

Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2021)
Heft: 1

Artikel: Neutralité dans le cyberspace : un défi pour la Suisse
Autor: Dahinden, Martin / Pangrazzi, Sara
DOI: <https://doi.org/10.5169/seals-977656>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

Download PDF: 15.01.2026

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>

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.

Desurcroît, 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 cyberspace ? 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 cyberspace 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