infrastructures et de systèmes numériques), ce principe est bien pris en compte, mais ne trouve pas à s'appliquer concrètement. En ce sens, il ne fera pas l'objet d'un développement en tant que tel.

58 Michael Schmitt and Liis Vihul (dir.), The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017, règle 84-85, pp. 391-400.

59 Article 48 du PA I : « [e]n vue d'assurer le respect et la protection de la population civile et des biens de caractère civil, les Parties au conflit doivent en tout temps faire la distinction entre la population civile et les combattants ainsi qu'entre les biens de caractère civil et les objectifs militaires et, par conséquent, ne diriger leurs opérations que contre des objectifs militaires ».

60 Article 51 alinéa 4 du PA I.

61 Articles 50 alinéa 3 et 52 alinéa 3 du PA I.

62 Article 52 alinéa 3 du PA I. "In case of doubt as to whether an object and associated cyber infrastructure that is normally dedicated to civilian purposes is being used to make an effective contribution to military action, a determination that it is so being used may only be made following a careful assessment", Michael Schmitt et Liis Vihul (dir.), The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017, règle 102, p. 448.

63

64 Article 52 alinéa 2 du PA I.

l'objet d'une cyberattaque, si ce dernier diffuse des instructions liées à la conduite des hostilités[65].

À l'opposé, tous les biens qui ne sont pas des objectifs militaires sont considérés comme des biens civils[66]. Une attaque menée dans le cyberespace ne peut être dirigée contre des systèmes informatiques utilisés par des écoles, des établissements médicaux, ou encore par tout autre service exclusivement civil, ni contre des systèmes dont la destruction entraînerait uniquement des effets tangibles sur des biens civils, sauf si ces derniers sont utilisés à des fins militaires. Au regard de la dépendance numérique actuelle, des données de contenu (comme des données civiles, des données bancaires, des données médicales etc.) sont protégées au titre du principe de distinction.

Les cyber-opérations doivent également prendre en compte la protection spéciale de certains biens, tels que les unités sanitaires[67], les biens culturels[68], l'environnement naturel[69], les biens indispensables à la survie de la population[70], ainsi que les installations contenant des forces dangereuses[71]. Cette protection s'étend aux équipements et aux services informatiques, ainsi qu'aux données nécessaires à leur fonctionnement (comme, par exemple, les données médicales liées au fonctionnement d'un établissement hospitalier).

Une infrastructure informatique, ou un système qui sert à la fois à des fins civiles et à des fins militaires, peuvent être considérés, après une analyse minutieuse et au cas par cas, comme un objectif militaire. Ils peuvent être ciblés à condition que soient respectés les principes de proportionnalité et de précaution. Compte tenu de l'hyperconnectivité des systèmes, le commandement exerce une vigilance sur l'ensemble de l'action pour éviter, ou du moins réduire au minimum dans le respect des principes de précaution et de proportionnalité, les effets sur les civils et les biens de caractère civil.

– La distinction entre civils et combattants[72].

Des cyber-combattants[73], notamment le personnel militaire affecté au sein d'un commandement d'opérations dans le cyberespace, un groupe de hackers placé sous commandement étatique, ou des membres de groupes armés organisés (GAO)[74] perpétuant des cyber-opérations à l'encontre de la partie adverse, peuvent faire l'objet d'attaques, sauf s'ils sont hors de combat.

Toute autre personne est considérée comme civile et jouit d'une protection générale contre les dangers résultant d'opérations militaires[75], sauf si elle participe directement aux hostilités et durant le temps de cette participation[76]. Une cyber-opération menée pour nuire aux opérations militaires ou à la capacité militaire d'une partie à un conflit armé au détriment de celle-ci et à l'avantage d'une partie adverse, ou qui est de nature à causer des pertes en vies humaines, des blessures et des dommages de caractère civil peut être constitutive d'une participation directe aux hostilités[77].

À titre d'exemple, la pénétration d'un système militaire d'une partie à un conflit armé en vue de collecter des renseignements tactiques au profit d'une partie adverse à des fins d'attaque est une participation directe aux hostilités, tout comme le fait d'installer un code malveillant, de préparer un botnet en vue de lancer une attaque par déni de service, ou encore de développer un logiciel spécifiquement destiné à la perpétration d'un acte hostile[78].

