L'OTAN et l'article 5 dans le cyberespace

L'OTAN a désigné le cyberespace comme un domaine de guerre et a reconnu qu'une cybercampagne ennemie pourrait déclencher le mécanisme de défense collective de l'Alliance en vertu de l'article 5. Compte tenu de la complexité des cyberattaques et des difficultés à y répondre, on ne peut dire avec certitude dans quelle mesure une cyberattaque pourrait déclencher une réponse de défense collective de la part de l'Alliance.

Par Sarah Wiedemar

Le Cooperative Cyber Defence Centre of Exellence (CCDCOE) de l'OTAN à Tallinn, en Estonie, lors de l'exercice de cyberdéfense Locked Shields, en avril 2019. *Ints Kalnins / Reuters*

Au sommet de l'OTAN au Pays de Galles il y a près de dix ans, l'OTAN a reconnu la cyberdéfense comme un élément indissociable de la défense collective. Par conséquent, une cyberattaque contre un ou plusieurs États membres est susceptible de déclencher la clause de défense collective de l'Alliance inscrite à l'article 5 du traité de Washington, pierre angulaire de l'alliance militaire. L'article 5 repose sur le principe qu'une attaque contre un État membre est considérée comme une attaque contre tous les États membres et que les Alliés, en exerçant leur droit de légitime défense individuelle ou collective tel que reconnu à l'article 51 de la Charte des Nations unies, peuvent prendre des mesures pour rétablir la sécurité de la région de l'Atlantique Nord. Une fois le mécanisme déclenché par un ou plusieurs États membres, le Conseil de l'Atlantique Nord (CAN), principal organe décisionnel de l'Alliance, doit décider à l'unanimité si l'attaque justifie le recours à l'article 5. Si tel est le cas, il appartient à chaque membre de déterminer comment réagir et dans quelle mesure, de concert avec les autres partenaires de l'OTAN. Depuis la création de l'OTAN en 1949, l'article 5 n'a été invoqué qu'une seule fois, à la suite des attentats terroristes du 11 septembre 2001.

La mission primordiale de l'OTAN consiste à préserver la liberté et la sécurité de ses États membres par des moyens politiques et militaires. L'article 5 s'appliquant également au cyberespace, l'Alliance a reconnu que les cyberattaques étaient susceptibles d'atteindre un seuil qui menacerait la prospérité, la sécurité et la stabilité nationales et euro-atlantiques. L'OTAN n'a pas fixé de lignes rouges spécifiques qui, une fois franchies, conduiraient à invoquer l'article 5. Au lieu de cela, la posture de l'Alliance repose sur une ambiguïté stratégique et est guidée par le principe du cas par cas pour chaque attaque. Selon la portée et l'ampleur de l'attaque ou de la campagne, la volonté politique de chaque État membre guiderait la réponse de l'OTAN, qui pourrait donc aller de représailles diplomatiques et économiques à des cyberopérations offensives ou à des frappes militaires. Si une certaine souplesse dans l'application de l'article 5 est essentielle à l'intégrité de l'Alliance, elle est également la cause d'une certaine incertitude spécifique à la question

© 2023 Center for Security Studies (CSS), ETH Zürich

du cyberespace. Déterminer les effets d'une attaque, ses auteurs et les intentions politiques qu'ils poursuivent est généralement considéré comme plus difficile dans le cyberespace que dans l'espace réel.

En été 2022, à la suite d'une cybercampagne perturbatrice contre l'Albanie, État membre de l'OTAN, le Premier ministre albanais Edi Rama a envisagé de se tourner vers le CAN pour invoquer l'article 5 comme option de réponse. Le déclenchement par l'Albanie de l'article 5 aurait été la première entrée en vigueur de la clause de défense collective de l'OTAN en réponse à une cyberattaque, créant de fait un précédent pour l'Alliance dans son ensemble. Bien que le gouvernement albanais se soit finalement abstenu de soulever la question avec le CAN, l'incident a néanmoins suscité de nouvelles discussions sur la manière dont l'article 5 devrait s'appliquer dans le cyberespace.

