



## La clause d'assistance mutuelle du Traité sur l'Union européenne (article 42§7 TUE) permet-elle de répondre adéquatement aux nouvelles menaces ?

Estelle HOORICKX & Carolyn MOSER<sup>1</sup>

*Cette e-Note s'inspire des analyses personnelles présentées par les auteures à la sous-commission SEDE (sécurité et défense) du Parlement européen, le 29 novembre 2021<sup>2</sup>.*

*Depuis une vingtaine d'années, les États membres de l'Union européenne (UE) affichent une volonté de renforcer leurs capacités de défense européenne. Un élément central à cet égard est la clause d'assistance mutuelle, consacrée depuis 2009 par l'article 42§7 du Traité sur l'Union européenne (TUE). À la suite de l'invasion de l'Ukraine par la Russie en février 2022, le débat autour de l'utilisation de la clause d'assistance mutuelle a pris une nouvelle ampleur, notamment parce que la clause fait partie des instruments de la puissance que l'UE souhaite utiliser pour faire face aux menaces actuelles. Clause invoquée pour la première et unique fois par la France en 2015, son emploi soulève néanmoins des interrogations. La présente note analyse dès lors les modalités d'action dont disposent les États européens, dans le cadre de la clause d'assistance mutuelle, pour faire face aux « nouvelles » menaces, qu'elles soient hybrides, de nature cyber ou qu'elles mettent en œuvre des technologies émergentes sur les différents champs d'affrontement (terre, mer, air, espace et cyber). Même si le déclenchement de la clause n'est pas chose aisée, l'article 42§7 TUE offre une base juridique précieuse pour une réponse collective aux cyberattaques et menaces hybrides, à condition que celles-ci constituent des agressions armées au sens juridique du terme.*

### L'invasion de l'Ukraine relance le débat sur la clause d'assistance mutuelle

Lors du Sommet de Versailles des 10 et 11 mars 2022, les chefs d'État et de gouvernement européens ont affirmé que l'invasion russe de l'Ukraine constituait un « bouleversement tectonique dans l'histoire européenne »<sup>3</sup>. Les États membres se sont dès lors engagés à considérablement renforcer d'ici 2030 leurs capacités de défense et à accorder beaucoup plus d'importance à contrer

<sup>1</sup> Estelle HOORICKX (Institut royal supérieur de défense) et Carolyn MOSER (Institut Max Planck de droit public comparé et de droit international).

<sup>2</sup> L'audition portait sur l'applicabilité de la clause d'assistance mutuelle du Traité sur l'UE (article 42§7 TEU) pour faire face aux nouvelles menaces, y compris les cyberattaques, les menaces hybrides ou des attaques qui utilisent des technologies nouvelles et émergentes

([www.europarl.europa.eu/cmsdata/242774/Programme\\_SEDE\\_Hearing\\_MutualDefenceClause\\_29112021.pdf](http://www.europarl.europa.eu/cmsdata/242774/Programme_SEDE_Hearing_MutualDefenceClause_29112021.pdf)).

<sup>3</sup> Conseil européen, « Déclaration de Versailles – Rencontre informelle des chefs d'État ou de gouvernement, 10 et 11 mars 2022 », 3 (<https://www.consilium.europa.eu/media/54777/20220311-versailles-declaration-fr.pdf>).

La clause d'assistance mutuelle du Traité sur l'Union européenne (article 42§7 TUE)  
permet-elle de répondre adéquatement aux nouvelles menaces ?

« une guerre hybride qui prend toujours plus d'ampleur » et à lutter contre la désinformation<sup>4</sup>. Ils ont également rappelé que la « solidarité entre les États membres est exprimée à l'article 42, paragraphe 7, du TUE [Traité sur l'Union européenne] »<sup>5</sup>. Cette clause d'assistance mutuelle<sup>6</sup> est d'ailleurs au cœur de la boussole stratégique adoptée par le Conseil de l'UE le 21 mars 2022<sup>7</sup>. Selon ce document, le nouveau paysage stratégique « oblige [les États membres] à agir avec beaucoup plus d'urgence et de détermination et à faire preuve d'assistance mutuelle et de solidarité en cas d'agression contre l'un des nôtres »<sup>8</sup>. Ce constat s'avère particulièrement pertinent dans le contexte géopolitique actuel où les menaces de plus en plus complexes connaissent une ampleur inédite<sup>9</sup>. En outre, l'assistance mutuelle en cas d'agression est fondamentale pour renforcer l'autonomie stratégique et décisionnelle de l'UE.

