Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des affaires étrangères DFAE

Direction du droit international public (DDIP)

Prise de position de la Suisse : application du droit international dans le cyberespace

Annexe GEG 2019/2021

Introduction

Dans les travaux du groupe d'experts gouvernementaux des Nations Unies chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale pour la période 2019-2021 (nommé ci-après « le GEG »), la dimension de politique de sécurité de l'espace numérique (cybersécurité) et les règles du droit international applicables dans ce contexte sont au premier rang des préoccupations des États[1]. La notion de cyberespace désigne la partie de l'espace numérique qui concerne la dimension de politique de sécurité. La prise de position de la Suisse traite d'abord de questions liées au droit international général, y compris les droits de l'homme (partie I), puis se concentre sur des questions relevant du droit international humanitaire (partie II).

La Suisse œuvre à bâtir et à garantir un cyberespace ouvert, libre, sûr et pacifique, et à promouvoir la reconnaissance, le respect et l'application du droit international dans cet espace[2]. Il est dans l'intérêt conjoint de tous les États de s'assurer que le cyberespace est régi selon les principes de l'état de droit et que l'utilisation qui en est faite est pacifique. Du point de vue de la Suisse, le droit international s'applique dans le cyberespace. La Suisse se félicite donc du consensus des GEGs précédents approuvé par les États membres de l'Assemblée générale des Nations Unies[3], selon lequel le droit international et en particulier la Charte des Nations Unies s'applique dans son intégralité dans le cyberespace[4]. Elle salue aussi la confirmation de ce consensus dans le rapport du 18 mars 2021[5] du groupe de travail à composition non limitée 2019-2021.

---

1 Concernant l'engagement de la Suisse en faveur d'une réglementation internationale applicable à l'espace numérique en général, se référer à la stratégie de politique extérieure numérique 2021-2024 et en particulier à l'annexe 4. (https://www.eda.admin.ch/dam/eda/fr/documents/publications/SchweizerischeAussenpolitik/20201104-strategie-digitalaussenpolitik_FR.pdf).

2 Objectif 4.4 de la stratégie de politique extérieure 2020-2023 et point 4.3 de la stratégie de politique extérieure numérique 2021-2024.

3 Résolution A/70/237.

4 Rapport 2013 (UNDOC A/68/98, par. 19) et rapport 2015 (UNDOC A/70/174, par. 24 et 28c) du groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale.

5 Rapport 2021 (UNDOC A/75/816, par. 8) du groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale.

La Suisse considère que les positions nationales des États contribuent de manière significative à concrétiser davantage l'application du droit international dans le cyberespace. Sa prise de position présente un aperçu général de la question, qui n'est ni définitif ni complet. Outre les positions nationales, il est essentiel de continuer à clarifier la manière dont le droit international est applicable dans le cyberespace. L'application concrète du droit international dans le cyberespace passe aussi et surtout par des échanges étroits entre les États dans un cadre multilatéral. Comme l'appréciation d'un cyberincident du point de vue du droit international n'est possible qu'à la lumière de ses circonstances concrètes, les règles du droit international évoquées ci-après doivent être interprétées et appliquées au cas par cas.

Les règles évoquées ci-après revêtent une importance particulière dans le contexte de la cybersécurité.

I. Droit international général

1. Règlement pacifique des différends

Conformément à l'art. 2, par. 3, et à l'art. 33 de la Charte des Nations Unies, les différends susceptibles de menacer le maintien de la paix et de la sécurité internationales doivent être réglés par des moyens pacifiques, comme une démarche diplomatique, ne arbitrage ou la saisine de la Cour internationale de Justice (CIJ). En tant que pays neutre avec un engagement et une expérience de longue date dans le domaine des bons offices, la Suisse s'investit afin que le principe du règlement pacifique des différends soit respecté dans le cyberespace également, soulignant ainsi que l'objectif premier est l'utilisation pacifique de cet espace. Elle salue donc le fait que le rapport 2015 du GEG et le rapport du groupe de travail à composition non limitée 2019-2021 ont confirmé que le règlement pacifique des différends, qui est l'un des principes centraux de la Charte des Nations Unies, s'applique également dans le cyberespace. Les différends dans le cyberespace doivent donc y être réglés par des moyens pacifiques et non par des mesures unilatérales.

2. Souveraineté

La souveraineté est un principe fondamental du droit international. D'une part, elle désigne la compétence des États à déterminer, appliquer et imposer leur ordre juridique dans les limites de leur territoire. D'autre part, elle implique que les États coexistent indépendamment les uns des autres et sur un pied d'égalité. Il découle du principe de souveraineté que chaque État a droit au respect de son intégrité territoriale et qu'il est protégé contre toute ingérence[6]. Chaque État doit de fait ne pas porter atteinte à la souveraineté d'un autre État[7]. De la souveraineté découle donc une règle primaire et contraignante du droit international, dont la violation constitue un acte contraire au droit international et engage la responsabilité de l'État auquel l'acte est attribué.

