Cyber

Neutralité dans le cyberespace : Un défi pour la Suisse

Martin Dahinden et Sara Pangrazzi

Ancien ambassadeur ; chercheuse à l'UNIZH

L'ampleur des cyberattaques connait une croissance exponentielle : le fameux *malware WannaCry*, par exemple, a infecté plus de 200'000 ordinateurs dans le monde en peu de temps depuis sa découverte en mai 2017 et a fait la une des journaux internationaux. Des ordinateurs appartenant au ministère russe de l'intérieur, à de nombreux hôpitaux du Royaume-Uni, au constructeur automobile Renault-Nissan ainsi qu'à la Deutsche Bahn ont été touchés. Le programme a exploité une faille de sécurité dans le système d'exploitation Windows, qui est largement utilisé dans le monde entier, et a causé des milliards de dollars de dommages. L'administration fédérale suisse est également confrontée régulièrement à des attaques numériques : en septembre 2017 selon un communiqué de presse, des cyberattaques ont été découvertes au sein du Département de la défense (DDPS), et en janvier 2016, des attaques ont conduit au vol de plus de 20 giga-octets de données de la société d'armement Ruag. Les investigations numériques pour déterminer l'origine de ces cyberattaques occupent les spécialistes aujourd'hui encore. Afin de faire face à ces risques, les Etats mettent à niveau leurs capacités informatiques militaires. La Suisse développe également ses capacités numériques et prévoit de mettre en place un Commandement cyber. Cependant, comme il existe encore de nombreuses incertitudes concernant l'application des normes internationales aux cyberattaques, il faut, en plus des défis techniques, faire face à des défis juridiques et politiques considérables.

Les cyberattaques peuvent-elles être comparées à des attaques armées ?

Avec le Commandement cyber, le Conseil fédéral cherche à renforcer la défense numérique de l'armée suisse. L'ordonnance sur la cyberdéfense militaire (OCMil), qui est entrée en vigueur le 1er mars 2019, régit les actions dans le cyberespace visant l'autoprotection et la « légitime défense » de l'armée suisse contre les cyberattaques. Mais qu'entend-on par légitime défense en rapport avec les cyberattaques ? Les mesures de légitime défense contre d'autres Etats doivent non seulement répondre aux exigences du droit national, mais doivent aussi toujours être autorisées par le droit international – en particulier lorsqu'elles vont au-delà de la protection et comprennent des mesures de défense offensives.

En 2013 et 2015 déjà, des groupes d'experts mis en place par l'ONU ont déclaré que le droit international traditionnel, et donc la Charte des Nations unies, était applicable au cyberespace. Toutefois, il existe toujours un désaccord sur la manière dont ces normes devraient être appliquées concrètement. La complexité et la nouveauté de la question, ainsi que les intérêts politiques divergents, font qu'il est extrêmement difficile pour les Etats de parvenir à un consensus. Une question clé est de savoir si et à quelle intensité les cyberattaques constituent des attaques armées au sens de l'article 51 de la Charte des Nations unies, constituant ainsi des actes de guerre. Seuls de tels actes légitimeraient des actions offensives de légitime défense, qui pourraient également être menées par des moyens militaires en dehors du cyberespace. Ce droit à la légitime défense est une exception à l'interdiction fondamentale de l'emploi de la force entre Etats. La plupart des Etats affirment que les cyberattaques peuvent constituer des actes de guerre si elles produisent les mêmes effets que des attaques armées conventionnelles. Cependant, il y a un désaccord sur les effets qui relèvent du contexte numérique. Selon la conception traditionnelle du droit international, les

Martin Dahinden a été ambassadeur de Suisse aux Etats-Unis, est membre du conseil d'administration du groupe de réflexion *ICT4Peace* et enseigne la politique de sécurité à l'Université de Zurich ; Sara Pangrazzi mène des recherches sur la cybersécurité à l'Institut de droit international de l'Université de Zurich.

attaques armées entraînent des destructions physiques et/ou infligent la mort. Le Conseil de sécurité des Nations unies n'a jamais jugé que des dommages économiques ou politiques étaient suffisants pour être comparés à une attaque armée.

