ICT for peace foundation

POLICY BRIEF

LA NEUTRALITÉ DE LA SUISSE À L'ÈRE DE LA CYBERGUERRE

Martin Dahinden

GENEVA 2021

ICT4Peace Foundation

ICT4Peace Publishing, Geneva. January 2021
Copies available from www.ict4peace.org

LA NEUTRALITÉ DE LA SUISSE À L'ÈRE DE LA CYBERGUERRE

Martin Dahinden

ICT for peace foundation

Document de discussion

LA NEUTRALITÉ DE LA SUISSE À L'ÈRE DE LA CYBERGUERRE

Martin Dahinden[1]

La cyberguerre est un défi nouveau et important pour la neutralité de la Suisse. Basé sur le droit de la neutralité et la politique suisse de neutralité, ce document de travail est destiné à offrir une interprétation des questions essentielles d'ordre juridique, politique et conceptuel touchant à la cyberguerre. Il s'agit à la fois de contribuer à un débat naissant et d'esquisser les possibilités d'action qui se présentent à la Suisse dans un environnement en constante évolution.[2]

INTRODUCTION

La question des droits et des devoirs des États neutres dans le cyberespace est complexe et ne peut en aucun cas trouver des réponses en extrapolant le droit de la neutralité applicable et la politique traditionnelle de neutralité .

Aujourd'hui, il existe un large consensus international sur le fait que le droit international est également applicable au cyberespace. Cependant, les avis juridiques et les positions politiques diffèrent largement sur ce que cela signifie concrètement

1 Martin Dahinden a été ambassadeur de Suisse aux États-Unis, il est membre du conseil de fondation du Think Tank ICT4Peace et enseigne la politique de sécurité à l'université de Zurich.

2 Je tiens à remercier Sanija Ameti, Anne-Marie Buzatu, Serge Droz, Alain Modoux, Sara Pangrazzi, Daniel Stauffacher et Regina Surber pour leurs commentaires et leurs contributions. Ce document de discussion est une traduction de la version originale en allemand.

pour les différentes normes du droit international. C'est ce que l'on peut conclure des délibérations qui ont eu lieu ces dernières années dans le cadre des Nations unies[3] . La compréhension de la problématique a progressé; des points de vue communs ont également été formulés, du moins partiellement. Toutefois, Il n'y a encore eu aucune véritable avancée sur les questions essentielles et les normes contraignantes , car les divergences politiques ne peuvent être résolues par des avis de droit.

Le droit de la neutralité a été abordé, directement ou indirectement, dans les forums internationaux traitant des questions de cybersécurité. Il est évident que même à l'ère de la cyberguerre, il y aura des conflits comme il y aura des États tiers qui n'y participeront pas. Pour ces derniers, les droits et obligations d'un neutre s'appliqueront. Il n'est donc pas surprenant que le manuel de Tallinn[4] contienne un chapitre distinct sur la neutralité.

Cependant, la neutralité permanente de la Suisse va bien au-delà des principes fondamentaux du droit de la neutralité. Même en temps de paix, la Suisse mène une politique qui rend crédible sa volonté de rester neutre dans les futurs conflits armés internationaux.

Le cyberespace est nouveau et présente de nombreuses particularités. C'est pourquoi

3 Cf. Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale (UN GGE). Le Groupe a été créé en 2004 par la Première Commission de l'Assemblée générale des Nations unies dans le but de donner des conseils sur la manière de renforcer la paix et la sécurité dans le cyberespace par des mesures de confiance et des normes de comportement responsable des États, ainsi que de renforcer les capacités nécessaires. Voir également le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale (UN OEWG) établi en parallèle par les Nations unies en 2018. Fiche d'information Processus intergouvernementaux sur l'utilisation de l'information et des télécommunications dans le contexte de la sécurité internationale 2019-2021 : https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/03/2019+03+26+-+Fact+Sheet+Cyber+-+OEWG+et+GGE+processus+-+2.pdf. Depuis 2011, ICT4Peace soutient les processus UN GGE et UN OEWG par le biais de rapports d'experts, de propositions concrètes et de programmes de formation pour les diplomates et les hauts fonctionnaires. L'objectif est de promouvoir un comportement responsable de la part des États, des mesures de confiance, des normes et le développement des capacités étatiques nécessaires (cf. aperçu: https://ict4peace.org/?category_name=support-to-un-oewg-and-un-gge&s=&load=all)