L'OTAN et la cybersécurité

Après une vague d'attaques par déni de service distribué (DDoS, voir encadré à la page 3), de dégradations de sites web et de campagnes de spam par courrier électronique visant les institutions de l'OTAN et des États membres à la suite de l'opération Force alliée en 1999 (voir encadré à la page 2), les États membres ont compris qu'ils devaient améliorer leurs capacités de cybersécurité et de défense pour protéger leurs propres systèmes d'information et de communication.

En 2021, l'OTAN a reconnu que l'impact d'importantes cyberactivités malveillantes cumulatives pourrait être considéré comme équivalant à une attaque armée.

C'est en partie grâce à cette expérience que l'Alliance a inscrit pour la première fois le cyberespace à l'ordre du jour politique du sommet de l'OTAN à Prague en 2002. L'OTAN y a également adopté le programme de cyberdéfense, qui a donné le coup d'envoi à la création de la capacité OTAN de réaction aux incidents informatiques (NCIRC), dont la tâche est de prévenir, de détecter et de répondre aux cyberincidents affectant l'Alliance. Mais ce n'est qu'avec la campagne DDoS sans précédent en 2007 contre l'Estonie, membre de l'OTAN, que l'Alliance a pris conscience de l'ampleur de la menace et des implications politiques qui peuvent émerger du cyberespace (voir encadré à la page 2). La demande d'assistance de l'Estonie à la suite de la campagne DDoS a été un signal d'alarme pour l'OTAN. Dix mois plus tard, lors du sommet de l'OTAN à Bucarest, les Alliés ont approuvé leur première politique en matière de cyberdéfense. Les États membres ont reconnu la nécessité pour l'OTAN non seulement de protéger les systèmes d'information essentiels pour l'Alliance, mais aussi de partager leurs bonnes pratiques et de fournir un soutien aux Alliés en cas de cyberattaque. Des préoccupations ont également été soulevées quant à savoir si une cyberattaque pourrait devenir un élément important dans la capacité à mener une guerre et, le cas échéant, dans quelle mesure. Au sommet de l'OTAN de 2014 au Pays de Galles, les États membres ont déclaré que la cyberdéfense faisait partie de la tâche fondamentale de défense collective de l'OTAN. Et au sommet de l'OTAN à Varsovie en 2016, l'Alliance a renforcé cet engagement en déclarant que le cyberespace était un nouveau milieu d'opérations, en plus de l'air, de la terre et de la mer.

Au sommet de l'OTAN à Bruxelles en 2021, l'Alliance est allée plus loin et a reconnu que, dans certaines circonstances, les incidences d'actes de cybermalveillance majeurs aux effets cumulés sont telles que ces actes peuvent être considérés comme équivalant à une attaque armée. Ce passage à une approche cumulative a probablement été adopté en réaction à la vague de campagnes de rançongiciels (voir encadré à la page 3) contre l'infrastructure numérique des États-Unis et d'autres États membres de l'OTAN qui a touché presque tous les secteurs des infrastructures critiques, y compris les soins de santé, l'agriculture et l'énergie.

L'article 5 et la cyberdéfense

Le 25 février 2022, au lendemain de l'invasion de l'Ukraine par la Russie, le secrétaire général de l'OTAN, Jens Stoltenberg, s'est empressé de réaffirmer que la cyberdéfense est une partie indissociable de la défense collective et de souligner que l'Alliance ne donnera pas à un adversaire potentiel le privilège de définir à quel moment l'article 5 serait déclenché. Bien que l'article 5 s'applique également aux cyberattaques, les particularités du cyberespace créent une multitude de défis supplémentaires. Par exemple, la question de l'attribution, c'est-à-dire déterminer qui est exactement responsable d'une cyberattaque, est à la fois fastidieuse et chronophage sans pouvoir forcément atteindre le niveau de certitude nécessaire pour justifier légalement des réponses politiques ou militaires spécifiques (voir analyse du CSS no 244). De même, la diversité des relations et des quasi-liens entre les acteurs étatiques et non étatiques dans le domaine cybernétique, ainsi que l'emplacement physique à partir duquel ils opèrent, soulèvent des questions quant aux cibles et aux motifs des sanctions.

