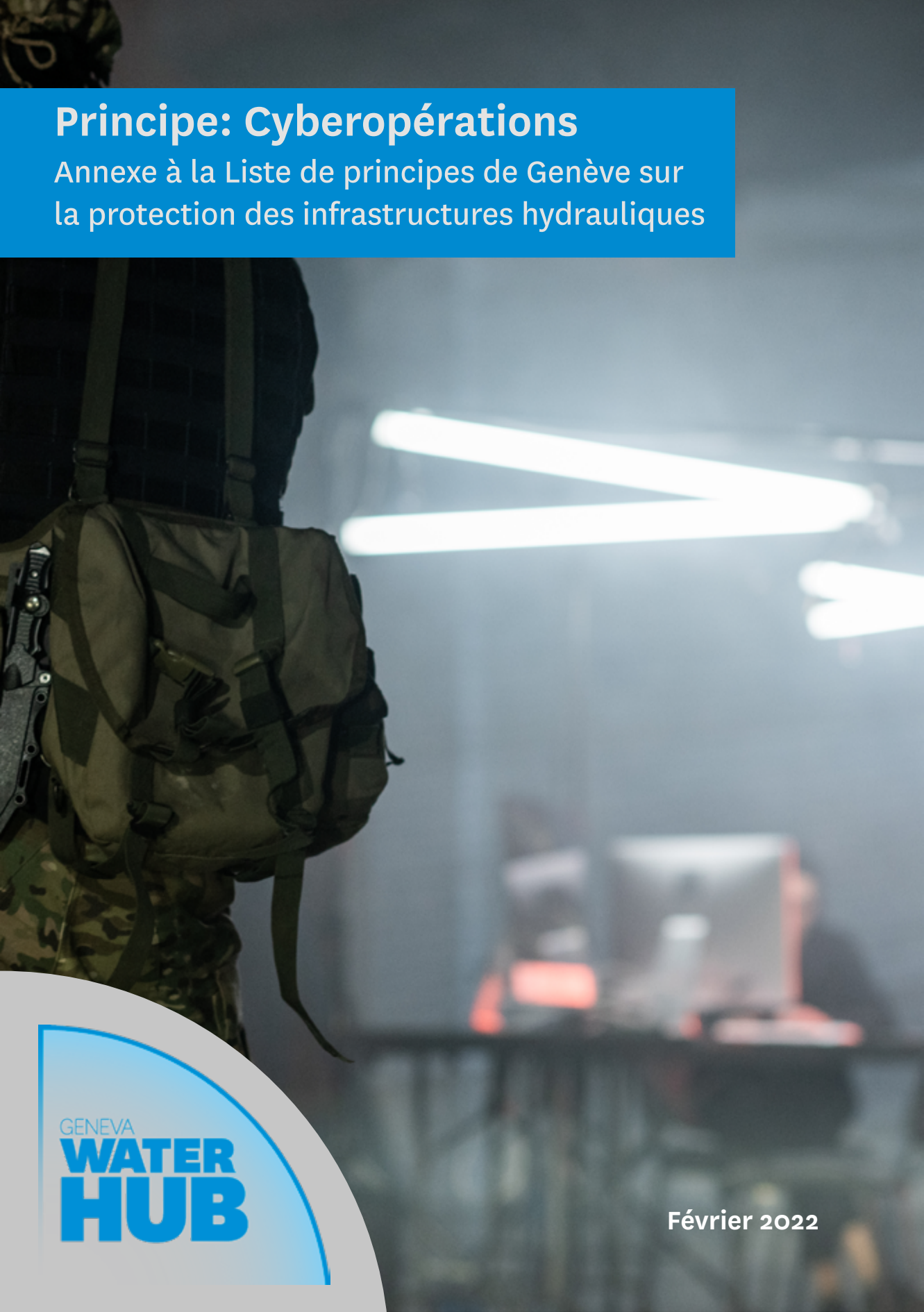
Principe: Cyberopérations

Annexe à la Liste de principes de Genève sur la protection des infrastructures hydrauliques



GENEVA WATER HUB

Février 2022

Crédit photo
Vue arrière de deux hommes en uniforme militaire en Getty Images/iStockphoto

Principe : Cyberopérations

Annexe à la Liste de principes de Genève sur la protection des infrastructures hydrauliques

Février 2022

Note d'introduction

Les progrès technologiques et la numérisation du secteur de l'eau ont accru sa vulnérabilité aux cyberattaques qui pourraient contaminer, perturber les systèmes de traitement et d'approvisionnement, ou libérer les eaux des barrages. Par exemple, en février 2021, des pirates informatiques ont fait irruption dans l'usine de traitement de l'eau de la ville d'Oldsmar (en Floride) et ont modifié les niveaux de produits chimiques, rendant l'eau impropre à la consommation.

De même, en 2020, Israël a affirmé qu'il y avait eu des tentatives de cyberattaques contre ses usines de traitement de l'eau et ses systèmes d'irrigation agricole. Ces nouvelles typologies d'attaques contre les systèmes et infrastructures d'eau présentent un risque réel et important pour la vie humaine, l'économie et la sécurité des États. Ainsi, il est clairement nécessaire de réglementer les menaces émanant de telles attaques.

En 2017, le Panel mondial de haut niveau sur l'eau et la paix, une initiative de quinze pays, a souligné la nécessité de renfocer les règles de droit international protégeant les infrastructures hydrauliques pendant les conflits armés. À cette fin, le Geneva Water Hub a élaboré la Liste de principes de Genève sur la protection des infrastructures hydrauliques (les Principes de Genève). Les Principes de Genève systématisent les principales règles applicables à la protection des infrastructures hydrauliques pendant les conflits armés, notamment dans la conduite des hostilités et des situations post-conflit, et formulent des recommandations qui vont au-delà du droit existant.