4 Manuel de Tallinn 2.0 sur le droit international applicable à la cyberguerre (2017). Cambridge : Cambride University Press. Le Manuel de Tallinn est une étude sur l'applicabilité du droit international de la guerre aux cyberconflits (ius ad bellum ; ius in bello). Le Manuel de Tallinn a été rédigé entre 2009 et 2012 par une vingtaine d'experts à l'invitation du Centre d'excellence de coopération pour la cyberdéfense de l'organisation (CCD COE) de lOTAN à Tallinn.

la politique de neutralité de la Suisse à l'ère de la cyberguerre ne peut pas simplement découler des doctrines existantes en matière de politique de neutralité. Elle demande avant tout une réflexion sur sa politique de sécurité[5] .

En outre, la neutralité permanente est également à la base du rôle particulier que joue la Suisse dans la communauté des États. Dans la mesure où la neutralité permanente présente des avantages, la Suisse a toujours estimé que son statut de neutralité impliquait une obligation de contribuer concrètement à la paix et à la sécurité dans le monde. Cela inclut , entre autres, l'engagement humanitaire, la volonté d'offrir ses bons offices, les efforts visant à renforcer le droit international, l'engagement en faveur de mesures de confiance, la prévention et la gestion des conflits. Comment ce rôle peut-il et doit-il être maintenu à l'ère de la cyberguerre ?

1. LA NEUTRALITÉ COMME PRINCIPE DE LA POLITIQUE ÉTRANGÈRE SUISSE

La neutralité permanente est un principe central de la conception suisse de l'État et de sa politique étrangère. Toutefois, elle n'est pas un objectif d'État en soi, mais sert à sauvegarder l'indépendance du pays et l'inviolabilité de son territoire. C'est pourquoi la neutralité n'est mentionnée ni dans l'article de la Constitution fédérale qui définit le but de la politique étrangère, ni dans celui qui en précise les principes[6] .

Le droit de la neutralité a été codifié dans les conventions de La Haye du 18 octobre 1907 et fait désormais partie du droit international coutumier. Il définit les droits et les obligations d'un État neutre[7] .

Le plus important de ces droits est l'inviolabilité du territoire de l'État.

5 Voir Dahinden, Martin, Pangrazzi, Sara (2020) : Neutralität im Cyberraum : Die Schweiz ist gefordert. Neue Zürcher Zeitung, 31.12.2020, 19.

6 Cette section est basée sur la présentation officielle de la neutralité par le Département fédéral des affaires étrangères (DFAE). Il s'agit de faire une référence claire à la conception actuelle de la neutralité.

7 https://www.fedlex.admin.ch/eli/cc/26/499_376_481/fr

Les obligations les plus importantes de l'État neutre sont les suivantes :

- ne pas participer à un conflit armé international ;
- assurer sa propre autodéfense ;
- traiter tous les belligérants sur un pied d'égalité en ce qui concerne l'exportation d'armes ;
- ne pas fournir des troupes ou des mercenaires aux belligérants ;
- ne pas mettre son propre territoire à la disposition des belligérants.

Le droit de la neutralité s'applique aux conflits entre États. Il ne s'applique pas aux opérations militaires autorisées par le Conseil de sécurité des Nations unies. Comme tous les États, les États neutres ont le droit de se défendre en cas d'attaque armée.

La politique de neutralité comprend l'ensemble des mesures prises par un État neutre pour rendre crédible son statut de neutralité. La forme concrète que prend la politique de neutralité dépend dans une large mesure de l'environnement international et de son appréciation.

En conséquence, la politique de neutralité a subi des changements considérables au fil du temps. La politique de neutralité conduit à une pratique réelle qui, en fin de compte, va bien au-delà des principes fondamentaux du droit de la neutralité.