L'emploi de la clause d'assistance mutuelle codifiée par l'article 42§7 TUE, déclenchée pour la première (et unique) fois par la France en novembre 2015 après les attentats de Paris, soulève encore des interrogations<sup>10</sup>. Étant donné qu'elle contient des obligations plutôt vagues et non précisées par d'autres sources européennes juridiques ou politiques, les modalités de sa mise en œuvre restent floues. En réalité, il revient aux États apportant leur aide et assistance de déterminer par quels moyens militaires ou civils ils souhaitent contribuer à la légitime défense collective. Les pays qui offrent leur soutien disposent donc d'une large marge de manœuvre décisionnelle et opérationnelle<sup>11</sup>. Ainsi, la réponse des États membres à l'appel d'aide et d'assistance lancé par la France en 2015 s'est avérée modeste, voire symbolique, et n'a pas permis à l'armée française de réduire sa présence dans ses missions extraterritoriales de lutte contre le terrorisme, comme le souhaitait l'Hexagone<sup>12</sup>.

Toutefois, pour les pays de l'UE non membres de l'OTAN, tels que la Finlande et la Suède en particulier<sup>13</sup>, qui ne peuvent pas (actuellement)<sup>14</sup> s'appuyer sur l'article 5 du Traité de l'Atlantique

<sup>4</sup> Conseil européen, « Déclaration de Versailles », 4.

<sup>5</sup> Conseil européen, « Déclaration de Versailles », 3.

<sup>6</sup> Si cet article a souvent été qualifié de « clause de défense mutuelle », la doctrine préfère généralement la terminologie générique de « clause d'assistance mutuelle ». Voir, par exemple, Matthias Fischer et Daniel Thym, « Article 42 [CSDP: Goals and Objectives; Mutual Defence] », in *The Treaty on European Union (TEU). A Commentary*, édité par Hermann-Josef Blanke et Stelio Mangiameli (Berlin ; Heidelberg : Springer, 2013) ; Panos Koutrakos, *The EU Common Security and Defence Policy*, EU law library (Oxford ; New York : Oxford University Press, 2013), 68–71. Par ailleurs, pour les juristes du Conseil de l'UE, qui ont produit une note confidentielle sur le sujet en juillet 2016, l'article 42§7 TUE n'est en effet pas une clause de *défense* mutuelle au sens de l'article 5 de l'OTAN, mais davantage une clause d'*assistance* mutuelle (André Dumoulin et Nicolas Gros-Verheyde, *La politique européenne de sécurité et de défense commune* (Bruxelles : Éditions du Villard, 2017), 324).

<sup>7</sup> Conseil de l'UE, « Une boussole stratégique en matière de sécurité et de défense », document du Conseil n° 7371/22 (21 mars 2022).

<sup>8</sup> Conseil de l'UE, « Boussole stratégique » (2022), 12.

<sup>9</sup> À ce sujet, voir le rapport annuel du Parlement européen sur la mise en œuvre de la Politique de sécurité et de défense commune (2021), ([https://www.europarl.europa.eu/doceo/document/TA-9-2022-0040\\_FR.html](https://www.europarl.europa.eu/doceo/document/TA-9-2022-0040_FR.html)).

<sup>10</sup> Nicolas Gros-Verheyde, « À défaut d'article 5 de l'OTAN peut-on utiliser l'article 42-7 de l'UE ? Faut-il l'encadrer ? », in *B2 Le quotidien de l'Europe géopolitique*, 8.10.2021 (<https://club.bruxelles2.eu/2021/10/a-defaut-darticle-5-de-lotan-peut-on-utiliser-larticle-42-7-de-lue-faut-il-lencadrer/>).

<sup>11</sup> Koutrakos, *The EU Common Security and Defence Policy*, 69 ; Carolyn Moser, « Awakening dormant law – or the invocation of the European mutual assistance clause after the Paris attacks », in *Verfassungsblog 18.11.2015*, <http://verfassungsblog.de/awakening-dormant-law-or-the-invocation-of-the-european-mutual-assistance-clause-after-the-paris-attacks/>.

<sup>12</sup> Dumoulin et Gros-Verheyde, *La politique européenne de sécurité et de défense commune*, 331.

<sup>13</sup> Six des 27 États membres de l'UE ne font pas partie de l'OTAN, à savoir : la Suède, la Finlande, l'Autriche, Chypre, l'Irlande et Malte.

<sup>14</sup> La récente invasion de l'Ukraine par la Russie a accéléré le débat sur une éventuelle adhésion de la Finlande et de la Suède à l'OTAN. Ces deux pays déposeront probablement officiellement leur candidature dans les prochains jours auprès de l'Organisation. Avant que leur adhésion ne soit ratifiée, la sécurité de ces deux pays reposera sur des assurances de sécurité que les pays membres de l'OTAN leur auront données. L'activation de l'article 42§7 mais également un soutien bilatéral des Américains font partie des options envisagées [Sur le sujet, lire : Aurélie Pugnet, « Adhésion de la Finlande et Suède à l'OTAN : des garanties de sécurité à trouver », in *B2 Le quotidien de l'Europe géopolitique*, 7.04.2022

La clause d'assistance mutuelle du Traité sur l'Union européenne (article 42§7 TUE)  
permet-elle de répondre adéquatement aux nouvelles menaces ?