Dans le contexte des conflits armés, le droit international humanitaire (DIH), qui, entre autres, fixe des limites aux moyens et méthodes de guerre, qu'ils soient cinétiques ou cybernétiques, et protège les civils et les biens civils, y compris les infrastructures hydrauliques et les infrastructures liées à l'eau. Ainsi, les parties aux conflits armés ne doivent pas perturber le fonctionnement des infrastructures hydrauliques et des infrastructures liées à l'eau par le biais de cyberopérations. Ils doivent prendre toutes les précautions possibles pour éviter tout dommage accidentel à ces installations et infrastructures connexes.

Cependant, dans les Principes de Genève, il n'y a pas de principe distinct dédié aux cyberopérations. Notant les menaces émergentes en matière de cybersécurité, l'évolution des cybercapacités militaires et la vulnérabilité du secteur de l'eau, le Geneva Water Hub a développé un principe sur les « Cyberopérations » traitant de la protection des infrastructures hydrauliques et des infrastructures liées à l'eau. Le principe transpose principalement les règles et principes existants du DIH concernant la conduite des hostilités à ce nouveau domaine. Le principe indique également que d'autres branches du droit international, telles que le droit relatif aux droits de l'homme, pourraient fournir une protection.

En juin 2021, le Geneva Water Hub et l'Académie de droit international humanitaire et des droits de l'homme de Genève ont organisé conjointement un atelier sur les **« Cyberopérations et la protection de l'eau ».** L'atelier a fait le point sur la pratique du droit international en matière de cybersécurité et s'est concentré sur la manière dont le droit applicable aux cyberopérations interagit avec l'eau et la protection des infrastructures liées à l'eau. Le principe, avec son commentaire, a été discuté au cours de l'atelier, et les contributions du Comité international de la Croix-Rouge (CICR), des praticiens de la cybersécurité, des conseillers militaires et des experts universitaires ont été intégrées. Le Geneva Water Hub saisit cette occasion pour exprimer sa gratitude à tous les participants à l'atelier pour leurs précieuses contributions.

Principe : Cyberopérations

1. Les infrastructures hydrauliques et les infrastructures liées à l'eau ne doivent pas être attaquées, y compris lors de l'utilisation de cybermoyens et de méthodes de guerre, à moins qu'elles ne soient considérées comme un objectif militaire.

2. Les parties à un conflit ne doivent pas employer de cybermoyens et méthodes de guerre pour :

(a) Attaquer, détruire, enlever ou mettre hors d'usage les infrastructures hydrauliques indispensables à la survie de la population, telles que les installations et approvisionnements en eau potable et les travaux d'irrigation; et

(b) Attaquer les infrastructures hydrauliques contenant des forces dangereuses, à savoir les barrages et les digues, même lorsqu'il s'agit d'objectifs militaires, et d'autres objectifs militaires situés sur ces ouvrages ou à proximité, si une telle attaque peut provoquer la libération de forces dangereuses et, en conséquence, des pertes sévères parmi la population civile.

3. Pendant les cyberopérations, les infrastructures hydrauliques et les infrastructures liées à l'eau ne devraient pas faire l'objet d'attaques, même s'il s'agit d'objectifs militaires, si une telle attaque est destinée ou est susceptible de causer des dommages significatifs à l'environnement.

4. Les cyberopérations contre les infrastructures hydrauliques et les infrastructures liées à l'eau doivent également respecter toutes les autres règles de droit international applicables identifiées dans la Liste des principes de Genève sur la protection des infrastructures hydrauliques.

Commentaire

1. L'utilisation de « cyberopérations »[1] comme moyen ou méthode de guerre dans un conflit armé représente un risque réel de préjudice pour les civils et les infrastructures critiques. Développé avec la guerre cinétique traditionnelle à l'esprit, le droit international humanitaire ne contient (DIH) pas de règles spécifiques régissant les cyberopérations. Cependant, ses règles et principes fondamentaux s'appliquent aux cyberopérations menées dans le cadre d'un conflit armé (conflit armé international et conflit armé non international).[2] Notamment, le Protocole additionnel I prévoit une obligation de procéder à des examens juridiques des nouvelles armes, moyens et méthodes de guerre,[3] qui s'étend aux cybercapacités militaires destinées à être utilisées ou devant être utilisées dans la conduite des hostilités.[4] Selon la Cour internationale de justice, le droit international humanitaire réglemente « toutes les formes de guerre et à toutes sortes d'armes, celles du passé, celles du présent et celles de l'avenir ».[5] Par ailleurs, le Comité international de la Croix Rouge (CICR) affirme que le droit international humanitaire limite les cyberopérations pendant les conflits armés, tout comme il limite l'utilisation de toute autre arme, moyen et méthode de guerre dans un conflit armé.[6] De nombreux États ont convenu que si les conflits armés s'étendaient au cyberespace, le droit international humanitaire et, le cas échéant, d'autres règles du droit international s'appliqueraient à de telles opérations.[7] Une telle acceptation par les États est vitale car un nombre croissant d'États développent des cybercapacités pour leurs armées, et leur utilisation est susceptible d'augmenter à l'avenir. Selon le Comité international de la Croix-Rouge, l'interprétation par les États des règles existantes du droit international humanitaire déterminera dans quelle mesure ce domaine

[1] Semblable à la définition utilisée par le CICR, le terme « cyberopérations » est utilisé pour décrire les opérations contre un ordinateur, un système ou un réseau informatique, ou un autre appareil connecté, via un flux de données, lorsqu'il est utilisé comme moyen et méthode de guerre dans le contexte d'un conflit armé. Voir CICR, *« International Humanitarian Law and Cyber Operations during Armed Conflicts », Document de position du CICR*, soumis au « Groupe de travail à composition non limitée sur les développements dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale » et le « Groupe des Experts sur *Advancing Responsible State Behaviour in Cyberspace in the Context of International Security »*, novembre 2019, (fn.1). Le manuel du DoD des États-Unis définit les opérations dans le cyberespace comme des opérations qui impliquent « l'emploi de cybercapacités dont le but principal est d'atteindre des objectifs ou des effets militaires dans ou à travers le cyberespace ». Voir le manuel du DoD américain (2016), § 16.1.2.