2. LE DÉFI DU CYBERESPACE

Les technologies de l'information et de la communication (TIC) recèlent un potentiel de développement économique et social sans précédent, mais présentent en même temps de grands risques pour la paix et la sécurité internationale. C'est ainsi que de nombreux États ont développé des capacités en matière de technologies de l'information et de la communication (TIC) à des fins militaires et continuent à le faire à grande échelle. Ce faisant, ils ont introduit une quatrième dimension de la guerre en plus de la guerre terrestre, maritime et aérienne.

Dans ce contexte, on peut distinguer trois grands types de cyberopérations :

1. **Les "Computer Network Exploitations"** (CNE) sont des opérations qui pénètrent des réseaux étrangers pour voler des informations, idéalement sans laisser de traces ("cyberespionnage").

2. **Les "Computer Network Attacks"** (CNA) sont des attaques contre des réseaux informatiques visant à les perturber, à les endommager ou même à les détruire, y compris les informations sauvegardées. Les CNA constituent les plus grands risques, surtout lorsque les attaques sont dirigées contre des infrastructures essentielles.

3. **Les "Information Operations"** (OI) visent à influencer les opinions dans un État étranger pour favoriser ses propres desseins[8] .

Les cyberattaques font typiquement partie d'une guerre hybride, c'est-à-dire qu'elles sont conduites en combinaison avec des formes de combat régulières et irrégulières, symétriques et asymétriques, militaires et non militaires, ouvertes et secrètes[9] . Dans les cyber-opérations, il est souvent difficile d'identifier les auteurs des attaques ("attribution"). Il est également difficile de déterminer quelles activités constituent une attaque ou un conflit armé et à partir de quel niveau d'intensité. Souvent, il est même difficile de déterminer s'il y a eu une attaque ou s'il s'agit d'un dommage collatéral[10] .

Dans le droit traditionnel de la neutralité, le territoire de l'État joue un rôle essentiel en ce qui concerne les droits et obligations de l'État neutre. Le territoire de l'État entre également en ligne de compte à l'ère de la cyberguerre, car les systèmes juridiques nationaux et le contrôle des faits continuent d'avoir une dimension géographique. Cependant, le cyberespace, physiquement insaisissable, est si complexe qu'il dépasse

8 Vgl. Meyer, Paul, Stauffacher, Daniel (2021) : Neue Zürcher Zeitung, 11 février 2021

9 Vgl. Countering Hybrid Warfare Project (CHW): https://www.gov.uk/government/publications/countering-hybrid-warfare-project-understanding-hybrid-warfare . Mérite de lire, même si vieillit, Frank G. (2007): Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington: Potomac Institute for Policy Studies.

10 Les opérations des TIC sont également utilisées à des fins terroristes ou par des organisations criminelles. Toutefois, ils ne font pas l'objet du présent document de travail, qui se concentre sur les aspects de la neutralité. https://ict4peace.org/wp-content/uploads/2019/08/ICT4Peace-2016-Private-Sector-Engagement-in-Responding-to-the-Use-of-the-Internet-and-ICT-for-Terrorist-Purposes.pdf

les expériences faites jusqu'ici.

Il faut considérer le cyberespace, l'Internet, comme un bien public mondial, sans pour autant abroger la souveraineté des États en matière d'équipements, de personnes, de propriété intellectuelle, etc. Ce point de vue n'est pas très répandu, probablement parce qu'il associe un concept politico-économique (global commons) à des catégories juridiques.

La complexité du cyberespace et de la cyberguerre est également due au fait que, contrairement à la guerre classique, tout le monde peut y accéder et que la distinction entre civils et combattants, qui est fondamentale en droit international humanitaire, est particulièrement floue.

3. NEUTRALITÉ DANS LE CYBERESPACE

Les sections suivantes traitent de la neutralité dans le cyberespace en termes juridiques et politiques, en fournissant un aperçu des questions et, dans la mesure du possible, des réponses. Le schéma suit les principaux droits et obligations des neutres, comme exposés plus haut.

Inviolabilité du territoire national

Le droit le plus important d'un État neutre est l'inviolabilité de son territoire. Mais que signifie l'inviolabilité du territoire de l'État dans le contexte des cyberopérations ? S'agit-il d'effets physiques (dommages aux personnes et aux objets) ? S'agit-il également de l'infrastructure et du fonctionnement des équipements dépendant de l'Internet ? S'agit-il d'une protection complète de l'espace numérique sous le contrôle et la juridiction d'un État?