La souveraineté étatique s'applique également dans le cyberespace[8]. Comme ce dernier ne connaît pas de frontières territoriales clairement délimitées, la concrétisation du principe de souveraineté y représente un défi particulier. La question est notamment de savoir quels États

---

6 Affaire de l'île de Palmas (1928), p. 838. Sous la notion d'indépendance, l'art. 2, al. 1, de la Constitution fédérale de la Confédération suisse reconnaît à un État souverain au sens du droit international la compétence exclusive de définir et d'imposer le droit qui s'applique sur l'ensemble de son territoire.

7 Activités militaires et paramilitaires au Nicaragua et contre celui-ci, arrêt, CIJ Recueil 1986, par. 292.

8 Rapports 2013 (par. 20) et 2015 (par. 27 et 28b) du GEG

exercent leur juridiction sur des données numériques ou ont accès à de telles données. Il convient également de s'intéresser au contrôle légitime des données numériques et au droit d'accéder à des données qui, selon les circonstances, peuvent être stockées sur un autre territoire ou dont la localisation géographique n'est pas possible. En matière de cybersécurité, le principe de souveraineté appliqué aux relations entre États permet toutefois d'identifier différents domaines protégés contre les cyberopérations. Ainsi, la souveraineté protège l'infrastructure des technologies de l'information et de la communication (TIC) située sur le territoire de l'État souverain contre les intrusions non autorisées et les dégâts matériels. Sont donc protégés les réseaux informatiques, les systèmes et les logiciels qui composent les infrastructures TIC, qu'elles soient privées ou publiques.

La Suisse reconnaît que la concrétisation de ce qui constitue, dans le cyberespace, une violation d'un domaine protégé par la souveraineté étatique représente un défi particulier et n'est pas encore définitivement tranchée. De son point de vue, l'appréciation d'une telle violation doit notamment se fonder sur deux critères. Il convient de vérifier, d'une part, si l'incident viole l'intégrité territoriale d'un État et, d'autre part, s'il constitue une ingérence dans une fonction intrinsèque de cet État, voire une appropriation illicite de celle-ci. La compréhension exacte de ces critères est une question d'interprétation devant faire l'objet de discussions. Doivent notamment être discutés les cas dans lesquels le fonctionnement d'une infrastructure ou de son matériel connexe est altéré ou limité, les cas dans lesquels la modification ou la suppression de données entrave l'exécution de fonctions intrinsèques de l'État (p. ex. fourniture de prestations sociales, tenue d'élections et de votations, prélèvement de l'impôt) et les cas dans lesquels un État, par l'emploi coordonné de méthodes légales et illégales dans le cyberespace (p. ex. propagande, désinformation, opérations secrètes des services de renseignements), tente d'influencer, de perturber ou de retarder des processus décisionnels démocratiques dans un autre État. L'appréciation du cas individuel considéré dépend de la nature du cyberincident et de ses conséquences.

3. Non-intervention

Le principe de non-intervention découle du principe de l'égalité souveraine des États (art. 2, par. 1, de la Charte des Nations Unies) et fait partie intégrante du droit international coutumier[9]. Par intervention, on désigne l'ingérence directe ou indirecte d'un État, par des moyens de contrainte, dans les affaires intérieures ou extérieures d'un autre État. Sont visées les affaires relevant de la compétence exclusive de l'État (domaine réservé). Le domaine protégé par le principe de non-intervention englobe notamment les affaires intérieures d'un État que sont le choix de son système politique, économique, social et culturel et l'élaboration de sa politique extérieure. Contrairement à la violation de souveraineté, la violation du principe de non-intervention suppose un élément de contrainte : par son intervention, un État tente d'amener un autre État à agir (action ou omission) autrement qu'il ne l'aurait fait en l'absence de cette contrainte[10]. Ainsi, le seuil de violation du principe de non-intervention est sensiblement plus élevé que celui d'une violation de souveraineté.

Le principe de non-intervention s'applique également dans le cyberespace, où les actes d'un État peuvent constituer, si les conditions correspondantes sont réunies, outre une violation de souveraineté, une ingérence politique ou économique non autorisée dans les affaires

---

9 Déclaration A/RES/2625 (XXV) du 24 octobre 1970 relative aux principes du droit international touchant les relations amicales et la coopération entre les États conformément à la Charte des Nations Unies ; Activités militaires et paramilitaires au Nicaragua et contre celui-ci, arrêt, CIJ Recueil 1986, par. 202.