[2] Voir *la prise de position du* CICR 2019, 4 ; et NATO Cooperative Cyber Defense, Centre of Excellence (Michael N. Schmitt (éd.)), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, Cambridge 2017), Commentary to Rule 80, § 1.

[3] Protocole additionnel I, Art.36.

[4] CICR, *Le droit international humanitaire et les défis des conflits armés contemporains* - Recommitting to Protection in Armed Conflict on the 70th Anniversary of the Geneva Conventions, 2019, 35.

[5] Voir *Licéité de la menace ou de l'emploi d'armes nucléaires* (Avis consultatif) 1996 CIJ Recueil 226, § 86.

[6] Position paper du CICR 2019, ci-dessus, note 1 ; et CICR Challenges Report 2019, ci-dessus note 4, 26-28.

[7] Voir La proposition du Haut Représentant de l'Union européenne pour les affaires étrangères et la politique de sécurité, Communication conjointe au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions - *Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé,* Bruxelles, 7.2.2013, 2013, 1 final.

du droit international protège contre les effets des cyberopérations. Cependant, selon le Comité international de la Croix-Rouge, les États devraient interpréter le droit international humanitaire de manière à préserver les infrastructures civiles des perturbations importantes.[8] De plus, dans la mesure où les cyberactivités contre les infrastructures hydrauliques et les infrastructures liées à l'eau menées au cours d'un conflit armé ne sont pas spécifiquement visées par les règles existantes du droit international humanitaire, la clause Martens,[9] qui reflète le droit international coutumier,[10] prévoit que ces infrastructures demeurent « sous la protection et l'autorité des principes du droit international dérivés de la coutume établie, des principes d'humanité et des préceptes de la conscience publique ».[11]

2. Les cyberopérations utilisées comme moyens et méthodes de guerre [12] dans le contexte d'un conflit armé, c'est-à-dire qui déclenchent un conflit armé ou ont un lien avec celui-ci, sont régies par le droit international humanitaire. Les cybermenaces qui ne sont pas menées en relation avec un conflit armé mais découlent de l'espionnage économique ou autre ou de la cybercriminalité organisée ne sont pas régies par le droit international humanitaire. Il est largement admis que les cyberopérations dont on peut raisonnablement s'attendre à ce qu'elles causent la mort, des blessures ou des dommages physiques constituent une « attaque » en vertu du droit international humanitaire.[13] Dans cette optique, la notion d'attaque englobe également les cyberopérations qui « perturbent des services essentiels sans nécessairement causer de dommages physiques constituent l'un des risques les plus importants pour les civils » et une telle interprétation est conforme à l'objet et au but des règles de droit international humanitaire sur la conduite des hostilités.[14] De plus, le Manuel de Tallinn 2.0 sur le droit international applicable aux cyberopérations (Manuel de Tallinn 2.0) recommande que « certaines cyberopérations, telles que celles affectant l'acheminement de l'aide humanitaire, soient régies par le DIH même si elles ne relèvent pas du niveau d'une 'attaque' ».[15]

3. Dans le contexte d'un conflit armé, les infrastructures civiles sont protégées contre les attaques, y compris l'utilisation de moyens informatiques et de méthodes de guerre, par les règles et principes fondamentaux existants du droit international

[8] Prise de position du CICR 2019, ci-dessus note 1, 2.
[9] Voir Protocole additionnel I, Art.1 (2) ; Protocole additionnel II, Préambule, § 5 ; Convention de La Haye (II), Préambule, § 9 ; et Convention de La Haye (IV), Préambule, § 8.
[10] Voir Avis consultatif sur les armes nucléaires, note 5 ci-dessus, § 84.
[11] Voir le principe 23 sur la clause de Martens ; et Manuel de Tallinn 2.0, note 2 ci-dessus, Commentaire de la Règle 80, §§ 11-12.
[12] Comme défini dans le Manuel de Tallinn 2.0, note 2 ci-dessus, Règle 103 : les « moyens de cyberguerre » sont les cyberarmes et leurs cybersystèmes associés, et les « méthodes de cyberguerre » sont les cybertactiques, techniques et procédures par lesquelles les hostilités sont menées.
[13] *Prise de position du* CICR 2019, note 1, 7 ci-dessus ; et Manuel de Tallinn 2.0, note 2 ci-dessus, règle 92.
[14] *Prise de position du* CICR 2019, ci-dessus note 1, 7-8.
[15] Manuel de Tallinn 2.0, note 2 ci-dessus, Commentaire de la Règle 80, § 4.

humanitaire, en particulier les principes de distinction, de proportionnalité et de précautions en cas d'attaque. Ainsi, même lorsque les infrastructures hydrauliques et les infrastructures liées à l'eau deviennent des objectifs militaires, les principes de distinction, de proportionnalité et de précaution, tels que réaffirmés par les principes 6, 7, 8, 9, 10 et 11 de la Liste de Genève sur la protection des infrastructures hydrauliques, qui s'appliquent à la fois aux conflits armés internationaux et non internationaux, doivent être respectés. Le principe de distinction exige que les cyberopérations ne soient pas dirigées contre des civils ou des objets civils.[16] Le droit international humanitaire interdit les attaques qui ne sont pas dirigées contre un objectif militaire spécifique (par exemple, les attaques qui traitent comme une cible unique un certain nombre d'objectifs militaires clairement distincts) et l'emploi de moyens et de méthodes de guerre qui ne peuvent pas être dirigés contre un objectif militaire spécifique ou dont les effets ne peuvent être limités comme l'exige la loi.[17] Ainsi, chaque fois que les parties à un conflit ont recours à des cyberopérations, elles doivent respecter le principe de distinction et éviter d'utiliser des cyberoutils qui se propagent et causent des dommages sans discernement (y compris des cybercapacités par nature sans discrimination).