L'inviolabilité de leur territoire national est, bien sûr, un droit de tous les États, et pas seulement des États neutres. Comme cette question est identique ou similaire pour tous, les discussions internationales dans ce domaine concernent aussi directement la Suisse.

La légitime défense en cas de cyberattaques

Selon l'article 51 de la Charte des Nations unies, les États qui sont attaqués ont le droit légitime de se défendre. Il s'agit d'une exception à l'interdiction générale de l'usage de la force dans la Charte des Nations unies.

La question du seuil à partir duquel une attaque atteint un degré qui légitime l'État attaqué à agir contre un agresseur avec des moyens numériques ou même cinétiques est cependant controversée[11] . Ici aussi, il ne s'agit pas seulement d'une question d'ordre juridique, mais finalement de décisions politiques quant au moment d'invoquer le droit de légitime défense et aux moyens à utiliser. Les doctrines correspondantes peuvent avoir un effet dissuasif ou conduire à une escalade, etc.

Il est vrai que ce problème touche tous les États. Cependant, elle revêt une importance particulière pour l'État neutre car il s'agit également de savoir si une cyberattaque viole "simplement" la neutralité et quand l'État neutre lui-même devient partie à un conflit armé.

Coopération dans les domaines de la protection et de la défense

La coopération avec d'autres États dans les domaines de la protection et de la défense est légitime pour les États neutres, mais c'est un domaine délicat car des dépendances peuvent se créer et la crédibilité de la neutralité peut être compromise en cas de conflit. En tout état de cause, l'adhésion à une alliance de défense n'est pas compatible avec la neutralité. Toutefois, les échanges d'expériences, la coopération en matière de formation et d'armement, etc. sont tout à fait permis.

Quelle est la situation dans le domaine du cyberespace ? Quelles formes spécifiques de coopération sont permises sans créer d'incertitude quant à la neutralité effective de l'État en cas de conflit ? Y a-t-il des limites juridiques (accords, etc.) ou des limites de fait (infrastructure partagée, interopérabilité, etc.) ?

11 Pangrazzi, Sara (2021): Self-Defence against Cyberattacks? Digital and Kinetic Defence in Light of Article 51 UN-Charter, ICT4Peace Publishing, Geneva, février 2021

L'ONU recommande que les États soient soutenus si leurs infrastructures sont exposées à une cyberattaque[12] . Dans quelles conditions l'assistance d'un État neutre est-elle acceptable (à l'instar de l'aide humanitaire) ? Quand la fourniture d'une assistance devient-elle un soutien à une partie à un conflit, ce qui la rendrait inadmissible en vertu du droit de la neutralité ?

Non-participation aux conflits armés

Il est interdit à l'État neutre de participer à des conflits armés. C'est certainement aussi le cas si un conflit est mené totalement ou en partie par des moyens numériques.

À première vue, cette disposition semble évidente. Encore faut-il qu'il soit clair qu'il existe un conflit armé. Le sujet renvoie aux questions du seuil de la guerre, de la classification des cyberattaques et du problème de la guerre hybride.

Assurer l'autodéfense

La disposition selon laquelle les États neutres doivent assurer leur propre autodéfense contribue à la crédibilité et à la prévisibilité de la neutralité. Que signifie une telle obligation à l'ère de la cyberguerre ? Par analogie avec la guerre conventionnelle, cela signifie que l'État neutre est obligé de protéger son infrastructure de telle sorte qu'elle ne puisse pas être utilisée par les parties au conflit. Un État neutre qui ne se protège pas ou qui ne prend pas de mesures de protection raisonnables ne remplirait donc pas les obligations d'un État neutre.

Indépendamment de la question de la neutralité, l'ONU exige que les États mettent en œuvre des mesures de protection contre les cyberattaques[13] .

Mais quelles sont les précautions concrètes à prendre ? Qu'est-ce qui est raisonnable ? S'agit-il de mesures de protection passive (pare-feu/firewall, refus d'accès aux

12 UN General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 22 July 2015, UN Doc. A/70/174 (UN GGE Report 2015)

13 UN GGE Report 2015

systèmes, protection contre les logiciels malveillants, etc.)[14] . Qu'en est-il des menaces externes à leur propre territoire, par exemple un site de phishing qui sert à collecter des données d'accès ? Une cybercapacité offensive dissuasive est-elle nécessaire et admissible pour empêcher des cyberattaques?