10 Activités militaires et paramilitaires au Nicaragua et contre celui-ci, arrêt, CIJ Recueil 1986, par. 202.

intérieures ou extérieures d'un autre État. Ils peuvent enfreindre ainsi le principe de non-intervention du droit international[11]. La limite entre l'action autorisée et la contrainte illicite doit être appréciée au cas par cas. Cela concerne en particulier la contrainte de nature économique, qui consiste par exemple à paralyser des entreprises d'importance systémique par l'intermédiaire d'une cyberopération. Un examen individuel est nécessaire afin d'établir si la cyberopération comprend un élément de contrainte et, donc, si elle porte atteinte au principe de non-intervention.

4. Interdiction du recours à la force et droit de légitime défense

L'un des principes fondamentaux de la Charte des Nations Unies est l'interdiction de recourir à la force (art. 2, par. 4). Des exceptions sont prévues si le Conseil de sécurité des Nations Unies estime nécessaire l'emploi de la force (art. 42) ou si les conditions strictes qui encadrent l'exercice du droit de légitime défense sont réunies (art. 51).

L'interdiction de recourir à la force et le droit de légitime défense s'appliquent également dans le cyberespace. Le droit de légitime défense ne peut être exercé que si l'État intéressé a été victime d'une agression armée. Selon la jurisprudence de la CIJ, toute violation de l'interdiction de recourir à la force ne constitue pas systématiquement une agression armée. Seules sont concernées les formes les plus graves d'emploi de la force, ce qui signifie que l'intensité et les effets de l'agression doivent atteindre une certaine gravité[12]. Selon cette même jurisprudence, une agression armée ne doit pas nécessairement être commise à l'aide de moyens ou d'armes cinétiques, car le moyen employé ne constitue pas un critère déterminant[13]. Un État peut exercer son droit de légitime défense en réaction à un cyberincident qui, au vu de la gravité des dégâts matériels ou des dommages aux personnes (blessées ou tuées), s'apparente dans son intensité et ses effets à une agression armée cinétique. Il n'existe pas de seuils quantitatifs et qualitatifs contraignants au-delà desquels l'intensité et les effets d'un emploi de la force qualifient une agression armée. Les discussions visant à caractériser une agression armée dans le cyberespace tendent à assimiler son intensité et ses effets à ceux d'une attaque contre une infrastructure critique (p. ex. une centrale nucléaire ou un réseau électrique) causant des dommages considérables aux personnes et/ou aux biens matériels.

En cas d'agression armée, l'interprétation de l'interdiction de recourir à la force et du droit de légitime défense doit tenir compte des objectifs de la Charte des Nations Unies – à savoir le maintien et, s'il y a lieu, le rétablissement de la paix et de la sécurité internationales. Même en cas d'agression armée, seuls sont autorisés les actes qui sont nécessaires et proportionnés pour se défendre contre l'agresseur. Le droit de légitime défense s'applique jusqu'à ce que le Conseil de sécurité de l'ONU ait pris les mesures nécessaires pour maintenir la paix et la sécurité internationales (art. 51 de la Charte des Nations Unies). Si la légitime défense sort de ce cadre, elle constitue elle-même un emploi illicite de la force. Si le seuil de l'agression armée n'est pas franchi, l'État intéressé a droit de prendre des contre-mesures non violentes immédiates et proportionnées (cf. point 6.2).

---

11 Commentaires relatifs à l'ordonnance du 30 janvier 2019 sur la cyberdéfense militaire (OCMil, RS 510.921).
12 Activités militaires et paramilitaires au Nicaragua et contre celui-ci, arrêt, CIJ Recueil 1986, par. 195.
13 Licéité de la menace ou de l'emploi d'armes nucléaires, avis consultatif, CIJ Recueil 1996, par. 39.

5. Neutralité

La Suisse estime que les droits et les devoirs d'un État neutre dans le contexte d'un conflit armé international sont en principe applicables dans le cyberespace également[14]. L'État neutre a le devoir d'empêcher que l'utilisation de son territoire par une partie au conflit porte atteinte à sa neutralité, et les parties au conflit ont l'obligation de respecter son intégrité territoriale. Il s'ensuit que les parties au conflit ne sont pas autorisées à mener des cyberopérations en lien avec le conflit à partir d'installations situées sur le territoire d'un État neutre ou placées sous son contrôle exclusif[15]. Il leur est également interdit de prendre le contrôle de systèmes informatiques appartenant à l'État neutre pour conduire de telles opérations[16].