Nord consacrant le principe de défense collective, la clause d'assistance mutuelle de l'UE constitue une garantie de sécurité particulièrement importante<sup>15</sup>. Celle-ci repose en effet sur l'obligation pour tous les États membres de fournir une aide et une assistance « au cas où un État membre serait l'objet d'une agression armée sur son territoire ». Mais à l'heure actuelle, l'article 42§7 TUE n'équivaut, ni dans la théorie ni dans la pratique, à l'article 5 de l'OTAN<sup>16</sup>. D'une part, il n'y a pas de volonté parmi les États membres de créer une alliance militaire alternative à l'OTAN ; d'autre part, l'UE ne dispose (actuellement) pas de moyens militaires suffisants pour agir de manière autonome<sup>17</sup>. Dès lors, même si le choc créé par l'agression armée de la Russie a poussé les pays européens à franchir un pas historique – à savoir, la mise à disposition et le financement d'armes létales et non létales pour soutenir l'Ukraine<sup>18</sup> –, les États membres ont des préférences divergentes quant au caractère subsidiaire ou complémentaire de la défense européenne par rapport aux engagements de l'OTAN. En témoigne le langage flou de la boussole stratégique concernant l'article 42§7 TUE et son rapport à la défense collective de l'OTAN.

Les alliés occidentaux craignent d'ailleurs que Moscou n'intensifie ses cyberattaques et campagnes de désinformation contre les 27 pays de l'UE ayant adopté des sanctions contre la Russie et/ou qui fournissent des équipements militaires à l'Ukraine assiégée<sup>19</sup>, y compris dans le cadre de la Facilité européenne pour la paix<sup>20</sup>. Dans ce contexte, la suspension de la diffusion des médias russes *Sputnik* et *Russia Today* en Europe vise à lutter contre les campagnes de désinformation et de manipulation de l'information à l'encontre de l'UE et de ses États membres<sup>21</sup>. Les cyberattaques peuvent en effet s'avérer extrêmement efficaces en matière de sabotage, d'espionnage et de subversion à grande échelle, mais également avoir des conséquences très lourdes sur les infrastructures, l'économie, les systèmes de santé et sur les processus démocratiques en Europe<sup>22</sup>.

La présente note se propose dès lors d'évaluer, dans le cadre de la clause d'assistance mutuelle consacrée par l'article 42§7 TUE, les modalités d'action dont disposent les États membres

---

(<https://club.bruxelles2.eu/2022/04/analyse-adhesion-de-la-finlande-et-suede-a-lotan-des-garanties-de-securite-a-trouver/>) ; Anne-Françoise Hivert, « La Finlande fait un premier pas vers une candidature à l'OTAN », *Le Monde*, 14 avril 2022 ([https://www.lemonde.fr/international/article/2022/04/14/la-finlande-fait-un-premier-pas-vers-une-candidature-a-l-otan\\_6122066\\_3210.html](https://www.lemonde.fr/international/article/2022/04/14/la-finlande-fait-un-premier-pas-vers-une-candidature-a-l-otan_6122066_3210.html))).

<sup>15</sup> En témoigne notamment une lettre des premiers ministres finlandais et suédois Sanna Marin et Magdalena Andersson envoyée au président du Conseil européen Charles Michel en amont de la réunion des chefs d'État et de gouvernement à Versailles, soulignant l'importance de la clause d'assistance mutuelle de l'UE. Pour plus de détails : <https://valtioneuvosto.fi/en/-/10616/prime-ministers-of-finland-and-sweden-stress-role-of-eu-as-security-provider>.

<sup>16</sup> Koutrakos, *The EU Common Security and Defence Policy*, 68–71.

<sup>17</sup> N. Gros-Verheyde, « À défaut d'article 5 de l'OTAN peut-on utiliser l'article 42-7 de l'UE ? Faut-il l'encadrer ? », in *B2 Le quotidien de l'Europe géopolitique*, 8 octobre 2021 (<https://club.bruxelles2.eu/2021/10/a-defaut-darticle-5-de-lotan-peut-on-utiliser-larticle-42-7-de-lue-faut-il-lencadrer/>) ; Philippe Gélie, « Charles Michel : “ L'UE vit un moment copernicien sur la défense ” », *Le Figaro*, 13 mars 2022 (<https://www.lefigaro.fr/international/charles-michel-l-ue-vit-un-moment-copernicien-sur-la-defense-20220313>).

<sup>18</sup> Les premières décisions du Conseil à ce sujet furent prises le 28 février. Voir : Décision (PESC) 2022/338 du Conseil du 28 février 2022 relative à une mesure d'assistance au titre de la facilité européenne pour la paix en vue de la fourniture aux forces armées ukrainiennes d'équipements et de plateformes militaires conçus pour libérer une force létale (<https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32022D0338>) ; Décision (PESC) 2022/339 du Conseil du 28 février 2022 relative à une mesure d'assistance au titre de la facilité européenne pour la paix afin de soutenir les forces armées ukrainiennes (<https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=OJ%3A2022%3A061%3AFULL>).