4. Une cyberattaque dont on peut s'attendre à ce qu'elle cause accidentellement des pertes de vies civiles, des blessures à des civils, des dommages à des biens civils, ou une combinaison de ceux-ci, qui serait excessive par rapport à l'avantage militaire concret et direct attendu, est interdite.[18] Lorsque les infrastructures hydrauliques et les infrastructures liées à l'eau deviennent des objectifs militaires, « ceux qui planifient ou décident d'une attaque doivent faire tout ce qui est faisable aux civils, aux dommages aux biens civils, ou à une combinaison de ceux-ci, qui seraient excessifs par rapport à l'avantage militaire concret et direct attendu. »[19] À l'instar de ce qui est inscrit au paragraphe 3 du Principe 9 de la Liste de Genève sur la protection des infrastructures hydrauliques, le CICR considère que l'évaluation des « dommages civils accidentels » comprend les dommages dus aux effets directs et indirects prévisibles (ou répercutés) des cyberopérations.[20]

[16] Protocole additionnel I, articles 48, 51(2) et 52(2) ; Protocole additionnel II, Art.13 (2) ; Étude du CICR sur le DIH coutumier, règles 1 et 7 ; Manuel de Tallinn 2.0, note 2 ci-dessus, règle 93 ; et Principe 6 sur les attaques contre les infrastructures hydrauliques et les infrastructures liées à l'eau, et Principe 7 sur les attaques contre le personnel.
[17] Protocole additionnel I, Art.51 (4) ; Étude du CICR sur le DIH coutumier, règles 11 et 12 ; Manuel de Tallinn 2.0, note 2 ci-dessus, Règles 111-112 ; et Principe 8 sur les attaques aveugles.
[18] Protocole additionnel I, articles 51 (5) (b) et 57 (2) (a) (iii) ; Étude du CICR sur le DIH coutumier, règle 14 ; Manuel de Tallinn 2.0, note 2 ci-dessus, règle 113 ; et Principe 9 sur la proportionnalité dans l'attaque.
[19] Voir Protocole additionnel I, Art.57 (2) (b); et Étude du CICR sur le DIH coutumier, règle 19.
[20] *Prise de position du* CICR 2019, ci-dessus note 1, 7.

5. Les infrastructures hydrauliques et les infrastructures liées à l'eau sont des objets civils et, par conséquent, tant la précaution dans les cyberattaques que la précaution contre les effets des cyberattaques s'appliquent à leur protection.[21] La responsabilité de prendre des mesures de précaution par ceux qui prennent des mesures offensives et ceux dont les réseaux et les systèmes risquent d'être attaqués se reflète également dans les normes de comportement responsable de l'État dans le cyberespace adopté par l'ONU.[22] Ainsi, lors d'opérations militaires, y compris lors de l'utilisation de moyens informatiques et de méthodes de guerre, un soin constant doit être pris pour épargner la population civile et les biens civils.[23] Ceux qui planifient ou décident d'attaquer doivent faire tout leur possible pour vérifier que les objectifs à attaquer ne sont ni des civils ni des biens à caractère civil et ne font pas l'objet d'une protection spéciale,[24] et dans le choix des moyens et méthodes d'attaque à éviter ou au moins à minimiser, pertes accidentelles de vies civiles, blessures aux civils et dommages aux biens civils.[25] Le CICR souligne également que lorsqu'elles utilisent des moyens ou des méthodes de guerre cybernétiques, les parties à un conflit doivent veiller constamment à épargner la population civile et les biens civils afin d'éviter ou au moins de réduire les dommages accidentels.[26] En outre, les parties au conflit doivent prendre toutes les précautions possibles pour protéger la population civile et les biens civils sous leur contrôle contre les effets des attaques.[27] Ces mesures, entre autres, pourraient inclure la réduction des cybervulnérabilités, l'isolement de l'armée des cyberinfrastructures et des réseaux civils, la séparation des systèmes informatiques dont dépendent les infrastructures civiles essentielles d'Internet, et le travail sur l'identification dans le cyberespace de la cyberinfrastructure et des réseaux servant de protection objets (marquage numérique des objets protégés).[28] Conformément à cela, les parties au conflit sont encouragées à isoler ou à marquer numériquement les cyberinfrastructures dont dépendent les infrastructures civiles essentielles, y compris les infrastructures hydrauliques et les infrastructures liées à l'eau.

[21] Voir le Principe 10 sur les précautions en cas d'attaque et le Principe 11 sur les précautions contre les effets des attaques ; et CICR, *Avoiding Civilian Harm From Military Cyber Operations during Armed Conflicts* , Rapport préparé par Ewan Lawson et Kubo Ma č ák , *Réunion d'experts du CICR* , Genève , 21-22 janvier 2020, 25-31 & 54.

[22] Assemblée générale des Nations Unies, Rapport du Groupe d'experts gouvernementaux sur les développements dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale, A/70/174, 22 juillet 2015, § 13 (f) et (g).

[23] Voir Protocole additionnel I, Art.57 (1) ; Étude du CICR sur le DIH coutumier, règle 15 ; Manuel de Tallinn 2.0, note 2 ci-dessus, règle 114 ; et Prise de position du CICR 2019, ci-dessus note 1, 6.

[24] Voir Protocole additionnel I, Art.57 (1) (a) ; Étude du CICR sur le DIH coutumier, règle 16 ; Manuel de Tallinn 2.0, note 2 ci-dessus, règle 115 ; et Principe 10 sur les précautions en cas d'attaque.

[25] Voir Protocole additionnel I, Art.57 (2) (a); Étude du CICR sur le DIH coutumier, règle 17 ; Manuel de Tallinn 2.0, note 2 ci-dessus, Règles 116 ; et les principes 10 sur les précautions en cas d'attaque.

[26] *Prise de position du* CICR 2019, ci-dessus note 1, 5-6.

[27] Voir Protocole additionnel I, Art.58 (c) ; Étude du CICR sur le DIH coutumier, règle 22 ; Manuel de Tallinn 2.0, note 2 ci-dessus, règle 121 ; et Principe 11 sur les précautions contre les effets des attaques.

[28] *Prise de position du* CICR 2019, ci-dessus note 1, 6 ; et Rapport de la *réunion d'experts du* CICR 2020, ci-dessus note 21, 27-28 et 54.