En raison de sa dimension transnationale globale, le cyberespace pose certaines limites aux droits et aux devoirs territoriaux des États neutres. Car s'il est possible d'interdire l'entrée d'un espace aérien à des aéronefs spécifiques, il est impossible de procéder de la même façon avec les données circulant sur Internet. D'autant que certaines données ne sont pas transmises uniquement par des câbles terrestres mais aussi par des satellites qui, parce qu'ils se situent dans l'espace, échappent au champ d'application du droit de la neutralité. Ces éléments doivent être pris en considération lorsque les droits et les devoirs des États neutres sont appliqués au cyberespace.

Il est fondamentalement interdit aux parties au conflit d'endommager les réseaux de données des pays neutres en raison des hostilités qu'elles mènent via les réseaux informatiques. Un État neutre n'est pas autorisé à soutenir les parties au conflit par l'envoi de troupes ou avec ses propres armes. Transposée aux cyberactivités militaires dans le contexte d'un conflit armé international, cette interdiction signifie qu'un pays neutre doit empêcher l'utilisation par les parties au conflit de ses propres systèmes et réseaux contrôlés militairement. En général, les réseaux militaires sont protégés et ne sont pas librement accessibles.

6. Responsabilité de l'État

Les règles sur la responsabilité de l'Etat reflètent essentiellement le droit international coutumier et sont largement reproduites dans le projet de la Commission du droit international[17]. Ces règles sont également applicables aux cyberincidents. Elles prévoient que tout fait internationalement illicite de l'État engage sa responsabilité internationale et donne droit à la réparation intégrale du préjudice. Cela ne s'applique que lorsqu'un comportement consistant en une action ou une omission est attribuable à l'État en vertu du droit international et constitue une violation d'une obligation internationale de l'État.

---

14 Licéité de la menace ou de l'emploi d'armes nucléaires, avis consultatif, CIJ Recueil 1996, par. 89 : « La Cour estime que, comme 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. »

15 Art. 2 et 3 de la Convention du 18 octobre 1907 concernant les droits et les devoirs des Puissances et des personnes neutres en cas de guerre sur terre (RS 0.515.21) et art. 2 et 5 de la Convention du 18 octobre 1907 concernant les droits et les devoirs des Puissances neutres en cas de guerre maritime (RS 0.515.22).

16 Art. 1 de la Convention du 18 octobre 1907 concernant les droits et les devoirs des Puissances et des personnes neutres en cas de guerre sur terre (RS 0.515.21).

17 Projet d'articles de la CDI sur la responsabilité de l'État pour fait internationalement illicite (août 2001)

6.1. Attribution

L'attribution d'un cyberincident relevant de la politique de sécurité suppose d'identifier l'auteur de l'acte au moyen d'une procédure interdisciplinaire globale qui analyse les caractéristiques techniques et juridiques de l'incident, prend en considération le contexte géopolitique et utilise l'ensemble des activités de renseignements pour acquérir des informations. Sur cette base, l'État lésé par l'incident peut l'attribuer, publiquement ou non, à un autre État ou à un acteur privé et décider d'autres mesures politiques.

L'attribution du point de vue juridique est un volet de l'analyse décrite ci-dessus. Elle détermine si le cyberincident peut être juridiquement attribué à un autre État en vertu du droit international, si la responsabilité de cet autre État peut être engagée en application des règles énoncées par la CDI et comment l'État lésé est autorisé à y répondre dans les limites du droit international (cf. point 6.2 concernant les contre-mesures). Le comportement des organes de l'État et des personnes ou entités habilitées par le droit de cet État à exercer des prérogatives de puissance publique est considéré comme un fait de l'État d'après le droit international[18]. Un cyberincident causé par un acteur non-étatique peut également être attribué à l'État si cet acteur agit en fait sur les instructions d'un l'État, ou sous la direction ou le contrôle de celui-ci. [19]. Ce comportement de l'acteur non-étatique doit alors être considéré comme un fait de l'État, ce qui autorise le pays lésé à prendre des contre-mesures (cf. point 6.2). En vertu du droit international, toute contre-mesure envers un autre État suppose toutefois que l'incident ait une dimension interétatique.

Les décisions découlant d'une telle attribution sont laissées à l'appréciation de l'État lésé. Le droit international n'impose aucunement à cet État de rendre publiques les informations l'ayant conduit à prendre ces décisions. Pour autant, toute accusation d'organiser et d'exécuter des actes illicites portée contre un État doit être étayée[20] .

6.2. Contre-mesures

Un État lésé par les actes indésirables d'un autre État dans le cyberespace doit réagir de manière proportionnée et propre aux faits d'espèce.