<sup>19</sup> Sue Halpern, « The Threat of Russian Cyberattacks looms large », *The New Yorker*, 22 mars 2022 (<https://www.newyorker.com/news/daily-comment/the-threat-of-russian-cyberattacks-looms-large>).

<sup>20</sup> Voir les décisions du Conseil citées plus haut (note 17).

<sup>21</sup> Décision (PESC) 2022/351 du Conseil du 1<sup>er</sup> mars 2022 modifiant la décision 2014/512/PESC concernant des mesures restrictives eu égard aux actions de la Russie déstabilisant la situation en Ukraine. Le Président du Tribunal de l'UE a rejeté la demande de référé de RT France par ordonnance du 30 mars 2022 (T-125/22 R), ce qui signifie que les mesures restrictives à l'égard des médias russes visés restent actuellement en place.

<sup>22</sup> Conseil de l'UE, « Boussole stratégique » (2022), 22.

La clause d'assistance mutuelle du Traité sur l'Union européenne (article 42§7 TUE)  
permet-elle de répondre adéquatement aux nouvelles menaces ?

de l'UE pour faire face aux nouvelles menaces, qu'elles soient hybrides, de nature cyber ou qu'elles mettent en œuvre des technologies émergentes. Elle vise également à approfondir les implications juridiques de l'invocation de la clause en droit européen et international. Avant de nous pencher sur les nouvelles menaces et leurs spécificités stratégiques et juridiques, il convient de rappeler le contenu de la clause d'assistance mutuelle et celui du droit à la légitime défense qui y est lié.

## L'article 42§7 TUE ou la consécration de la légitime défense collective

---

L'article 42§7 TUE consacre un droit à la légitime défense collective. Il est formulé comme suit :

*« Au cas où un État membre serait l'objet d'une agression armée sur son territoire, les autres États membres lui doivent aide et assistance par tous les moyens en leur pouvoir, conformément à l'article 51 de la charte des Nations unies. Cela n'affecte pas le caractère spécifique de la politique de sécurité et de défense de certains États membres. Les engagements et la coopération dans ce domaine demeurent conformes aux engagements souscrits au sein de l'Organisation du traité de l'Atlantique Nord, qui reste, pour les États qui en sont membres, le fondement de leur défense collective et l'instance de sa mise en œuvre. »*

La légitime défense est un élément crucial du droit international qui permet aux États de protéger et défendre leur souveraineté. La légitime défense, consacrée par l'article 51 de la Charte des Nations unies (ci-après « la Charte ») constitue, en effet, la principale exception à l'interdiction de recourir à la force telle qu'imposée par l'article 2§4 de la Charte<sup>23</sup>. Il s'agit d'une des questions juridiques les plus controversées, non seulement parce que les circonstances sécuritaires ne cessent d'évoluer, mais également parce que certains États font appel au concept de légitime défense pour donner une apparence de légalité à leur usage de la force pas nécessairement légal<sup>24</sup>. Quoi qu'il en soit, si la légitime défense concernait traditionnellement deux États, elle est de plus en plus employée de manière collective, y compris pour répondre à des attaques perpétrées par des acteurs non étatiques<sup>25</sup>.

Malgré les incertitudes – pour ne pas dire les ambiguïtés – qui entourent la notion de légitime défense, il existe un consensus sur le fait que son invocation est soumise à cinq critères issus de la pratique des États et de la jurisprudence internationale<sup>26</sup>. Primo, le recours à la légitime défense doit répondre à une agression armée (en anglais, *armed attack*), que l'on peut définir comme un incident transfrontalier d'une certaine ampleur et suivi d'effets particuliers, qui peuvent être causés par un acte unique ou une série d'attaques mineures. Si le seuil d'une agression armée n'est pas atteint, les

---

<sup>23</sup> Christopher Greenwood, « Self-Defence » in *Max Planck Encyclopedia of Public International Law* (Oxford ; New York : Oxford University Press, 2012 [dernière mise à jour en 2021]), §1.

<sup>24</sup> La Russie, par exemple, tente de justifier son invasion récente en Ukraine (plus précisément, les oblasts ukrainiens de Louhansk et Donetsk) en prétendant que l'usage de la force sur le territoire ukrainien correspond à de la légitime défense. Voir, à ce sujet, la notification du 24 février 2022 du représentant permanent de la Fédération de Russie auprès des Nations unies en vertu de l'article 51 de la Charte (document diffusé sous la cote S/2022/154).

<sup>25</sup> Voir la discussion académique à ce sujet dans Greenwood, « Self-Defence », § 19 et Karl Zemanek, « Armed Attack » in *Max Planck Encyclopedia of Public International Law* (Oxford ; New York : Oxford University Press, 2012 [dernière mise à jour en 2013]).