Dans la conduite d'opérations de lutte informatique, le processus de ciblage numérique s'attache essentiellement à respecter le critère de l'objectif militaire en termes de distinction, compte tenu de la nature des cibles (systèmes et infrastructures numériques). Contrairement au *Manuel de Tallinn*, la France interprète l'article 52 alinéa 3 du PA I comme obligeant les États à appliquer une présomption de caractère civil d'un bien normalement affecté à un usage civil en cas de doute et non pas comme nécessitant

65 Tribunal pénal international pour le Rwanda (TPIR), Le procureur c. Nahimana, Barayagwiza et Ngeze, 3 décembre 2013, ICTR-99-52-T, Jugement. Tel était le cas de la Radio des mille collines au Rwanda qui transmettait des informations précises relatives à la localisation des Tutsis et donnait de fausses informations à ces derniers pour les encourager à se regrouper dans des zones prétendument protégées.

66 Article 52 alinéa 1 du PA I.

67 Articles 19.1, 24, 25, 35 et 36 de la première Convention de Genève (1949) ; articles 22 alinéa 1, 36 et 39 de la deuxième Convention de Genève (1946) ; articles 18 alinéa 1, 20 alinéa 1 et 22 alinéa 1 de la quatrième Convention de Genève (1949) ; articles 12.1, 15.1 et 21 du PA I.

68 Article 53 du PA I et Convention pour la protection des biens culturels en cas de conflit armé, 1954.

69 Article 35 alinéa 3 et 55 alinéa 1 du PA I.

70 Articles 54 alinéa 2 du PAI et 14 du PA II.

71 Article 54 alinéa 2 du PA I.

72 Article 48 du PA I.

73 Article 43 du PA I.

74 Le Tribunal pénal international pour l'ex-Yougoslavie (TPIY) a recensé plusieurs critères indicatifs permettant de considérer un groupe armé comme étant « organisé », parmi lesquels : l'existence d'une structure de commandement et de règles et mécanismes disciplinaires au sein du groupe, l'existence d'un quartier général, le contrôle d'un certain territoire par le groupe, sa capacité à se procurer des armes, d'autres équipements militaires, des recrues et une formation militaire, sa capacité à planifier, coordonner et exécuter des opérations militaires, y compris des mouvements de troupes et des opérations logistiques, son aptitude à définir une stratégie militaire unifiée et à appliquer une tactique militaire, et sa capacité à parler d'une seule voix et à négocier et conclure des accords tels que cessez-le-feu ou accords de paix. Pour en savoir plus sur le degré d'organisation requis, voir notamment TPIY, Le Procureur c. Boškoski et Tarčulovski, ICTY-IT–04–82-T, arrêt de la Chambre de première instance du 10 juillet 2008, §§ 194-205.

75 Article 51 alinéa 1 du PA I.

76 Article 51 alinéa 3 du PA I et article 13 du PA II.

77 Les critères de seuil de nuisance, de causation directe et de lien de belligérance doivent être remplis.

78 Les critères susmentionnés doivent être remplis

une nouvelle détermination pour conclure au fait que ce dernier apporte une contribution effective à l'action militaire.
Malgré leur caractère intangible, la France considère que des données civiles de contenu peuvent être considérées comme des biens protégés, contrairement à la position de la majorité des experts du *Manuel de Tallinn*[79]. La protection spéciale applicable à certains biens s'étend aux systèmes et aux données qui assurent leur fonctionnement.
Les cyber-combattants intégrés ou affiliés aux forces armées ou membres de groupes armés organisés peuvent être pris pour cible par le biais de moyens conventionnels, tout comme les civils perpétuant des activités offensives constitutives d'une participation directe aux hostilités. Compte tenu des difficultés d'identification des auteurs d'une cyberattaque, le ciblage de ces individus demeure marginal.

• Les principes de proportionnalité et de précaution

Les cyber-opérations sont conduites en veillant constamment à épargner la population civile, les personnes civiles et les biens de caractère civil[80].

En dépit de l'adoption des précautions nécessaires, si la neutralisation ou la destruction d'un objectif militaire par des moyens numériques risque tout de même d'engendrer des dommages civils, ceux-ci ne doivent pas excéder l'avantage militaire direct et concret attendu[81]. Les risques inhérents au cyberespace (immédiateté des effets, dualité intrinsèque des objectifs militaires, hyperconnectivité, faible traçabilité des opérations, vulnérabilité des systèmes) doivent ainsi être pris en compte afin de déterminer les modes d'action et les moyens à mettre en œuvre en matière de lutte informatique afin de veiller au respect du principe de proportionnalité.