6. En vertu du droit international humanitaire, outre la protection générale, certains objets, installations et zones sont spécifiquement protégés pendant la conduite des hostilités. Cette protection ne se limite pas à l'utilisation de moyens cinétiques mais couvre tous les moyens et méthodes de guerre, y compris les cyberopérations, compte tenu notamment de leur coût humain potentiel.[29] Parmi ces protections spécifiques, le Principes de Genève comprennent trois règles pertinentes pour la protection des infrastructures hydrauliques et des infrastructures liées à l'eau, à savoir les objets indispensables à la survie de la population, les ouvrages et installations contenant des forces dangereuses et la protection de l'environnement.

7. Les biens indispensables à la survie de la population bénéficient d'une protection spécifique au titre du droit international humanitaire. Il interdit d'attaquer, de détruire, d'enlever ou de rendre inutiles les objets indispensables à la survie de la population, tels que les installations et approvisionnements en eau potable et les travaux d'irrigation.[30] En conséquence, les parties au conflit ne doivent pas attaquer, détruire, enlever ou rendre inutilisables les infrastructures hydrauliques indispensables à la survie de la population civile.[31] Il est évident que les cyberopérations contre les installations de traitement de l'eau pour contaminer l'eau potable ou perturber les systèmes de distribution affectent négativement la qualité et l'approvisionnement en eau, entraînant des pénuries d'approvisionnement, ce qui pourrait également provoquer la propagation de maladies d'origine hydrique, entraînant une crise de santé publique.[32] Ainsi, de telles interdictions sont applicables, y compris lorsque des moyens informatiques et des méthodes de guerre sont employés contre les infrastructures hydrauliques. [33] En outre, les infrastructures hydrauliques peuvent être rendues inutilisables en ciblant les infrastructures liées à l'eau qui sont nécessaires à leur fonctionnement (par exemple, en tant que source d'alimentation), telles que les installations de production d'électricité. Dans de tels cas, l'interdiction doit être comprise comme couvrant également les infrastructures liées à l'eau.

8. Les ouvrages et installations contenant des forces dangereuses et d'autres objectifs militaires situés sur ces ouvrages ou à proximité bénéficient également

[29] CICR, *The Potential Human Cost of Cyber Operations*, Rapport préparé par Laurent Gisel et Lukasz Olejnik, CICR *Expert Meeting* Genève, 14-16 novembre 2018, 73-74 ; & *Prise de position du* CICR 2019, ci-dessus note 1, 5.
[30] Voir Protocole additionnel I, Art.54 (2) ; Protocole additionnel II, Art.14 ; Étude du CICR sur le DIH coutumier, Règle 54.
[31] Principe 12 sur la famine et les infrastructures hydrauliques indispensables à la population civile.
[32] *Réunion d'experts du* CICR 2018, note 29 ci-dessus, 63 ; Règles de Madrid, Art.1 ; Règles de Berlin, Commentaire de l'article 50, « Les civils ont droit à un approvisionnement en eau adéquat en toutes circonstances. D'où l'interdiction de toute action, quel qu'en soit le motif, qui aurait pour effet de priver la population civile de l'approvisionnement en eau nécessaire.
[33] Voir le Manuel de Tallinn 2.0, note 2 ci-dessus, Règle 141 ; *Réunion d'experts du* CICR 2018, note 29 ci-dessus, 73.

d'une protection spécifique. En vertu du droit international humanitaire coutumier, il est établi qu'une attention particulière doit être portée en cas d'attaque d'ouvrages et d'installations contenant des forces dangereuses et d'autres installations situées sur ces ouvrages ou à proximité, afin d'éviter la libération de forces dangereuses et les pertes graves qui en résultent parmi les populations civiles.[34] Il est interdit aux États parties au Protocole additionnel I d'attaquer des ouvrages ou des installations contenant des forces dangereuses, même lorsque ces objets sont des objectifs militaires, et d'autres objectifs militaires situés dans ou à proximité de ceux-ci, si une telle attaque peut entraîner la libération de forces dangereuses et de graves pertes en conséquence parmi la population civile, sous réserve des excetions de l'article 56 (2).[35] Pour les conflits armés non internationaux, le Protocole additionnel II stipule une interdiction similaire en vertu de l'article 15 mais n'inclut pas les exceptions mentionnées à l'article 56 (2). Ainsi, les infrastructures hydrauliques renfermant des forces dangereuses, à savoir les barrages et les digues, même lorsqu'il s'agit d'objectifs militaires, et d'autres objectifs militaires situés à ou à proximité de ceux-ci, ne doivent pas faire l'objet d'attaques si une telle attaque peut entraîner la libération de forces dangereuses et de graves pertes parmi la population civile.[36] L'interdiction s'applique également aux cas où les parties dans un conflit armé emploient des moyens et des méthodes de guerre cybernétiques.[37] Les parties au conflit sont encouragées à étendre l'interdiction d'utiliser des moyens et méthodes de guerre cybernétiques contre les barrages, les digues et les centrales nucléaires, et d'autres installations situées dans ou à proximité de toutes les infrastructures hydrauliques contenant des forces dangereuses telles que les usines de traitement des eaux, et les infrastructures liées à l'eau dont ils dépendent.

9. Le droit international humanitaire interdit également expressément l'utilisation de moyens et de méthodes de guerre qui sont destinés ou susceptibles de causer des dommages étendus, durables et graves à l'environnement naturel.[38] Concernant l'utilisation de moyens et méthodes cybernétiques contre l'environnement naturel, le Manuel de Tallinn 2.0 souligne que « l'environnement naturel est un objet civil et, en tant que tel, bénéficie d'une protection générale contre les cyberattaques et

[34] Étude du CICR sur le DIH coutumier, Règle 42.
[35] Protocole additionnel I, article 56.
[36] Principe 13 sur les infrastructures hydrauliques contenant des forces dangereuses.
[37] Voir le Manuel de Tallinn 2.0, note 2 ci-dessus, Règle 140.
[38] Voir Protocole additionnel I, articles 35 (3) et 55 (1) ; et Étude du CICR sur le DIH coutumier, Règle 45. Voir aussi, Commission du droit international, Protection de l'environnement en relation avec les conflits armés : texte du projet de principes provisoirement adopté au cours de la présente session par le Comité de rédaction, A/CN.4/L. 937 (6 juin 2019), Principe 13 ; et CICR, Lignes directrices sur la protection de l'environnement naturel dans les conflits armés : règles et recommandations relatives à la protection de l'environnement naturel en vertu du droit international humanitaire, avec commentaire, 2020, règle 2.