<sup>26</sup> La référence jurisprudentielle clef dans ce contexte est l'arrêt (fond) de la Cour internationale de justice dans *l'Affaire relative aux activités militaires et paramilitaires au Nicaragua* (Nicaragua c. États-Unis) du 27 juin 1986. Pour une analyse exhaustive de ces critères, voir Greenwood, « Self-Defence », §§ 7-51.

La clause d'assistance mutuelle du Traité sur l'Union européenne (article 42§7 TUE)  
permet-elle de répondre adéquatement aux nouvelles menaces ?

États ne peuvent légalement pas recourir à la force mais bien à des mesures de rétorsion<sup>27</sup> ou encore adopter des contre-mesures<sup>28</sup>, y compris des sanctions économiques ou financières, ou des mesures restrictives individuelles, telles que des gels d'avoirs et des restrictions à l'entrée d'un territoire. Secundo, la légitime défense doit être nécessaire et proportionnée. Tertio, une attaque doit être terminée, en cours ou sur le point de se produire<sup>29</sup> pour que l'État attaqué puisse invoquer la légitime défense<sup>30</sup>. Quarto, tout État membre des Nations unies doit immédiatement signaler les mesures de légitime défense au Conseil de sécurité des Nations unies en vertu d'article 51 de la Charte. Et la même obligation s'applique aux États qui décident d'aider un pays agressé dans le cadre de la légitime défense collective. Quinto, le recours à la légitime défense, au regard du droit international, peut avoir lieu sur le territoire du pays agressé, mais également en dehors de celui-ci<sup>31</sup>.

L'article 42§7 TUE inscrit dans ce cadre juridique international toute réponse européenne collective à une agression armée qui toucherait l'un des États membres<sup>32</sup>. D'une part, la clause stipule que la légitime défense collective européenne doit être conforme à l'article 51 de la Charte. Cela signifie, entre autres, qu'une fois la clause déclenchée, l'État qui l'invoque et les États membres qui assistent le pays agressé doivent en informer le Conseil de sécurité. D'autre part, la mise en œuvre de la clause doit être compatible avec les engagements pris vis-à-vis de l'OTAN. Enfin, le recours à la légitime défense collective peut avoir lieu en dehors du territoire de l'UE. Ce dernier élément constitue une des raisons principales du choix français d'activer l'article 42§7 TUE en 2015 plutôt que l'article 222 TFUE (Traité sur le fonctionnement de l'Union européenne) relatif aux attaques terroristes ou catastrophes naturelles ou d'origine humaine dont un pays de l'UE pourrait être victime, qui ne concerne qu'une assistance internationale sur le territoire des États membres<sup>33</sup>. *A contrario*, en invoquant la clause de l'article 42§7 TUE, la France pouvait garder le contrôle de sa souveraineté et notamment de sa politique extérieure tout en cherchant à renforcer l'engagement des Européens dans les opérations internationales de lutte contre le terrorisme et permettre ainsi d'alléger le dispositif français<sup>34</sup>.

---

<sup>27</sup> Une mesure de rétorsion est une « mesure inamicale, licite en elle-même, prise par un [État], en riposte à un comportement inamicale d'un autre [État], que ce comportement soit ou non licite ». Voir Jean Salmon (dir.), *Dictionnaire de Droit international public* (Bruxelles : Bruylant, 2001), 1007.

<sup>28</sup> Il s'agit de « mesures prises par un État en vue de faire respecter et de protéger ses intérêts au cas où ceux-ci seraient lésés par un autre État ». Voir Jean Salmon (dir.), *Dictionnaire de Droit international public* (Bruxelles : Bruylant, 2001), 259-260. Pour plus de détails juridiques sur les contre-mesures, voir Federica Paddeau, « Countermeasures », in *Max Planck Encyclopedia of Public International Law* (Oxford ; New York : Oxford University Press, 2012 [dernière mise à jour en 2015]).

<sup>29</sup> Pour un pays comme Israël, par exemple, l'imminence d'une agression armée peut également constituer un critère autorisant le recours à la légitime défense. On parle alors de légitime défense « préventive », c'est-à-dire une légitime défense basée sur la probabilité avec laquelle la « menace » se transformera réellement en attaque. Une telle conception de la légitime défense n'est néanmoins pas reconnue par l'OTAN ni par l'UE (Greenwood, « Self-Defence » ; Michael Wood, « International Law and the use of force: What happens in practice? », *Indiana Journal of International Law* 53, 2013).

<sup>30</sup> Sur la temporalité de la légitime défense, voir Greenwood, « Self-Defence », §§ 41-51 et Wood, « International Law and the use of force: What happens in practice? ».

<sup>31</sup> Cette flexibilité territoriale s'étend à la légitime défense collective comme le démontre, par exemple, la pratique (récente) des États.

<sup>32</sup> Moser, « Awakening dormant law ».