Même si l'effet attendu d'une cyber-arme peut être difficile à mesurer compte tenu de l'interconnectivité des systèmes d'information, notamment en raison du risque de propagation au-delà de la cible visée, ces risques peuvent être maîtrisés à travers le développement de cyber-armes spécifiques, dont l'utilisation est décidée en fonction d'effets souhaités préalablement déterminés (activation du logiciel malveillant uniquement en présence d'un réseau spécifique préalablement identifié par une pénétration du système, existence d'un délai de désactivation, etc.).

Le recours à des programmes malveillants qui se reproduisent volontairement et se propagent sans contrôle ou réversibilité possible, et donc susceptibles de provoquer des dommages significatifs sur des systèmes ou des infrastructures civiles critiques, est contraire au DIH, tout comme. L'interruption temporaire sans avantage militaire d'un système adversaire suivi de dommages physiques sur des infrastructures civiles est contraire au DIH.

L'évaluation des effets d'une cyber-opération prend en compte l'ensemble des dommages prévisibles de la cyber-arme, que ces derniers soient de type direct (comme les dommages sur l'équipement informatique directement visé, ou l'interruption du système) ou indirects (comme les effets sur l'infrastructure contrôlée par le système attaqué, mais également sur les personnes affectées par le dysfonctionnement ou la destruction des systèmes ou des infrastructures visées, ou par l'altération et la corruption de données de contenu).

Afin que les opérations de LIO soient menées dans le respect du principe de précaution, le ministère des Armées s'appuie sur des experts opérationnels de la cyberdéfense militaire, placés sous la responsabilité du commandant de la cyberdéfense (COMCYBER), disposant des connaissances techniques nécessaires, d'une capacité à exploiter les informations disponibles (exploitation des renseignements collectés, capacité d'identification stricte des cibles, de corrélation entre l'arme et les effets recherchés etc.), et qui bénéficient de formations dédiées à la complexité de la cyber-arme.

Ces mesures de précaution dans l'attaque se doublent de mesures de précaution contre les effets de l'attaque qu'il incombe à l'État d'assurer pour protéger la population civile et les biens à caractère civil contre les effets des dangers résultant des cyber-opérations[82].

Malgré la complexité du cyberespace, le cadre d'emploi des opérations cyber menées en contexte de conflit armé reste déterminé par le respect des principes de précaution et de proportionnalité. À ce titre, le processus de ciblage numérique prend en compte les effets directs et indirects d'une cyber-arme. En dépit de l'interconnectivité des systèmes militaires et civils, le fait de pouvoir configurer la cyber-arme en fonction d'effets spécifiquement recherchés lors d'une opération permet d'éviter des dommages excessifs par rapport à l'avantage militaire direct et concret attendu. En effet, **l'absence de caractère létal et la capacité de cantonner les effets de la cyber-arme à un système préalablement identifié participent de l'obligation de choisir les moyens et méthodes d'attaque les mieux à même d'éviter, ou du moins de réduire au minimum, les pertes en vies humaines dans la population civile, les blessures aux personnes civiles et les dommages aux biens de caractère civil qui pourraient être causés incidemment.**

79 "The majority of the International Group of Experts agreed that the law of armed conflict notion of 'object' is not to be interpreted as including data, at least in the current state of the law. In the view of these Experts, data is intangible and therefore neither falls within the ordinary meaning' of the term object, nor comports with the explanation of it offered in the ICRC Additional Protocols 1987 Commentary", "In case of doubt as to whether an object and associated cyber infrastructure that is normally dedicated to civilian purposes is being used to make an effective contribution to military action, a determination that it is so being used may only be made following a careful assessment", Michael Schmitt et Liis Vihul (dir.), The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017, règle 100, comment 6, p. 437. Pour le Comité international de la Croix-Rouge, ces commentaires ne doivent pas être interprétés comme excluant le fait que des données puissent être considérées comme des biens protégés au regard du DIH. En effet, au regard de la dépendance numérique actuelle, une telle interprétation serait contraire au but et à l'objet du DIH.