Cela conduit à l'épineuse question de savoir dans quelle mesure l'État neutre lui-même devrait disposer de cybercapacités offensives afin de pouvoir agir de manière préventive et anticipée[15] . En termes de politique de neutralité, la retenue pourrait être de mise. Cependant, au moins deux arguments plaident également en faveur d'une cybercapacité offensive. Premièrement, il est difficile d'imaginer que des mesures de protection efficaces puissent être mises en place contre les cyberattaques sans disposer des capacités correspondantes. Deuxièmement, l'État neutre ne peut exclure la possibilité qu'il soit lui-même attaqué et souhaite exercer son droit de légitime défense en vertu de l'article 51 de la Charte des Nations unies.

Égalité de traitement de tous les belligérants en ce qui concerne l'exportation d'armements

En ce qui concerne l'exportation d'armements (équipement, technologie), un État neutre doit traiter toutes les parties belligérantes sur un pied d'égalité. Il ne s'agit donc pas d'une interdiction d'exportation, mais d'une interdiction de discrimination. Toutefois, la politique d'exportation de matériel de guerre de la Suisse ne consiste pas seulement à vérifier sa compatibilité avec le droit et la politique de neutralité, mais aussi à atteindre des objectifs de politique étrangère plus larges (droits de l'homme, politique de développement, etc.). Par conséquent, cela soulève également la question de savoir comment l'exportation de biens et de technologies utilisables dans la cyberguerre doit être traitée.

Les équipements et technologies utilisés pour la cyberguerre sont en grande partie des biens à double usage, c'est-à-dire des biens qui peuvent être utilisés à la fois à des fins civiles et militaires. À cet égard, ils présentent des caractéristiques similaires aux biens à double usage dans le domaine de la technologie des missiles ou dans les

14 Vgl. Basismassnahmen der Cyber-Sicherheit des deutschen Bundesamtes für Sicherheit in der Informationstechnik: https://docplayer.org/114578396-Basismassnahmen-der-cyber-sicherheit.html

15 Artikel 5 Kriegsmaterialverordnung (https://www.fedlex.admin.ch/eli/cc/1998/808_808_808/de)

secteurs nucléaire, biologique et chimique, où il existe des régimes internationaux de contrôle des exportations. La Suisse est généralement favorable à des mesures de contrôle multilatérales contre la prolifération indésirable des biens à double usage. Un tel régime de contrôle n'existe pas pour la cybertechnologie. Certains equipements et technologies sont contrôlés dans le cadre de l'Arrangement de Wassenaar. Il y a peu de chances que des contrôles multilatéraux efficaces des exportations soient réalisables dans un avenir prévisible, que ce soit dans le cadre de Wassenaar ou dans un autre. Il est probable que les États-Unis, la Chine et l'Union Européenne introduiront des contrôles unilatéraux et feront pression sur des pays tiers tels que la Suisse, ce qui peut être délicat du point de vue de la politique de neutralité ou, en cas de conflit, de celui du droit de la neutralité[16] .

Sanctions

Le Conseil de sécurité des Nations unies a le pouvoir d'imposer des sanctions qui sont juridiquement contraignantes pour tous les États. Ces derniers peuvent également imposer des sanctions, seuls ou conjointement avec d'autres, afin de poursuivre des objectifs de politique étrangère, tels que le respect du droit international ou le respect des droits de l'homme. Ces sanctions n'ont que rarement un lien avec le droit de la neutralité. Cependant, comme pour les contrôles à l'exportation, elles peuvent affecter la crédibilité de l'État neutre. Cela vaut également pour les sanctions qui seraient prises à l'encontre des cyber-opérations.

Interdiction de fournir des troupes ou des mercenaires aux parties belligérantes

Les États neutres ne peuvent pas fournir des troupes ou des mercenaires aux belligérants, ni autoriser leur recrutement sur leur propre territoire.