<sup>33</sup> L'article 222 du traité sur le fonctionnement de l'Union européenne dispose que « l'Union et ses États membres agissent conjointement dans un esprit de solidarité si un État membre est l'objet d'une attaque terroriste ou la victime d'une catastrophe naturelle ou d'origine humaine. L'Union mobilise tous les instruments à sa disposition, y compris les moyens militaires mis à sa disposition par les États membres, pour (...) porter assistance à un État membre sur son territoire, à la demande de ses autorités politiques (...) » (<https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A12016E222>).

<sup>34</sup> Moser, « Awakening dormant law » ; Estelle Hoorickx, « La défense contre les "menaces hybrides" : la Belgique et la stratégie euro-atlantique », *Sécurité & Stratégie* 131, Octobre 2017, 39-40. (<http://www.irsd.be/website/images/livres/etudes/VS131.pdf>).

## La mise en œuvre relativement flexible de la clause d'assistance mutuelle

---

Après le déclenchement de l'article 42§7 TUE, les États membres sont obligés d'apporter leur soutien. La clause contient, en effet, une obligation qui, même si elle ne peut pas être sanctionnée par une instance judiciaire<sup>35</sup>, n'est pas uniquement d'ordre symbolique. Toutefois, une série de critères relativement flous permettent aux États membres d'atténuer le caractère contraignant de leur devoir d'aide et d'assistance<sup>36</sup>. Ainsi, il revient à chaque État membre de déterminer « en totale discrétion » l'aide et l'assistance qu'il souhaite fournir au pays attaqué<sup>37</sup>, y compris le déploiement de moyens militaires mais également une assistance économique, un soutien diplomatique, une aide logistique, ou encore une mise à disposition de personnel ou l'échange de renseignements<sup>38</sup>. La coordination de ces différentes formes de soutien incombe au pays attaqué ayant déclenché la clause : c'est lui qui, de manière bilatérale, coordonne avec les autres États les mesures à prendre pour répondre à l'agression.

Puisque la clause émet une obligation interétatique, elle n'évoque pas les institutions européennes – ni en tant que victime potentielle d'une agression armée, ni en tant qu'acteur dans sa mise en œuvre. On peut toutefois supposer que, si une institution européenne devait être victime d'une agression armée, l'État hôte déclencherait la clause à sa place. Il devrait ensuite décider de mettre en œuvre cette disposition de manière bilatérale – l'État hôte prenant la direction des opérations et assurant la liaison avec les autres États membres – ou de conférer ce rôle à un organe ou à une institution de l'UE<sup>39</sup>. La boussole stratégique préconise quant à elle que l'état-major militaire de l'UE (EUMS) joue un rôle dans la mise en œuvre de l'article 42§7 TUE, mais uniquement à la demande des États membres<sup>40</sup>.

## La difficile applicabilité de l'article 42§7 TUE face à une « guerre ambiguë »<sup>41</sup>

---

Comme expliqué précédemment, la clause d'assistance mutuelle ne peut être déclenchée qu'en cas d'agression armée. Or, il n'est pas toujours aisé de savoir si les nouvelles pratiques de la guerre, telles que les cyberattaques ou les campagnes de désinformation, correspondent à ce type d'agression.

Les « nouvelles menaces » – que ce soient des cyberattaques ou des campagnes hybrides – partagent plusieurs caractéristiques essentielles, à savoir leur nature à la fois coercitive et subversive, leur emploi par des acteurs étatiques et non étatiques<sup>42</sup>, ainsi que leur objectif principal qui consiste à exploiter les vulnérabilités de la cible visée tout en créant de l'ambiguïté afin de ne pas avoir à subir les conséquences d'une réaction politique, militaire (y compris cyber) et/ou juridique de la

---

<sup>35</sup> Dumoulin et Gros-Verheyde, *La politique européenne de sécurité et de défense commune*, 328.

<sup>36</sup> Moser, « Awakening dormant law ».

<sup>37</sup> Sénat (France), Rapport d'information n° 626(2018-2019) de M. Ronan Le Gleut et M<sup>me</sup> Hélène Conway-Mouret, fait au nom de la commission des affaires étrangères, de la défense et des forces armées, déposé le 3 juillet 2019, <https://www.senat.fr/rap/r18-626-1/r18-626-14.html>.

<sup>38</sup> Dumoulin et Gros-Verheyde, *La politique européenne de sécurité et de défense commune*, 327.

<sup>39</sup> *Ibid.*, 329-30.

<sup>40</sup> Conseil de l'UE, « Boussole stratégique » (2022), 26.

<sup>41</sup> La « guerre ambiguë » – parfois assimilée à la notion de guerre hybride – est associée à la question de l'*attribution*, c'est-à-dire au fait de pouvoir ou non déterminer l'auteur d'une attaque (Hoorickx, « La défense contre les "menaces hybrides" », 11).

<sup>42</sup> *Ibid.*, 14.