L'État lésé est autorisé à user de rétorsion dans tous les cas, que l'acte indésirable constitue ou non une violation du droit international. Les mesures de rétorsion se définissent comme des mesures hostiles mais conformes au droit international, prises en réaction à la commission d'un acte indésirable par un autre État. Il s'agit ordinairement de refuser un accord commercial intéressant pour cet autre État, de rappeler son ambassadeur ou, en dernier recours, de rompre les relations diplomatiques avec cet État.

Si l'acte est juridiquement attribué et s'il est contraire au droit international, l'État lésé est autorisé à prendre des contre-mesures dans le respect des règles de la CDI définissant la responsabilité de l'État[21]. Les contre-mesures sont des mesures intrinsèquement contraires au droit international, qui se justifient toutefois lorsqu'un État réagit à une violation préalable du droit international par un autre État. Les contre-mesures ne peuvent néanmoins porter

---

18 Art. 4 et 5 du Projet d'articles de la CDI (août 2001).
19 Art. 8 du Projet d'articles de la CDI (août 2001).
20 Rapport 2015 du GEG (par. 28f).
21 Projet d'articles de la CDI sur la responsabilité de l'État pour fait internationalement illicite (août 2001). Si tant est qu'elles ne soient pas interdites par le droit international, les contre-mesures sont assorties de conditions strictes.

aucune atteinte à certaines obligations fondamentales telles que l'interdiction du recours à la force, la protection des droits de l'homme fondamentaux et l'obligation de respecter les normes du droit international humanitaire, les règles de *ius cogens* et le principe d'inviolabilité des missions diplomatiques et consulaires[22]. Il est donc exclu de faire usage de la force militaire, c'est-à-dire de prendre des mesures conduisant à la perte de vies humaines.

Les contre-mesures doivent toujours avoir pour but d'amener l'autre État, par l'imposition de sanctions (juridiques), à faire cesser son comportement violant le droit international et/ou à le réparer. En principe, elles ne peuvent être mises en œuvre que si elles ont été annoncées et si l'autre État a été préalablement enjoint de faire cesser son comportement. Dans le contexte des cyberopérations, il est possible de déroger à cette règle si l'État lésé doit prendre des contre-mesures immédiates afin de préserver ses droits et d'éviter d'autres dommages. Dans tous les cas, les contre-mesures doivent être proportionnelles au préjudice subi.

Les contre-mesures en réaction à un cyberincident ne doivent pas nécessairement être prises dans le domaine cyber : d'après les règles définissant la responsabilité de l'État, d'autres types de contre-mesure sont autorisés pour amener l'autre État à s'acquitter des obligations qui lui incombent en vertu du droit international. Si les contre-mesures interviennent dans le domaine cyber, elles ne doivent pas nécessairement viser le système informatique à l'origine de l'incident. D'autres cybermesures sont possibles pourvu qu'elles aient pour objectif d'amener l'autre État à faire cesser le comportement à l'origine de la violation du droit international. En fonction des circonstances concrètes de l'incident, le droit international autorise par exemple l'État lésé à bloquer l'exécution à l'étranger du système informatique incriminé ; dans certains cas individuels, il peut également l'autoriser à porter atteinte à des systèmes informatiques à l'étranger qui ne sont pas eux-mêmes à l'origine du cyberincident.

Conformément aux règles de la CDI sur la responsabilité de l'État, certaines circonstances spéciales peuvent exclure l'illicéité d'un fait de l'État non conforme à l'une de ses obligations internationales. Tel est notamment le cas si un tel fait de l'État constitue pour lui le seul moyen de protéger un intérêt essentiel contre un péril grave et imminent. Dans le cadre strict des exceptions prévues par les règles de la CDI, l'État peut déroger à des obligations internationales dans le contexte de cyberopérations également[23].

6.3. Devoir de diligence

Du point de vue de la Suisse, le devoir de diligence est un principe établi de longue date qui fait aujourd'hui partie intégrante du droit international coutumier et s'applique également dans le cyberespace. La CIJ décrit ce standard général de comportement comme « l'obligation, pour tout État, de ne pas laisser utiliser son territoire aux fins d'actes contraires aux droits d'autres États »[24]. Le devoir de diligence est fidèle aux principes fondamentaux du droit international que sont notamment la souveraineté étatique, l'égalité, l'intégrité territoriale et la non-ingérence.

---

22 Art. 50 du Projet d'articles de la CDI sur la responsabilité de l'État pour fait internationalement illicite (août 2001).

23 Chap. V du Projet d'articles de la CDI sur la responsabilité de l'État pour fait internationalement illicite (août 2001).