Comment un État neutre doit-il se comporter à l'égard des entreprises privées et des particuliers qui sont actifs sur son territoire dans le domaine de la cybersécurité et

16 gl. Holzer, Patrick Edgar (2020): Das Güterkontrollgesetz (Definitionen im Güterkontrollgesetz. In: Cottier, Thomas, Oesch, Matthias (Hrsg.) Schweizerisches Bundesverwaltungsrecht Band XI, Allgemeines Aussenwirtschafts- und Binnenmarktrecht. Basel: Helbing Lichtenhahn Verlag, 147-230. Publications de l'Arrangement de Wassenaar: https://www.wassenaar.org/de/

qui mettent à disposition des technologies ou des services pour des cyberopérations ? Dans ce domaine, les dispositions du droit de la neutralité échappent en partie à l'interdiction de la discrimination et nécessitent des interdictions spécifiques. Le problème est analogue à celui des sociétés de sécurité privée. Il est donc utile d'approfondir la question par analogie avec le document et le processus de Montreux - non seulement du point de vue de la sécurité humaine, mais aussi de celui de la neutralité[17] .

Il est également nécessaire de clarifier des termes tels que soldats et mercenaires. Que signifient-ils dans le contexte de la cyberguerre ? S'agit-il exclusivement de personnes qui utilisent les ressources numériques comme moyen de lutte ? Ce terme couvre-t-il également les robots (bots), les fermes de robots (bot farms), etc.? Et qu'en est-il de la responsabilité de l'État dans ce contexte ?

Interdiction de mettre le territoire national à la disposition des parties belligérantes

Il est interdit aux Etats neutres de mettre leur territoire national à la disposition des parties belligérantes. Cette obligation est une interdiction qui va au-delà du principe d'égalité de traitement (interdiction de discrimination).

La Convention de La Haye du 18 octobre 1907 contient des dispositions sur les communications radio sans fil. Selon ces dispositions, les États neutres ne peuvent pas autoriser de telles installations sur leur territoire si elles servent à la communication entre les forces armées des États belligérants (article 3). En revanche, ils ne sont pas tenus d'interdire aux belligérants d'utiliser leur territoire pour les autres communications radio sans fil (article 7)[18] .

Par analogie, cela signifierait probablement que l'Etat neutre ne doit pas permettre l'utilisation de son infrastructure (serveurs, réseaux de communication, etc.) pour la cyberguerre d'autres États. Toutefois, même en cas de conflit armé, il ne serait pas obligéd'empêcher toute utilisation (c'est-à-dire également civile) de ses capacités en

17 Voir DFAE, Document de Montreux: https://www.eda.admin.ch/eda/fr/dfae/politique-exterieure/droit-international-public/droit-international-humanitaire/entreprises-militaires-securite-prives/document-montreux.html)

18 Convention concernant les droits et les devoirs des Puissances et des personnes neutresen cas de guerre sur terre: https://www.fedlex.admin.ch/eli/cc/26/499_376_481/fr

matière de TIC. Une telle délimitation n'est pas simple et nécessite des éclaircissements ; on pense, par exemple, aux opérations d'information dans le contexte de la guerre hybride, où il n'est souvent pas possible de déterminer l'infrastructure TIC par laquelle l'information est diffusée.

Il convient de noter dans ce contexte que les experts de l'ONU exigent que les États ne permettent pas sciemment l'utilisation des TIC sur leur territoire à des fins contraires au droit international[19] .

4. DES PISTES DE RÉFLEXION POUR LA PAIX ET UNE PLUS GRANDE SÉCURITÉ DANS LE CYBERESPACE

La politique de neutralité suisse façonne la politique étrangère suisse bien au-delà des principes fondamentaux du droit de la neutralité et au-delà des doctrines de la neutralité. Elle est ancrée dans l'expérience historique et la culture politique de la Suisse. Il n'y a aucune raison d'abandonner ces traditions en raison de nouvelles formes de conflit. Au contraire, il est nécessaire de réfléchir à la manière dont les contributions à la paix et à la sécurité peuvent être apportées à l'ère de la cyberguerre.

L'éventail des activités possibles est large. Les sections qui suivent ne portent nullement sur tous les domaines d'activité possibles dans le cyberespace, mais elles fournissent quelques pistes qui méritent d'être prises en considération.