leurs effets », et que l'utilisation de moyens et méthodes de guerre cybernétiques qui sont destinés ou dont on peut s'attendre à ce qu'ils causent des dommages étendus, durables et graves à l'environnement naturel est interdite.[39] Les ressources en eau font partie du milieu naturel et bénéficient d'une telle protection. En outre, les usines de traitement des eaux et les stations de pompage peuvent contenir des réserves de produits chimiques industriels toxiques, et le fait de les attaquer (par exemple, utiliser des moyens informatiques pour déclencher un déversement de pétrole dans une voie navigable) pourrait avoir des effets néfastes importants sur l'environnement. À cette fin, les Principes de Genève prévoient que les infrastructures hydrauliques et les infrastructures liées à l'eau ne doivent pas faire l'objet d'attaques, même lorsqu'il s'agit d'objectifs militaires, si une telle attaque est destinée ou est susceptible de causer des dommages significatifs à l'environnement.[40] Ainsi, les cyberopérations doivent être employées en tenant dûment compte de la protection et de la préservation de l'environnement, y compris les infrastructures hydrauliques et infrastructures liées à l'eau.

10. Comme le prévoit le paragraphe 4, outre les protections réaffirmées aux paragraphes (1), (2) et (3), il existe d'autres règles pertinentes identifiées par les Principes de Genève applicables à la protection des infrastructures hydrauliques dans le contexte des conflits armés, ainsi que dans les situations de post-conflit. Ils comprennent certaines protections et interdictions spécifiques en vertu du droit international humanitaire, du droit international relatif aux droits de l'homme et du droit international de l'eau. Par exemple, le droit international humanitaire interdit les actes ou menaces de violence dont le but premier est de semer la terreur parmi la population civile.[41] Une telle conduite est interdite, y compris lorsqu'elle est effectuée par des moyens informatiques ou des méthodes de guerre.[42] De même, comme l'utilisation de poison ou d'armes empoisonnées est interdite, les moyens informatiques ou les méthodes de guerre ne doivent pas être utilisés pour empoisonner l'eau.[43] Par ailleurs, le droit international humanitaire interdit le déplacement forcé de la population civile.[44] En conséquence, les cyberopérations contre les infrastructures hydrauliques, telles que le contrôle de l'approvisionnement en eau, la libération (inondation) ou la privation d'eau, ne doivent pas être utilisées pour forcer le déplacement de civils.[45] De plus, les

[39] Manuel de Tallinn 2.0, note 2 ci-dessus, règle 143 ; et *réunion d'experts* du CICR 2018, note 29 ci-dessus, 73
[40] Voir Principe 15 sur la protection de l'environnement.
[41] Protocole additionnel I, Art.51 (2) ; Protocole additionnel II, Art.13 (2) ; Étude du CICR sur le DIH coutumier, règle 2.
[42] Voir le Manuel de Tallinn 2.0, note 2 ci-dessus, Règle 98 ; et le Principe 14 sur les actes ou menaces de violence dont le but premier est de semer la terreur parmi la population civile.
[43] Voir Convention de La Haye II), Art.23 (a); Étude du CICR sur le DIH coutumier, règle 72 ; et Principe 5 sur le poison ou les armes empoisonnées.
[44] Voir Convention de Genève IV, Art.49 ; Protocole additionnel II, Art.17 ; et Étude du CICR sur le DIH coutumier, règle 129.
[45] Voir Principe 16 sur le déplacement forcé.

parties à un conflit armé ont le devoir de ne pas entraver l'accès et l'assistance humanitaires nécessaires.[46] Comme le souligne le Manuel de Tallinn 2.0, « les cyberopérations ne doivent pas être conçues ou menées pour interférer indûment avec des efforts impartiaux pour fournir une assistance humanitaire » [47]. En outre, en situation d'occupation, la Puissance occupante a l'obligation de rétablir et d'assurer l'ordre et la sécurité publics (englobant la restauration et la garantie de la vie civile)[48] et s'assurer que la population sous son contrôle dispose des denrées alimentaires nécessaires et d'autres fournitures essentielles à sa survie.[49] De telles obligations impliquent, entre autres, la restauration et l'entretien des cyberinfrastructures indispensables pour assurer le traitement de l'eau et le réseau d'approvisionnement.[50]

11. Conformément aux principes 1 (2) et (3), les Principes de Genève sont destinés à la fois aux conflits armés internationaux et aux conflits armés non internationaux et s'adressent à la fois aux États et aux acteurs non étatiques. En conséquence, pendant un conflit armé non international, toutes les parties impliquées sont tenues de respecter les règles pertinentes du DIH applicables aux cyberopérations.

12. Les Principes de Genève ont également identifié d'autres règles pertinentes issues d'autres branches du droit international qui régissent et protègent les infrastructures hydrauliques et les infrastructures liées à l'eau. Ces règles sont vitales concernant les cyberactivités qui ne déclenchent pas de conflit armé ni n'ont de lien avec celui-ci mais qui impactent ces infrastructures. Par exemple, le droit international relatif aux droits de l'homme, qui s'applique en temps de paix et continue de s'appliquer dans les conflits armés,[51] reconnaît que chacun a droit à l'eau et à l'assainissement en tant qu'éléments du droit à un niveau de vie suffisant et indispensables à la pleine jouissance de tous les droits humains, y compris le droit à la vie.[52] Le Manuel de Tallinn 2.0 reconnaissait que le droit international relatif aux droits de l'homme (à la fois le droit conventionnel et le droit coutumier) s'applique aux « activités liées à la cybercriminalité », y compris dans