La clause d'assistance mutuelle du Traité sur l'Union européenne (article 42§7 TUE)  
permet-elle de répondre adéquatement aux nouvelles menaces ?

communauté internationale<sup>43</sup>. Ainsi, l'auteur d'une attaque hybride aura recours, autant que possible, à des modes opératoires – tels que les cyberattaques, les campagnes de désinformation ou la « guerre par procuration » – qui vont lui permettre de créer de l'ambiguïté sur la nature et l'origine de l'attaque<sup>44</sup>. Une telle ambiguïté peut entraver l'invocation de la clause d'assistance mutuelle puisque celle-ci ne peut être déclenchée qu'à condition que l'agression armée soit dirigée ou lancée sur l'État visé depuis l'extérieur<sup>45</sup>.

Face aux réalités complexes de la légitime défense et aux nouvelles pratiques de la guerre (hybride), il convient de déterminer si les nouvelles menaces peuvent constituer une « agression armée » au sens juridique du terme, autorisant la légitime défense et, par conséquent, l'invocation de l'article 42§7 TUE, ou s'il s'agit plutôt de modes opératoires qui constituent, certes, des actes illicites au regard du droit international – telle l'ingérence dans des affaires internes par des campagnes de désinformation massives –, mais qui ne permettent pas d'invoquer la légitime défense. Pour résoudre cette question, il convient de se référer aux conditions d'invocation de l'article 42§7 TUE, tout en tenant compte des spécificités juridiques nationales des États membres<sup>46</sup>.

Comme expliqué préalablement, et conformément aux définitions de légitime défense et d'agression armée communément admises par la pratique des États ainsi que la jurisprudence internationale et la doctrine, le déclenchement de la clause d'assistance mutuelle nécessite un certain nombre de conditions. Pour rappel, l'État concerné doit être victime d'une agression armée – peu importe les armes ou les techniques utilisées – qui soit terminée, en cours ou imminente, provoquée par un acte unique ou une série d'attaques mineures, d'une ampleur et d'une gravité significatives,<sup>47</sup> mais également dirigée ou lancée sur l'État visé depuis l'extérieur par un acteur étatique ou non étatique. En outre, cette violation doit se faire sur le territoire de l'État visé<sup>48</sup>. Trois facteurs à prendre en compte pour pouvoir qualifier une nouvelle menace d'attaque armée et être ainsi en mesure d'invoquer l'article 42§7 TUE s'avèrent particulièrement difficiles à identifier, à savoir le critère géographique, celui de la gravité de l'agression et enfin celui de l'attribution.

Tout d'abord, déterminer si le cyberspace<sup>49</sup>, où sont menées les cyberattaques et où se propagent les fausses informations, peut être considéré comme un territoire au sens géographique du terme, n'est pas chose aisée<sup>50</sup>. Il est en effet souvent techniquement compliqué d'identifier l'origine géographique, voire territoriale d'une cyberattaque. De plus, si la naissance mais également

---

<sup>43</sup> Joseph Henrotin, « La guerre hybride comme avertissement stratégique », *Stratégique*, n° 111, Paris, 2016, 20. Voir également Commission européenne, *Communication conjointe au Parlement européen et au Conseil – Cadre commun en matière de lutte contre les menaces hybrides une réponse de l'Union européenne*, JOIN/2016/018 final.

<sup>44</sup> Henrotin, « La guerre hybride comme avertissement stratégique », 11 et 14.

<sup>45</sup> Sur le sujet, voir Service juridique du Conseil de l'UE, « Article 42(7) du TUE », 12 juillet 2016, document du Conseil n° 11176/16, non publié (limité) (consultable par extraits en ligne à <https://data.consilium.europa.eu/doc/document/ST-11176-2016-INIT/fr/pdf>) ; cité par André Dumoulin et Nicolas Gros-Verheyde, *La politique européenne de sécurité et de défense commune*, 326.

<sup>46</sup> Voir par exemple : Ministère des Armées (France), « Droit international appliqué aux opérations dans le cyberspace », 2018 ; Gouvernement Fédéral allemand, « On the Application of International Law in Cyberspace », 2021.

<sup>47</sup> Zemanek, « Armed attack ».

<sup>48</sup> Ainsi par exemple, l'agression armée doit être distinguée d'une menace « terroriste domestique ». À ce sujet, voir Service juridique du Conseil de l'UE, « Article 42(7) du TUE », tel que cité par Dumoulin et Gros-Verheyde, *La politique européenne de sécurité et de défense commune*, 326.

<sup>49</sup> Olivier Kempf définit le cyberspace comme « l'espace constitué de systèmes informatiques de toute sorte connectés en réseaux et permettant la communication technique et sociale d'informations par des utilisateurs individuels ou collectifs » (Olivier Kempf, *Introduction à la cyberstratégie*, Paris, 2012, 14).

<sup>50</sup> Sur le sujet, lire : Frédéric Douzet, « La géopolitique pour comprendre le cyberspace », *Hérodote*, 2014/1-2 (n° 152-153), 3-21 (<https://www.cairn.info/revue-herodote-2014-1-page-3.htm>) ; Alix Desforges, « Les représentations du cyberspace : un outil géopolitique », *Hérodote*, 2014/1-2 (n° 152-153), 67-81 (<https://www.cairn.info/revue-herodote-2014-1-page-67.htm>).