Bons offices

Les États neutres sont particulièrement aptes à fournir des bons offices. Aujourd'hui, on entend par là toutes sortes d'assistance à des tiers (mandats de puissance protectrice, accueil de conférences et d'organisations internationales, établissement

19 "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs … States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts;" (UN GGE Report 2015)

de faits, contribution au règlement pacifique de différends, etc.).

Le soutien financier aux activités d'enquête (attribution des cyberincidents jusqu'à la vérification des faits en rapport avec les opérations d'information) est un domaine d'activité qui pourrait s'inscrire dans la tradition des bons offices. Il en va de même pour le soutien d'initiatives telles que FIRST ("Forum for Incident Response and Security Teams")[20] .

La promotion de la Suisse en tant que centre de gouvernance et les efforts visant à faire de Genève une plaque tournante de la coopération dans le domaine numérique s'inscrivent également dans ce cadre[21] . Les synergies avec les structures multilatérales existantes peuvent être exploitées à cette fin.

Mesures de confiance

Les mesures de confiance, qui ont un grand potentiel pour prévenir et atténuer les conflits, sont souvent prévues dans le cadre d'accords internationaux ou dans celui d'organisations internationales. Un État neutre peut apporter un soutien efficace en utilisant sa crédibilité pour présenter des propositions et, si nécessaire, mettre en œuvre lui-même des mesures de confiance.

Lors des délibérations dans le cadre des Nations unies, un consensus a été trouvé sur le fait qu'une meilleure coopération et une plus grande transparence sont de nature à réduire les risques de conflit[22] . Des mesures volontaires de renforcement de la confiance ont également été identifiées. Bien que la responsabilité principale incombe aux États, il est important que le secteur privé, les milieux scientifiques et la société civile soient également impliqués dans la recherche de solutions. La Suisse peut y apporter une contribution particulière grâce à ses relations directes

20 Le "Forum for Incident Response and Security Teams" (FIRST) est une association internationale de centres d'alerte et de réaction aux attaques informatiques (CERT) qui travaillent ensemble pour échanger des informations techniques relatives à la sécurité. Il comprend plus de 220 membres de 42 pays. Les membres des équipes de réponse aux incidents représentent des gouvernements, des organismes chargés de l'application de la loi, des universités, le secteur privé et d'autres institutions.

21 Stratégie de politique extérieure numérique 2021–2024: https://www.eda.admin.ch/dam/eda/fr/documents/publications/SchweizerischeAussenpolitik/20201104-strategie-digitalaussenpolitik_FR.pdf

22 UN GGE Report 2015

et sereines avec ces groupes d'intérêt, comme elle l'a déjà fait, par exemple, dans le cadre du développement des mesures de confiance pour le cyberespace[23] .

Engagement et assistance humanitaire

La cyberguerre peut causer des pertes de vies humaines et des destructions physiques qui nécessitent une aide humanitaire, comme dans les conflits conventionels.

Est-il approprié, dans la logique de l'assistance aux États attaqués, d'envisager un cadre plus large d'assistance, par exemple sous la forme de capacités de cybersauvetage ?

Une autre forme d'assistance envisageable serait le soutien au renforcement des capacités en matière de cybersécurité. La protection des infrastructures essentielles constitue un défi énorme, en particulier pour les pays en développement, car ils sont à leur tour de plus en plus dépendants des capacités numériques. Au-delà du renforcement des capacités techniques, cela implique également des conseils législatifs, des mesures réglementaires et l'élaboration de stratégies efficaces en matière de cybersécurité[24]. Dans le cadre des Nations unies, de telles formes de coopération sont préconisées et même soutenues. Cependant, la coopération n'en est qu'à ses débuts. Le fait que les programmes de cybersécurité ne soient pas éligibles au titre de l'aide publique au développement (APD) selon les critères du CAD de l'OCDE complique la situation. La Suisse pourrait coopérer avec des pays partageant les mêmes idées pour améliorer la situation. L'expérience avec le Covid-19 a mis en évidence l'importance des réseaux numériques pour les pays en développement et a permis d'accroître le travail de sensibilisation.