[46] Voir Convention de Genève IV, Art.23 ; Protocole additionnel I, Art.70 ; Protocole additionnel II, art.18 (2) ; Étude du CICR sur le DIH coutumier, Règle 55 ; et Principe 17 sur l'accès et l'assistance humanitaires.
[47] Manuel de Tallinn 2.0, note 2 ci-dessus, règle 145.
[48] Voir Règlement de La Haye, Art.43. Voir aussi, CICR, *Occupation et autres formes d'administration d'un territoire étranger,* rapport (2012), 56-58.
[49] Convention de Genève IV, articles 55-56 ; et Protocole additionnel I, Art.69 (1).
[50] Manuel de Tallinn 2.0, note 2 ci-dessus, Commentaire de Règle 147, § 2.
[51] Voir Avis consultatif sur les armes nucléaires, note 5 ci-dessus, § 25 ; et *Conséquences juridiques de la construction d'un mur dans le territoire palestinien occupé* (Avis consultatif) 2005 CIJ Recueil 13, § 106.
[52] Voir également Comité des droits économiques, sociaux et culturels des Nations Unies, *Observation générale n°15 : Le droit à l'eau (Art. 11 et 12 du Pacte)* (2003), § 3 ; Convention sur l'élimination de toutes les formes de discrimination à l'égard des femmes (18 décembre 1979), art.14 (2) (h); Convention relative aux droits de l'enfant (20 novembre 1989), art.24 (2) (c) et (e); Convention relative aux droits des personnes handicapées (13 décembre 2006), art.28 (2) (a); UNHRC Res. 15/9 (6 octobre 2010), § 3 ; UNGA Res. 70/169 (17 décembre 2015), § 7.

le contexte d'un conflit armé, et impose l'obligation de respecter et de protéger les droits de l'homme [53] De même, les Principes de Genève réaffirment l'importance des droits humains à l'eau et à l'assainissement pour la pleine jouissance de tous les droits humains et réaffirme l'obligation d'assurer l'accès à une eau suffisante, sûre, potable, physiquement accessible et abordable, et un accès physique et abordable à l'assainissement.[54] Par conséquent, les cyberopérations qui interfèrent avec les systèmes de traitement ou d'approvisionnement en eau ou ont généralement un impact sur les infrastructures hydrauliques et les infrastructures liées à l'eau pourraient violer les droits humains, y compris les droits à l'eau et à l'assainissement, le droit à la vie et le droit à la santé.

13. Il est généralement admis que les États assument des obligations extraterritoriales en matière de droits humains envers ceux qui sont sous leur « pouvoir ou contrôle effectif »,[55] quelles que soient les circonstances dans lesquelles ce pouvoir ou ce contrôle effectif a été obtenu.[56] En ce qui concerne l'obligation extraterritoriale des droits de l'homme pour les cyberactivités, le Manuel de Tallinn 2.0 mentionne qu'il existe un certain désaccord sur la question de savoir si les obligations des traités relatifs aux droits de l'homme s'appliquent de manière extraterritoriale, mais affirme que le droit international coutumier des droits de l'homme s'applique de manière extraterritoriale dans les situations où un État exerce « un pouvoir ou un contrôle effectif » comme il le fait hors ligne (quand un État exerce un contrôle physique sur un territoire ou des personnes).[57] Le Manuel de Tallinn 2.0, cependant, reconnaît qu'il n'y a pas de consensus parmi les experts sur la question de savoir si les mesures étatiques qui n'impliquent pas un exercice de contrôle physique (activités menées dans le cyberespace uniquement) peuvent être qualifiées de « pouvoirou de contrôle effectif » [58]. Lorsque les États exercent un pouvoir ou un contrôle effectif extraterritorial, ils doivent s'abstenir d'actes susceptibles d'interférer indûment avec la jouissance des droits humains à l'eau et à l'assainissement, y compris en limitant l'accès aux services et infrastructures

[53] Voir le Manuel de Tallinn 2.0, note 2 ci-dessus, Règles 34 - 36.
[54] Voir le Principe 3 sur les droits de l'homme à l'eau et à l'assainissement avec son commentaire.
[55] Le Comité des droits de l'homme des Nations Unies a élaboré la notion d'exercice du pouvoir ou de contrôle effectif en vertu de son Observation générale 36, Article 6 (Droit à la vie). Il illustre que « l'État partie a l'obligation de respecter et de garantir les droits énoncés à l'article 6 de toutes les personnes se trouvant sur son territoire et de toutes les personnes relevant de sa juridiction, c'est-à-dire toutes les personnes sur lesquelles il exerce la jouissance du droit à la vie pouvoir ou contrôle effectif. Cela inclut les personnes situées en dehors de tout territoire effectivement contrôlé par l'État, dont le droit à la vie est néanmoins affecté par ses activités militaires ou autres d'une manière directe et raisonnablement prévisible. Voir Comité des droits de l'homme des Nations Unies, *Observation générale no. 36, article 6 (Droit à la vie)* (2019), § 63.
[56] Comité des droits de l'homme des Nations Unies, Observation générale n°31 : *La nature de l'obligation juridique générale imposée aux États parties au Pacte,* (2004), CCPR/C/21/Rev.1/Add.13, § 10 ; CIJ, *Conséquences juridiques de la construction d'un mur dans le territoire palestinien occupé*, avis consultatif, 2004, §§ 107-112 ; et *Affaire concernant les activités armées sur le territoire du Congo (République démocratique du Congo c. Ouganda)* (Arrêt) 2005 CIJ Recueil 168, §§ 216-217.
[57] Voir Manuel de Tallinn 2.0, note 2 ci-dessus, Commentaire de la Règle 34, §§ 1-7.
[58] *Ibid.*, Commentaire de la Règle 34, §§ 8-11.

d'eau ou en les détruisant.[59] Une telle obligation négative de respecter les droits à l'eau et à l'assainissement s'applique de manière extraterritoriale, car les États sont tenus de respecter la jouissance de ce droit dans d'autres pays et la coopération internationale exige également des États qu'ils « s'abstiennent d'actions qui interfèrent, directement ou indirectement, avec la jouissance du droit à l'eau dans d'autres pays. »[60] En outre, un État devrait avoir une obligation de prévenir un préjudice extraterritorial s'il contrôle la cyberinfrastructure ou si l'infrastructure à partir de laquelle la cyberopération est lancée se trouve sur son territoire.