La difficulté rencontrée dans la confrontation entre les normes traditionnelles du droit international et les cyberattaques provient en premier lieu du fait que les attaques numériques ne sont pas « armées » au sens traditionnel du terme. En principe, elles provoquent des dysfonctionnements dans les systèmes informatiques, ce qui signifie que les dommages ne sont pas, pour l'essentiel, de nature physique. Les dommages causés indirectement par la perte de données, la manipulation d'informations ou la manipulation de logiciels sont également pour la plupart non physiques et généralement difficiles à quantifier. De plus, à ce jour, il y a eu très peu de destructions à grande échelle causées par des cyberattaques qui pourraient même être comparées aux effets d'une attaque armée. Les cyberattaques ne répondent donc que rarement – voire jamais – aux exigences de l'article 51 de la Charte des Nations unies. On est régulièrement en dehors du champ de la légitime défense si les cyberattaques n'entraînent pas de destruction physique et/ou ne causent pas la mort. Les cyberattaques sont techniquement difficiles à tracer et ne peuvent parfois pas être clairement attribuées à un Etat d'un point de vue légal. Cela est compliqué par le fait qu'elles font souvent partie d'une guerre hybride qui inclut à la fois des acteurs étatiques et non étatiques. Les cyberattaques touchent souvent les territoires de plusieurs États en même temps. Dans la plupart des cas, il n'est même pas tout à fait clair s'il s'agit d'une attaque ciblée ou de dommages collatéraux liés à une attaque, car d'une manière générale, les vers informatiques se propagent de façon autonome à de nombreux systèmes.

De surcroit, les attaquants utilisent souvent l'infrastructure de (nombreux) tiers non impliqués comme tête de pont pour rester anonymes. En raison des difficultés techniques et juridiques liées à l'attribution d'une cyberattaque, la désignation de leurs auteurs réels restera souvent empreinte de doute. Les contre-attaques peuvent facilement affecter des pays tiers non impliqués. Il semble donc qu'une grande retenue s'impose. La neutralité de la Suisse pose des défis supplémentaires. En plus des normes générales du droit international, les obligations liées à la neutralité doivent également être respectées. Le droit de la neutralité impose à la Suisse de ne pas participer à la guerre, de garantir l'égalité de traitement des belligérants et de ne pas mettre son territoire à la disposition des parties en guerre. Qu'est-ce que cela signifie dans le contexte du cyberespace ? En raison de la mise en réseau croissante des infrastructures dans le monde entier et de la distribution mondiale de programmes numériques, les cyberattaques des belligérants transitent fréquemment par des infrastructures privées et/ou publiques neutres. Cela soulève des questions délicates sur les obligations de diligence d'un Etat neutre en vertu du droit international. Un Etat est en principe responsable des violations du droit international par un autre Etat émanant de son territoire s'il en a connaissance et s'il a la capacité de les prévenir ou de les faire cesser. Dans quelle mesure ces normes de diligence raisonnable sont applicables dans le cyberespace est controversé.

Rester crédible – mais comment ?

Le statut de neutralité a par ailleurs des effets en temps de paix déjà. Un Etat qui exerce une neutralité permanente, comme la Suisse, ne peut prendre aucun engagement qui mettrait en danger sa neutralité ou sa crédibilité en cas de conflit. A l'heure actuelle, il n'est pas clair comment ces obligations doivent être appliquées dans le domaine cybernétique et quelles sont les possibilités et les limites de la coopération internationale. Dans le contexte de l'obligation de diligence raisonnable, le contrôle des technologies numériques (à double usage) constitue également un défi particulier. Une question qui se pose est notamment celle des mesures de contrôle nécessaires pour que la Suisse puisse remplir ses obligations de neutralité ainsi que d'autres objectifs de politique étrangère lorsqu'elle produit ou transmet de telles technologies, et dans quelle mesure elle est responsable si ces technologies sont utilisées en violation du droit international. En tant que petit Etat neutre, la Suisse a un intérêt certain à clarifier l'application des normes du droit international dans le cas de cyberattaques et que l'ONU joue un rôle efficace en tant qu'organisation de sécurité collective dans ce domaine. Dans la perspective de la mise en place d'un Commandement cyber, il s'agit notamment de clarifier le droit de légitime défense selon le droit international dans le cas de telles attaques. Toutefois, cela ne résoudra pas les questions liées à la neutralité. Pour que la Suisse puisse se positionner de manière crédible en tant qu'Etat neutre en termes de politique étrangère, elle doit s'efforcer de traiter davantage les aspects de la politique de cybersécurité liés à la neutralité. Le projet de la Suisse d'augmenter ses capacités numériques avec un Commandement cyber souligne cette nécessité.

M. D. et S. P.

Publié dans la *Neue Zürcher Zeitung*: 30.12.2020
Neutralität im Cyberraum: Die Schweiz ist gefordert | NZZ

Traduction et adaptation française :
Claude MEIER, François CHAMBETTAZ, Marc-André RYTER