Un autre problème fondamental découle de la position d'ambiguïté stratégique de l'OTAN. Le Manuel de Tallinn 2.0, un document d'expert sur la manière dont le droit international pourrait s'appliquer au cyberespace, définit une cyberattaque comme une cyberopération, qu'elle soit offensive ou défensive, dont on peut raisonnablement attendre qu'elle blesse ou tue des individus, qu'elle induise des dommages ou détruise des biens. Le Manuel précise également

L'OTAN et les cyberattaques dans le passé

L'opération Force alliée de 1999: Pendant la guerre du Kosovo (1998/1999), la campagne militaire de l'OTAN *opération Force alliée* visait à forcer l'armée serbe à quitter le Kosovo. Divers groupes d'hacktivistes nationalistes de Serbie, de Russie et de Chine (en particulier après l'attentat à la bombe contre l'ambassade de Chine à Belgrade le 7 mai 1999) ont tenté de perturber la capacité de combat de l'OTAN par une série d'attaques par déni de service distribué DDoS (voir encadré à la page 3) et de dégradations de sites web.

Estonie, 2007: En 2007, l'Estonie, membre de l'OTAN, a connu une campagne DDoS persistante menée par des hacktivistes russes patriotes qui a duré 22 jours et a ciblé une multitude de réseaux publics et privés estoniens, y compris le système estonien d'administration en ligne, des banques et des médias. L'incident s'est produit peu de temps après le déplacement d'une statue controversée de la Seconde Guerre mondiale du centre de Tallinn, qui symbolisait pour la minorité russophone le Jour de la Victoire, tandis que pour les Estoniens de souche, elle rappelait l'occupation et la répression soviétique. Ce type de campagne DDoS soutenue, couplé à l'environnement géopolitique tendu, était sans précédent à l'époque.

© 2023 Center for Security Studies (CSS), ETH Zürich

qu'il n'est pas nécessaire qu'une attaque entraîne des dommages physiques à des biens ou à des individus. Pendant assez longtemps cependant, on partait de l'hypothèse commune que, pour susciter une réponse militaire légale, les effets d'une cyberattaque devaient être équivalents à ceux d'une frappe cinétique pour franchir le seuil d'une attaque armée.

Depuis le sommet de Bruxelles de 2021, l'OTAN a adapté son point de vue sur cette question. Aujourd'hui, l'Alliance affirme que l'impact de multiples cyberactivités malveillantes menées en dessous du seuil d'une attaque armée peut s'accumuler jusqu'à atteindre un impact significatif et peut donc constituer une attaque armée susceptible de faire l'objet d'une action collective en vertu de l'article 5. En raison de ce changement, il est devenu encore plus difficile de définir les cyberactivités ennemies qui pourraient relever du champ d'application de l'OTAN. Une simple comparaison avec une frappe cinétique n'est plus suffisante. Se posent également des questions non résolues quant à ce qui pourrait suivre si l'article 5 était déclenché en réponse à une cyberattaque. En raison de l'approche au cas par cas de l'OTAN, on ne peut dire avec certitude si les Alliés sont actuellement d'accord ou pourraient parvenir à un consensus sur le type ou les effets de cyberattaques ainsi que le type d'impacts graves qui seraient éligibles pour invoquer l'article 5.

Cyberattaques: Aperçu de méthodes et d'outils

Une **attaque par déni de service distribué (DDoS)** est un type d'attaque dans le cadre de laquelle le serveur, le service ou le réseau cible est surchargé par un trafic provenant de plusieurs sources, par exemple, un groupe d'appareils. L'objectif d'une DDoS est de rendre le système de la victime inaccessible.