14. Le droit international de l'eau offre également une certaine protection aux ressources en eau dans le contexte des cyberopérations. Par exemple, la Convention sur le droit des cours d'eau internationaux à des fins autres que la navigation (Convention des Nations Unies sur les cours d' eau) stipule que « les cours d'eau internationaux et les installations, équipements et autres ouvrages connexes bénéficient de la protection accordée par les principes et règles du droit international applicables en conflits armés internationaux et non internationaux .[61] Comme indiqué ci-dessus, ces protections du droit international humanitaire s'appliquent également lorsque les parties à un conflit armé utilisent des moyens informatiques ou des méthodes de guerre, et cela est vital face à la numérisation toujours croissante du secteur de l'eau et de la gestion des cours d'eau transfrontaliers. Le droit international de l'eau impose également l'obligation de ne pas causer de dommages transfrontaliers, tels que des empoisonnements ayant des effets transfrontaliers.[62] De même, le principe d'une utilisation équitable et raisonnable des cours d'eau partagés requiert l'utilisation durable de l'eau et la protection des écosystèmes.[63] Les États qui partagent des cours d'eau transfrontaliers ont l'obligation de « faire de leur mieux pour entretenir et protéger les installations, installations et autres ouvrages liés à un cours d'eau international »,[64] notamment en prenant toutes les précautions raisonnables pour protéger ces ouvrages contre les dommages prévisibles. De plus, les États du cours d'eau devraient coopérer, même dans les situations de conflit armé, y compris l'échange de données et d'informations, la notification, la communication, les consultations et les négociations.[65] En outre, les États du cours d'eau devraient créer des mécanismes et des commissions conjointes pour assurer la protection, l'exploitation sûre et l'entretien des infrastructures hydrauliques sur les ressources

[59] Voir Observation générale n°15, note ci-dessus 52, § 21.
[60] *Ibid.*, § 31.
[61] Voir Convention des Nations Unies sur les cours d'eau, Art.29.
[62] Voir Convention des Nations Unies sur les cours d'eau, Art.7 ; et Convention CEE-ONU), art.2.
[63] Voir, par exemple, la Convention des Nations Unies sur les cours d'eau, articles 5, 7 et 20 ; et Art.2 (1) et 2 (2) de la Convention de la CEE-ONU.
[64] Voir Convention des Nations Unies sur les cours d'eau, Art.26 (1).
[65] *Ibid.*, Art.30-31.

en eau transfrontalières.[66] En conséquence, dans la protection et l'utilisation des cours d'eau transfrontaliers, les cyberactivités des États, à la fois pendant et en dehors du contexte d'un conflit armé, devraient être menées dans le respect de ces obligations.

15. Enfin, les infrastructures critiques, telles que les systèmes d'approvisionnement en eau et les égouts, sont particulièrement vulnérables aux cyberattaques malveillantes d'autres États ou d'acteurs non étatiques. En vertu du droit international, les États ont l'obligation de diligence raisonnable de ne pas permettre sciemment que leur territoire soit utilisé pour des actes internationalement illicites contre un autre État,[67] ce qui est également pertinent pour les activités dans le cyberespace. L'ONU a créé un Groupe de travail à composition non limitée (OEWG) sur les développements dans le domaine de l'information et des télécommunications, et le rapport de ce dernier souligne que « les États ne devraient pas mener ou soutenir sciemment des activités de TIC (techniques de l'information et de la communication) contraires à leurs obligations en vertu du droit international qui portent intentionnellement des dommages d'infrastructure ou entrave de quelque manière que ce soit l'utilisation et le fonctionnement des infrastructures essentielles pour fournir des services au public. En outre, les États devraient continuer à renforcer les mesures pour protéger toutes les infrastructures critiques contre les menaces liées aux TIC et accroître les échanges sur les meilleures pratiques en matière de protection des infrastructures critiques.»[68] De même, le Manuel de Tallinn 2.0 a inclus le principe de diligence raisonnable et a mentionné que « l'État doit faire preuve de diligence raisonnable en n'autorisant pas que son territoire ou de sa cyber-infrastructure se trouvant sous son contrôle gouvernemental, soient utilisés pour des cyberopérations qui affectent les droits d'autres États et entraînent de graves conséquences négatives pour eux.»[69]
En outre, il déclare que « le principe de diligence raisonnable exige qu'un État prenne toutes les mesures possibles dans les circonstances pour mettre fin aux cyberopérations qui affectent un droit et entraînent des conséquences négatives graves pour d'autres États. »[70] Néanmoins, comme indiqué dans le Tallinn Manual 2.0, il y a quelques questions délicates concernant ce principe.[71]

---

[66] Voir Convention des Nations Unies sur les cours d'eau, articles 8 et 24 (1) ; Convention CEE-ONU, art.9 (2) ; et Principe 20 sur les mécanismes et commissions conjoints.
[67] Voir CIJ, *Détroit de Corfou (Royaume-Uni c. Albanie)* , arrêt, 9 avril 1949, 22 ; et *affaire de la Fonderie du Trail* (États-Unis c. Canada), Tribunal arbitral, 3 UN Rep. Int'l Arb. Prix 1905.
[68] AGNU, Groupe de travail à composition non limitée sur les développements dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale, Rapport de fond final, A/AC.290/2021/CRP.2, 10 mars 2021, § 31.
[69] Manuel de Tallinn 2.0, note 2 ci-dessus, règle 6.
[70] *Idem.* , règle 7.
[71] Voir par exemple, *Ibid*., Commentaire de la Règle 6, §§ 29-30 ; et Commentaire de la Règle 7, §§ 3-4 & 14-15.

Le Geneva Water Hub

Secrétariat su Panel mondial de haut niveau sur l’eau et la paix