Une forme efficace de coopération et de soutien qui mérite d'être examinée est la création d'équipes d'intervention en cas d'urgence informatique (CERT), qui sont déployées pour résoudre des incidents de sécurité technologiques spécifiques. Il est également important que cette forme de coopération dans le domaine civil ne soit pas entravée par des sanctions existantes. En tant qu'État neutre, la Suisse est

23 Voir ICT4Peace Paper: CONFIDENCE BUILDING MEASURES AND INTERNATIONAL CYBER SECURITY (Geneva 2013), préparé avec le soutien du DFAE. https://ict4peace.org/wp-content/uploads/2019/08/ICT4Peace-2013-Confidence-Building-Measure-And_Intern-Cybersecurity.pdf

24 Voir International ICT4Peace Cyber Security Policy and Diplomacy Capacity Building Program https://ict4peace.org/wp-content/uploads/2021/01/Cybersecurity-Policy-and-Diplomacy-Capacity-Building-25-January-2021-2.pdf

également bien placée pour répondre à ces préoccupations.

Normes dans le cyberespace et renforcement du droit international

La Suisse fonde ses relations internationales sur le droit et non sur la puissance. Elle s'intéresse particulièrement aux normes contraignantes dans le cyberespace. Cela s'applique également en cas de conflits armés dans le cyberespace.

Des efforts pour renforcer le droit sont déjà en cours au niveau international. Dans ce domaine, comme dans d'autres domaines du droit international humanitaire, le respect et l'application des normes juridiques sont particulièrement importants. C'est aussi un domaine d'action intéressant pour la Suisse, qui a une dimension politique, juridique et technique[25] .

5. CONCLUSION

Ce document de travail pose plus de questions qu'il n'apporte de réponses. C'est son but. Il ne s'agit pas de fournir des plans directeurs ou de faire des déclarations inaccessibles, mais de poser des questions qui, espérons-le, susciteront des commentaires et des répliques. Le moment est opportun en raison du retour de la rivalité entre grandes puissances et des transformations technologiques fondamentales à venir. Les États européens, y compris la Suisse, pays neutre, seront fortement touchés par cette évolution.

Les réponses aux nombreuses questions soulevées dans ce texte, ainsi que les concepts et les doctrines qui les sous-tendent finiront par faire émerger des décisions politiques concrètes. C'est pourquoi il est nécessaire de traiter ces questions à temps et de manière approfondie.

La problématique de la neutralité dans la cyberguerre est l'objet principal de ce

25 Voir les contributions de ICT4Peace à l'appui des normes de comportement responsable des États et des mesures de renforcement de la confiance dans le cyberespace: https://ict4peace.org/activities/norms-of-responsible-state-behavior/?load=all

texte. Depuis toujours, celle-ci est remise périodiquement en question suite aux changements géopolitiques et aux innovations dans le domaine des armements. Après la création de la Société des Nations et plus tard des Nations Unies, avec l'avènement des armes nucléaires ou après la guerre froide, la fin de la neutralité suisse était annoncée. En fait, elle s'est révélée être non seulement un guide politique sûr, mais aussi une grille de réflexion utile qui permet d'aborder les questions essentielles que nous devons traiter dans le contexte des conflits et de leur prévention. Cela est certainement également vrai à l'ère de la cyberguerre.

About ICT4Peace Foundation

ICT4Peace is a policy and action-oriented international Foundation. The purpose is to save lives and protect human dignity through Information and Communication Technology. Since 2003 ICT4Peace explores and champions the use of ICTs and new media for peaceful purposes, including for peacebuilding, crisis management and humanitarian operations. Since 2007 ICT4Peace promotes cybersecurity and a peaceful cyberspace through inter alia international negotiations with governments, international organisations, companies and non-state actors.

The ICT4Peace project was launched with the support of the Swiss Government in 2003 with the publication of a book by the UN ICT Task Force on the practice and theory of ICT in the conflict cycle and peace building in 2005 and the approval of para 36 of the Tunis Commitment of the UN World Summit on the Information Society (WSIS) in 2005.

ICT4Peace on Twitter - www.twitter.com/ict4peace

ICT4Peace on Facebook - www.facebook.com/ict4peace

ICT4Peace official website: www.ict4peace.org

ICT4Peace additional publications: www.ict4peace.org/publications

ICT for peace foundation