Les **rançongiciels** sont des logiciels malveillants utilisés pour chiffrer des données ou en bloquer l'accès afin d'exiger que l'utilisateur paie pour déverrouiller ou déchiffrer les données et pouvoir les récupérer. Différents types de logiciels malveillants peuvent cibler les systèmes de bureau et les appareils mobiles. Les rançongiciels ciblent à la fois les individus et les organisations. Dans tous les cas, une attaque réussie entraîne des temps d'arrêt et des coûts pour la récupération des données. Toutefois, les dommages causés par les rançongiciels ne sont pas toujours réversibles. Par exemple, le rançongiciel peut s'avérer être un wiper, c'est-à-dire un type de logiciel malveillant qui détruit ou endommage irrémédiablement les données.

Les **menaces persistantes avancées (advanced persistent threats, APT)** sont des attaques concertées contre des organisations spécifiques. Généralement, les attaques APT sont commanditées par les gouvernements et utilisent des logiciels malveillants sophistiqués pour pénétrer les défenses de sécurité d'une organisation.

Un **wiper** est un type de logiciel malveillant qui vise à effacer les données du disque dur de l'ordinateur qu'il infecte.

Source: Kaspersky IT Encyclopedia

Il y a également des questions non résolues quant à ce qui pourrait suivre si l'article 5 était déclenché en réponse à une cyberattaque.

Peu de clarté

Les cybercampagnes malveillantes passées visant ou affectant indirectement les membres de l'OTAN n'ont pas suscité de grands débats publics sur l'article 5, à l'exception du cas de l'Albanie. Les trois cas suivants, l'attaque par rançongiciels de Colonial Pipeline en 2021, le piratage de Viasat en 2022 et la cybercampagne destructrice contre l'Albanie en 2022, illustrent la complexité à laquelle l'OTAN est confrontée en matière de cyberincidents.

En 2021, les États-Unis et d'autres pays occidentaux ont été confrontés à une vague de campagnes de rançongiciels dans leurs secteurs d'infrastructures critiques. La campagne de rançongiciels menée par le groupe cybercriminel russe DarkSide contre Colonial Pipeline en mai 2021 est probablement la plus connue. Colonial Pipeline est le plus grand exploitant de pipelines aux États-Unis. DarkSide a pénétré le réseau informatique de l'entreprise, a réussi à exfiltrer une grande quantité de données, puis a déployé un rançongiciel contre le système de facturation et de comptabilité de Colonial Pipeline. En réaction à l'intrusion, la société a suspendu toutes ses opérations de pipeline pour contenir l'attaque, ce qui a provoqué des pénuries temporaires de carburant et des embouteillages le long de toute la côte est des États-Unis. En conséquence, le président américain Joe Biden a déclaré l'état d'urgence dans dix-huit États, la première déclaration de ce type en réponse à une cyberattaque.

DarkSide est un groupe cybercriminel très prolifique opérant probablement depuis le territoire russe. Selon les spéculations, le groupe pourrait travailler avec des agences gouvernementales russes, mais aucune preuve définitive n'est venue appuyer cette thèse. En réponse à l'attaque, l'administration américaine a décidé de tracer une ligne rouge. Lors de sa réunion au sommet de Genève en juin 2021, le président Joe Biden a remis au président russe Vladimir Poutine une liste de 16 secteurs d'infrastructures critiques américains interdits à toute cyberattaque russe. Joe Biden a précisé que chaque pays devait prendre des mesures contre les cybercriminels opérant à partir de son territoire.

La campagne de rançongiciels contre Colonial Pipeline était un acte cybercriminel commis par un acteur non étatique qui a perturbé des infrastructures critiques, provoqué un état d'urgence et s'est transformé en problème de sécurité nationale aux États-Unis. Malgré cela, l'administration américaine ne s'est pas tournée vers l'OTAN et n'a pas discuté ouvertement de l'article 5. Washington a plutôt choisi d'aborder la question de manière bilatérale.