24 Affaire du détroit de Corfou, arrêt du 9 avril 1949, CIJ Recueil 1949, p. 22. Le devoir de diligence est d'une part un principe général du droit international reconnu comme coutumier et, d'autre part, une obligation ancrée, concrétisée et développée dans des traités internationaux relevant de différents domaines (p. ex. droit de l'environnement, droits de l'homme, droit international humanitaire, droit international de la santé).

Ce principe s'applique aussi dans le cyberespace. Un État qui a ou devrait avoir connaissance de tels actes doit prendre toutes les mesures adéquates et raisonnables en son pouvoir pour faire cesser les cyberincidents contraires aux droits d'autres États ou pour minimiser leurs risques. Le devoir de diligence est un standard variable qui dépend des capacités et des possibilités de chaque État et des circonstances particulières de chaque cas. Il oblige l'État souverain à engager tous les moyens raisonnables à sa disposition pour empêcher que des activités menées sur son territoire ou dans une zone sous son contrôle effectif portent des préjudices graves à un autre État. En ce sens, le devoir de diligence est une obligation de comportement et non de résultat. Si les conditions énoncées sont réunies, le droit international oblige l'État responsable à combler immédiatement les failles de protection et à contribuer, par son aide, à lutter contre l'incident et à le tracer.

Le devoir de diligence concerne en particulier les situations dans lesquelles les droits d'autres États sont enfreints par des actes commis par des entités privées (p. ex. des groupes de hackers) qu'il n'est pas possible d'imputer clairement à l'État selon le principe d'attribution décrit au point 6.1. Si l'État responsable ne remplit pas le devoir de diligence exigé de lui en pareille situation, l'État lésé peut prendre des contre-mesures conformes aux règles de la CDI sur la responsabilité de l'État afin de l'amener à remplir ses obligations. Ces contre-mesures correspondent aux différentes options présentées ci-dessus et peuvent être prises dans le domaine cyber ou en dehors. L'État responsable peut par ailleurs être tenu de réparer le préjudice[25].

7. Droits de l'homme

Les droits de l'homme sont un pilier central du droit international. Ils sont garantis par différents traités internationaux dont le Pacte des Nations Unies relatif aux droits civils et politiques (Pacte II de l'ONU) et la Convention européenne des droits de l'homme (CEDH). Les droits de l'homme fondamentaux font également partie intégrante du droit international coutumier et constituent pour partie des normes impératives (*ius cogens*). Aujourd'hui, les droits de l'homme imposent aux États de s'abstenir de toute ingérence dans les droits de l'homme garantis aux individus (*obligation de respecter*), de protéger ces droits contre l'ingérence de tiers (*obligation de protéger*) et de prendre des mesures positives pour faciliter l'exercice de ces droits (*obligation de mettre en œuvre*).

Les droits de l'homme s'appliquent aussi dans l'espace numérique et sont un pilier central de la réglementation internationale en matière de numérisation. Quelles que soient les activités numériques considérées, les individus disposent des mêmes droits que dans l'espace physique. Cette règle s'applique également aux activités de politique sécuritaire que les États mènent dans le cyberespace, autrement dit dans un domaine partiel de l'espace numérique : lorsqu'ils opèrent dans le cyberespace, les États sont tenus de remplir leurs obligations en matière de droits de l'homme exactement comme dans l'espace physique – y compris lorsque ces cyberopérations sont extraterritoriales (dès lors que les États exercent ce faisant leur souveraineté). Si des cyberactivités aboutissent à une violation des droits de l'homme, les individus lésés disposent en principe des mêmes mécanismes d'exécution prévus par le droit international et applicables à l'échelle nationale que si la violation avait été commise dans l'espace physique. Dans ce domaine, la pratique des organes internationaux de contrôle et juridictionnels est appelée à se développer en tenant compte de la portée et de l'applicabilité des droits de l'homme.

---

[25] Art. 31 du Projet d'articles de la CDI sur la responsabilité de l'État pour fait internationalement illicite (août 2001).

Certains droits de l'homme spécifiques peuvent être particulièrement concernés par des cyberopérations et autres mesures liées au domaine cyber, dans le sens où elles peuvent par exemple limiter le droit des individus à avoir accès à des informations, à préserver leur vie privée ou à exprimer librement leur opinion.

Les règles selon lesquelles un État peut justifier une restriction des droits de l'homme dans le cyberespace sont identiques aux règles applicables dans l'espace physique. Cela signifie que la restriction doit avoir une base légale suffisante et que l'État doit établir au moyen d'une pesée des intérêts que son ingérence est adaptée, nécessaire et raisonnable pour atteindre le but légitime visé.