80 Article 57 alinéa 1 du PA I.

81 Article 57 alinéa 2.a.iii du PA I.

82 Article 58 du PA I

2.3. Le droit de la neutralité a vocation à s'appliquer dans le cyberespace

Les cyber-opérations menées dans le cadre d'un CAI, ou qui déclenchent un tel conflit, sont soumises au droit de la neutralité[83]. À ce titre, les États parties à un CAI ne peuvent ni mener des cyber-opérations en lien avec ce conflit depuis des installations situées sur le territoire d'un État neutre ou sous le contrôle exclusif de celui-ci, ni prendre le contrôle de systèmes informatiques de l'État neutre pour conduire de telles opérations[84]. De son côté, l'État neutre doit empêcher tout usage des infrastructures informatiques situées sur son territoire ou sous son contrôle exclusif par des États belligérants. Néanmoins, il n'est pas tenu d'empêcher ces derniers d'utiliser ses réseaux informatiques à des fins de communication[85].

Le fait d'acheminer une cyber-opération constitutive d'une attaque via les systèmes d'un État neutre sans aucun effet sur celui-ci ne constitue pas une violation du droit de la neutralité lequel prohibe uniquement le passage physique de troupes ou de convois.

Le droit de la neutralité s'applique aux cyber-opérations. Les belligérants doivent s'abstenir de provoquer des effets dommageables sur les infrastructures numériques situées sur le territoire d'un État neutre ou de lancer une cyber attaque depuis ces infrastructures.

83 « [C]omme dans le cas des principes du droit humanitaire applicable dans les conflits armés, le droit international ne laisse aucun doute quant au fait que le principe de neutralité - quel qu'en soit le contenu - qui a un caractère fondamental analogue à celui des principes et règles humanitaires, s'applique (sous réserve des dispositions pertinentes de la Charte des Nations unies) à tous les conflits armés internationaux, quel que soit le type d'arme utilisé », Licéité de la menace ou de l'emploi d'armes nucléaires, avis consultatif, C.I.J Recueil 1986, p. 31, § 89.

84 Article 1 des Conventions V et XIII concernant les droits et les devoirs des Puissances neutres en cas de guerre maritime, La Haye, 18 octobre 1907.

85 Article 8 de la Convention V concernant les droits et les devoirs des Puissances neutres en cas de guerre maritime, La Haye, 18 octobre 1907.

GLOSSAIRE

Cyber-arme

Moyen(s) numérique(s), à l'inclusion des armes, des moyens et des méthodes de guerre numériques, mis en œuvre dans une cyber-opération menée à l'encontre de la partie adverse en contexte de conflit armé et en lien avec celui-ci.

Cyberattaque

Action volontaire, offensive ou malveillante, menée au travers du cyberespace et destinée à provoquer un dommage (en disponibilité, intégrité ou confidentialité) aux données ou aux systèmes qui les traitent, pouvant ainsi nuire aux activités dont ils sont le support. Une cyberattaque peut être une cyber-opération conduite par un Etat contre les intérêts de l'Etat français.

Cyberdéfense

Ensemble des mesures techniques et non techniques mis en place par un État pour défendre dans le cyberespace les systèmes d'information jugés d'importance vitale, qui contribuent à assurer la cybersécurité.

Cyberdéfense militaire

Ensemble coordonné d'actions défensives et offensives menées dans le cyberespace lors de la planification, de la préparation ou de la conduite d'opérations militaires. Elle s'articule autour de six grandes missions : prévenir, anticiper, protéger, détecter, réagir et attribuer.

Cyberespace

Espace de communication constitué par l'interconnexion mondiale d'infrastructures et d'équipements de traitement automatisé de données numériques et par les objets qui y sont connectés et les données qui y sont traitées.

Cyber-opérations

Actions de lutte informatique défensive (LID), de lutte informatique offensive (LIO), ou de cyber renseignement.

Cybersécurité

État recherché pour un système d'information lui permettant 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.

Infrastructures critiques

Infrastructures qui fournissent des biens et des services indispensables à la Nation, ou pour lesquelles des atteintes à la disponibilité, à l'intégrité ou à la confidentialité peuvent présenter un danger grave, notamment pour la population.

Lutte informatique défensive (LID)

Ensemble coordonné d'actions menées par un État qui consiste à détecter, à analyser et à prévenir des cyberattaques, et à y réagir le cas échéant.

Lutte informatique offensive (LIO)

Ensemble des actions entreprises dans le cyberespace produisant des effets à l'encontre d'un système adverse, pour en altérer la disponibilité ou la confidentialité des données.