En février 2022, plusieurs heures avant l'invasion de l'Ukraine, le fournisseur mondial de communications par satellite Viasat a été victime d'une cyberopération offensive probablement menée par l'agence de renseignement militaire russe (GRU). Les attaquants ont ciblé sans discernement les modems de Viasat et ont réussi à effacer les données d'environ 20 000 appareils. L'opération a coupé l'accès à Internet de dizaines de milliers de personnes en Ukraine et d'utilisateurs de Viasat dans au moins treize autres pays européens, les plus grandes interruptions de service ayant touché le Royaume-Uni et la France. En Allemagne, elle a bloqué la surveillance et le contrôle à distance de 5800 éoliennes, affectant la production et la distribution d'électricité. L'attaque a également paralysé temporairement les communications de l'armée, de la police et des services de renseignement ukrainiens, ce qui était probablement l'objectif principal de l'opération.

Le 10 novembre 2022, le secrétaire général de l'OTAN, Jens Stoltenberg, a souligné que le piratage de Viasat avait causé des

© 2023 Center for Security Studies (CSS), ETH Zürich

dommages collatéraux au-delà de l'Ukraine. Les États-Unis, le Royaume-Uni et l'UE ont officiellement attribué le piratage de Viasat au gouvernement russe et ont condamné l'attaque. Selon l'agence de presse Bloomberg, les services de renseignement américains ont estimé que le GRU avait volontairement pris des risques diplomatiques et stratégiques importants, sachant que l'attaque affecterait plusieurs pays en dehors de l'Ukraine. Malgré les retombées de l'attaque et le ciblage aveugle des modems de Viasat dans le contexte d'un conflit armé international, l'Alliance n'a pas délibéré publiquement sur l'application de l'article 5.

Entre mai et septembre 2022, l'Albanie, membre de l'OTAN, a été victime d'une cybercampagne destructrice coordonnée. Les premiers rapports des médias ont attribué la cyberattaque à des cybercriminels russes, dans la foulée d'autres campagnes de rançongiciels à travers le monde. À la suite des investigations menées par Microsoft, Mandiant, le FBI américain et d'autres, la campagne a finalement été attribuée à quatre acteurs différents de menaces persistantes avancées (*advanced persistent threats,* APT) qui sont probablement liés au Ministère iranien du Renseignement et de la Sécurité. Les quatre acteurs d'APT ont utilisé une approche multivectorielle qui comprenait le chiffrement des données (rançongiciels), la suppression des données (wipers, voir encadré à la page 3), l'exfiltration des données et le déversement de données dans le domaine public pour maximiser les effets perturbateurs. Plusieurs sites web et services en ligne du gouvernement albanais, y compris le portail centralisé e-Albania et l'Agence nationale pour la société de l'information, ont été mis hors service par la campagne. Même le système de gestion totale de l'information de la police nationale, qui stocke les données des personnes entrant et sortant d'Albanie, était temporairement indisponible, provoquant des files d'attente à la frontière.

> Dans l'état actuel des choses, l'OTAN est réticente à s'éloigner de l'ambiguïté stratégique.

Le 18 juillet 2022, un groupe ou un personnage en ligne connu sous le nom de Home-Land Justice (HLJ) s'est attribué publiquement le mérite de la campagne destructrice. HLJ a publié des documents du gouvernement albanais et a posté plusieurs vidéos sur sa chaîne Telegram et son site web montrant, entre autres, le déploiement de rançongiciels sur les serveurs albanais. Dans son message public, HJL a déclaré avoir mené les cyberattaques pour exprimer sa colère envers Tirana pour avoir accueilli la conférence annuelle de groupes d'opposition iraniens en Albanie en juillet de la même année. Le logo de HLJ est également particulièrement révélateur en ce qui concerne l'attribution. Il présente un aigle attaquant un oiseau d'Angry Birds (du jeu vidéo du même nom) entouré de l'étoile de David. L'oiseau d'Angry Birds est un symbole utilisé par un autre groupe connu sous le nom de Predatory Sparrow. En juin 2022, Predatory Sparrow a mené une cybercampagne destructrice contre trois usines sidérurgiques iraniennes qui auraient appartenu au Corps des Gardiens de la révolution islamique. Comme l'a noté Predatory Sparrow dans l'une de ses vidéos, ces cyberattaques ont été menées en réaction à l'agression de la République islamique. On ne sait pas si Predatory Sparrow est lié à l'État d'Israël, mais le symbolisme de HLJ suggère que Téhéran pourrait le croire. Dans l'ensemble, il semble que les quatre acteurs d'APT iraniens aient mené leur campagne non seulement pour envoyer un signal au gouvernement albanais de ne pas accueillir de groupes d'opposition iraniens en exil, mais aussi potentiellement en avertissement à Predatory Sparrow et à l'État d'Israël.