S'il ne fait aucun doute pour la Suisse que les droits de l'homme s'exercent également dans le cyberespace, l'application de ce principe au cas par cas soulève toutefois de nouvelles questions. Prenons l'exemple d'une cyberactivité bloquant l'accès à des médias sociaux : s'agit-il d'une ingérence dans le bien public protégé qu'est la liberté d'expression ? Si oui, à partir de quel stade ? Le droit à la liberté d'expression peut-il s'exercer par d'autres moyens de communication ? Dans quelle mesure les acteurs privés sont-ils liés par les droits de l'homme ? Afin de garantir le respect des droits de l'homme dans le cyberespace, les instances compétentes en charge de cette thématique doivent encore mener des travaux complémentaires.

II. Droit international humanitaire

Du point de vue de la Suisse, le droit international est applicable au cyberespace, ce qui est également valable pour le droit international humanitaire (DIH) dans le contexte de conflits armés. Le respect, le renforcement et la promotion du DIH sont des priorités de la politique extérieure de la Suisse – pays qui se caractérise par sa neutralité, sa tradition humanitaire et son statut d'État dépositaire des Conventions de Genève. C'est pour cette raison que la Suisse examine plus en profondeur la question du DIH dans la présente prise de position.

1. Applicabilité du DIH

Le DIH est applicable lorsqu'un conflit armé, international ou non-international, existe de fait. Il s'applique à tous les types de conflits armés et à l'ensemble des parties au conflit. Il s'intéresse aux réalités des conflits, indépendamment des motifs ou de la licéité du recours à la force. Il n'apporte aucune réponse à la question de la licéité des conflits et ne légitime aucunement l'emploi de la force entre États[26]. Le DIH a pour but de réglementer la conduite des hostilités et de protéger les victimes de conflits armés, principalement en limitant l'utilisation des méthodes et moyens de guerre. Selon la CIJ, les principes et règles établis du DIH s'appliquent « à toutes les formes de guerre et à toutes les armes, celles du passé, comme celles du présent et de l'avenir »[27].

---

[26] Tout recours à la force entre États est réglementé par la Charte des Nations Unies et par le droit international coutumier applicable (cf. point 4 ci-dessus).

[27] Licéité de la menace ou de l'emploi d'armes nucléaires, avis consultatif, CIJ Recueil 1996, par. 86.

Cela est valable pour le cyberespace de la même manière que pour les théâtres d'opérations conventionnels ou nouveaux (p. ex. espace, air, sol, espace maritime, espace électromagnétique, espace de l'information). Ainsi, le DIH est la principale branche du droit international réglementant les cyberopérations en situation de conflits armés. Sa mise en œuvre effective contribue à garantir la sécurité internationale. Le DIH existant, et en particulier ses principes fondamentaux, posent d'importantes limites à l'exécution de cyberopérations dans le contexte de conflits armés.

2. Dispositions fondamentales du DIH réglementant la conduite des hostilités

2.1. Principe relatif aux méthodes et moyens de guerre

Le DIH restreint ou interdit les méthodes et moyens (armes) de guerre en fixant d'une part des principes généraux qui réglementent les comportements et prohibent la production de certains effets et, d'autre part, des règles spécifiques qui s'appliquent à des méthodes et moyens de guerre en particulier. S'agissant des armes, le DIH fait une distinction entre la licéité de l'arme elle-même (*weapons law*) et la licéité liée à son emploi (*law of targeting*). Les caractéristiques inhérentes à certaines catégories d'armes impliquent que leur utilisation - dans certaines ou toutes les circonstances - est illégale en soi. Pour l'ensemble des autres armes, la licéité de l'emploi dépend de sa conformité avec le DIH.

Cela s'applique également dans le cyberespace. En effet, le développement et l'emploi de nouvelles méthodes et moyens de guerre doivent respecter le droit international en vigueur, et en particulier le DIH. Il en va également ainsi si l'arme n'est pas couverte par une norme spécifique et si les dispositions conventionnelles réglementant la conduite des hostilités ne se rapportent pas expressément aux nouvelles technologies. Les règles coutumières du DIH sont applicables de manière égale à l'ensemble des méthodes et moyens de guerre, donc également dans le cyberespace. En effet, selon un principe établi de longue date, le droit des parties à un conflit armé de choisir les méthodes ou moyens de guerre n'est pas illimité.