À la suite des résultats de l'enquête médico-légale, le gouvernement albanais a rompu toutes ses relations diplomatiques avec Téhéran. C'est la première fois qu'un gouvernement prend une telle mesure en réponse à une cybercampagne destructrice. Au cours des délibérations internes sur la manière de répondre à la campagne, le gouvernement albanais a également discuté de l'article 5 de l'OTAN. Publiquement, le Premier ministre albanais Edi Rama a dénoncé les attaques comme étant en tout point identiques à une agression militaire conventionnelle par d'autres moyens. Cependant, Edi Rama a finalement décidé de ne pas se tourner vers l'OTAN, notant qu'il avait trop de respect pour ses amis et alliés pour leur dire quoi faire.

Perspectives

L'attaque par rançongiciel contre Colonial Pipeline, le ciblage indiscriminé des modems de Viasat et la cybercampagne destructrice contre l'Albanie montrent clairement que l'OTAN est en terrain inconnu en ce qui concerne l'article 5 et le cyberespace. Dans aucun de ces cas, les gouvernements concernés n'ont jugé les campagnes adverses suffisamment importantes pour franchir le seuil d'une attaque armée ou remplir le critère des effets cumulatifs. À ce jour, il est difficile de dire si une cyberattaque causera un jour autant de destruction et de morts à grande échelle que lors du 11 septembre, ou si une telle situation est même nécessaire pour invoquer l'article 5.

Dans l'état actuel des choses, l'OTAN est réticente à s'éloigner de l'ambiguïté stratégique, et les États membres individuels ne semblent pas enclins à créer de précédents lorsqu'il s'agit d'invoquer l'article 5 en réponse à des cyberattaques. L'Alliance doit continuer à gérer l'équilibre consistant à conserver une marge de manœuvre et à maintenir l'unité, d'une part, et à relever les défis et donc faire face aux nouvelles ambiguïtés que le cyberespace comporte, d'autre part.

Voir le site thématique du CSS pour en savoir plus sur la cybersécurité.

Sarah Wiedemar est Researcher dans le Cyberdefence Project au sein du Risk and Resilience Team du Center for Security Studies (CSS) à l'ETH de Zürich.

Les **analyses de politique de sécurité** du CSS sont publiées par le Center for Security Studies (CSS) de l'ETH de Zürich. Le CSS est un centre de compétence en matière de politique de sécurité suisse et internationale. Deux analyses paraissent chaque mois en allemand, français et anglais.

Editeur: Fabien Merz
Révision linguistique: Névine Scheppers
Layout et graphiques: Miriam Dahinden-Ganzoni

Feedback et commentaires: analysen@sipo.gess.ethz.ch
Plus d'éditions et abonnement: www.css.ethz.ch/cssanalysen

Parus précédemment:

Les Nations Unies et la lutte contre le terrorisme No 322
Interdiction des armes biologiques et progrès scientifiques No 321
Armes autonomes et défis réglementaires No 320
LPromesses et écueils des wargames No 319
L'empreinte de la Russie en Afrique No 318
L'«ordre international fondé sur des règles» No 317

© 2023 Center for Security Studies (CSS), ETH Zürich
ISSN: 2296-0228; DOI: 10.3929/ethz-b-000610329