2.2. Licéité d'un type particulier d'armes

En application du DIH, les méthodes et moyens de guerre qui présentent une ou plusieurs des caractéristiques suivantes sont intrinsèquement illicites :

la méthode ou le moyen de guerre

(1) est de nature à causer des maux superflus ;
(2) produit des effets indiscriminés parce qu'il ne peut pas être dirigé vers un objectif militaire déterminé~~e~~ ou parce que ses effets ne peuvent pas être limités de la manière prescrite par le DIH ;
(3) est conçu pour causer, ou dont on peut attendre qu'il causera, des dommages étendus, durables et graves à l'environnement naturel ; *ou*
(4) est expressément interdit par le droit conventionnel ou le droit coutumier.

Cela s'applique également dans le cyberespace et donc aux méthodes et moyens de guerre relevant du domaine cyber.

2.3. Licéité de l'emploi des méthodes et moyens de guerre

En ce qui concerne l'utilisation licite des moyens et méthodes de guerre cybernétiques, les règles et principes régissant la conduite des hostilités doivent être respectés. Cela signifie que les belligérants doivent respecter en particulier les principes de distinction, de proportionnalité et de précaution, c'est-à-dire :

(1) distinguer les objectifs militaires, d'une part, et la population civile ou les biens civils, d'autre part, en présumant du caractère civil en cas de doute ;
(2) évaluer si les dommages potentiels pour la population civile ou les biens civils ne seraient pas disproportionnés par rapport à l'avantage militaire direct et concret attendu ;
(3) prendre toutes les mesures de précaution pratiquement possibles afin que les personnes et les biens protégés soient épargnés par les conséquences des opérations militaires.

Cela s'applique également dans le cyberespace lorsque des méthodes et moyens de guerre relevant du domaine cyber sont utilisés. Ces principes s'appliquent en particulier aux cyberopérations assimilables à une attaque au sens du DIH, c'est-à-dire aux actes de violence contre l'adversaire, que ces actes soient offensifs ou défensifs. Ce qui constitue une « attaque cyber » dans le contexte d'un conflit armé reste toutefois à clarifier. Cela comprend pour le moins des cyberopérations dont on peut raisonnablement s'attendre qu'elles auront pour effet direct ou indirect de blesser voire de tuer des personnes et/ou d'endommager physiquement voire de détruire des biens. En l'absence de tels dégâts physiques, un des défis qui demeure est de savoir dans quelle mesure les données sont protégées. Dans la pratique, un acteur conscient de ses responsabilités devrait pouvoir estimer les effets possibles de ses actions et les dégâts y relatifs. Mais comme cette estimation dépend notamment des informations disponibles au moment de décider d'une opération, l'obligation de prendre toutes les mesures de précaution pratiquement possibles pour épargner la population et les biens civils avant d'employer des méthodes et des moyens de guerre dans le domaine cyber joue de fait un rôle particulièrement important.

3. Autres dispositions du DIH

L'obligation de respecter pleinement le DIH ne se limite pas aux règles et aux principes régissant la conduite des hostilités. Il existe d'autres règles spécifiques du DIH qui doivent être respectées, y compris lors d'opérations militaires ne constituant pas une « attaque ». C'est notamment le cas des personnes et des biens bénéficiant d'une protection spéciale. Par exemple, le personnel médical, religieux ou humanitaire et les biens y associés doivent être respectés et protégés en toutes circonstances.

Cela s'applique également dans le cyberespace. Les cyberopérations affectant des catégories de personnes ou d'objets particulièrement protégées ou d'autres aspects réglementés par le DIH doivent tenir compte de toutes les règles spécifiques applicables.

4. Garantie du respect du DIH

Les États et les parties à un conflit ont l'obligation fondamentale de « respecter et faire respecter » le DIH en toutes circonstances. Il est incontesté que des mesures préparatoires doivent être prises pour permettre la mise en œuvre du DIH et que sa mise en œuvre doit être surveillée. Ainsi, les États et les parties à un conflit doivent notamment prendre des mesures

afin de s'assurer que le développement et l'emploi de méthodes et de moyens de guerre respectent strictement le DIH et pour éviter toute conséquence contraire au droit.

Cela s'applique également au cyberespace et donc aux méthodes et moyens de guerre relevant du domaine cyber. Comme pour toute autre arme, méthode ou moyens de guerre, les États ont l'obligation positive, lorsqu'ils les étudient, mettent au point, acquièrent ou adoptent, de déterminer si leur emploi serait susceptible, dans certaines ou en toutes circonstances, de contrevenir au droit international existant. Dans cette optique, l'obligation de déterminer la conformité des nouvelles armes avec le DIH conformément à l'art. 36 du Protocole additionnel aux Conventions de Genève[28] constitue un élément important pour empêcher ou limiter le développement et l'emploi de nouvelles cyberarmes qui, en particulier, ne rempliraient pas les conditions précitées.

[28] Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux (Protocole I), RS 0.518.521.