La clause d'assistance mutuelle du Traité sur l'Union européenne (article 42§7 TUE)  
permet-elle de répondre adéquatement aux nouvelles menaces ?

la diffusion de fausses rumeurs ont très souvent lieu en dehors du territoire des États visés<sup>51</sup>, celles-ci peuvent avoir des conséquences directes dans ces pays et constituer des « ingérences étrangères dans l'espace de l'information »<sup>52</sup>, notamment au travers des réseaux sociaux et autres plateformes numériques<sup>53</sup>.

Ensuite, il est également difficile de déterminer si les modes opératoires cyber ou hybrides peuvent être qualifiés d'agression armée,<sup>54</sup> qu'il s'agisse d'un seul incident ou d'une série d'activités malveillantes mineures<sup>55</sup>. Cette qualification est en effet fonction de l'ampleur de l'agression ainsi que de ses effets sur les acteurs étatiques, les infrastructures critiques ou les individus. C'est cette approche que l'on retrouve dans les doctrines nationales de la plupart des États membres de l'UE et au sein de l'OTAN. Lors du Sommet de Bruxelles de juin 2021, l'OTAN a en effet décidé qu'une attaque dans l'espace mais également une « cyberattaque grave » pourraient entraîner l'invocation de l'article 5<sup>56</sup>. Les États membres de l'UE calquent quant à eux leurs doctrines (juridiques) relatives aux cyberattaques sur le manuel de Tallinn qui, en appliquant les règles du droit international au cyberspace et donc à la guerre cybernétique, se focalise sur les effets d'une cyberattaque pour qualifier celle-ci d'agression armée ou non<sup>57</sup>. Ainsi, par exemple, la France estime qu'une cyberattaque provoquant « des pertes humaines substantielles, ou des dommages physiques ou économiques considérables » peut être qualifiée d'agression armée à condition qu'elle ait été « perpétrée, directement ou indirectement, par un État »<sup>58</sup>. L'attaque d'une infrastructure critique qui entraînerait des dommages d'une ampleur et d'une gravité considérables fait partie des exemples cités. Des piratages numériques qui cloueraient au sol l'aviation ou la marine militaire d'un pays ou qui endommageraient des centrifugeuses nucléaires, comme ce fut le cas en Iran en 2010, sont aussi des scénarios à envisager<sup>59</sup>. Le Service juridique du Conseil de l'UE estime néanmoins que le fait de qualifier une cyberattaque d'« agression armée » doit se définir au cas par cas, en se référant au manuel de Tallinn<sup>60</sup>. Ainsi par exemple, une « arsenalisation des politiques migratoires »<sup>61</sup> ou, en d'autres termes, la manipulation des flux migratoires à des fins de déstabilisation ne constitue pas un

---

<sup>51</sup> Sur le sujet, lire : Alexis Albarian, « Bref aperçu du traitement juridique de la désinformation en droit comparé : de la mise en place de sanctions strictement internes au recours à de véritables sanctions extraterritoriales », *Légicom*, 2018/1 n° 60, 46.

<sup>52</sup> Communication conjointe au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions relative au plan d'action pour la démocratie européenne, 3 décembre 2020 [COM(2020) 790 final], 22 (<https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52020DC0790&from=EN>).

<sup>53</sup> Sur le sujet, lire : Estelle Hoorickx, « La lutte euro-atlantique contre la désinformation : état des lieux et défis à relever pour la Belgique », *Sécurité & Stratégie* 150, Octobre 2021 (<https://www.defence-institute.be/wp-content/uploads/2021/10/ss-150.pdf>).

<sup>54</sup> Le Service juridique du Conseil de l'UE précise que l'attaque doit revêtir « un certain niveau de gravité pour atteindre le niveau d'une attaque armée » et doit donc être ainsi « distinguée des attaques terroristes en général ». Service juridique du Conseil de l'UE, « Article 42(7) du TUE », tel que cité par André Dumoulin et Nicolas Gros-Verheyde, *La politique européenne de sécurité et de défense commune*, 326.

<sup>55</sup> Dans ce sens, voir Cour internationale de justice, *Affaire des plateformes pétrolières* (République islamique d'Iran c. États-Unis), arrêt, 2003, § 64.

<sup>56</sup> Voir § 32 du Communiqué du sommet de Bruxelles publié par les chefs d'État et de gouvernement participant à la réunion du Conseil de l'Atlantique Nord tenue à Bruxelles le 14 juin 2021 ([https://www.nato.int/cps/fr/natohq/news\\_185000.htm](https://www.nato.int/cps/fr/natohq/news_185000.htm)).

<sup>57</sup> Michael Schmitt (éd), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge : Cambridge University Press 2017).

<sup>58</sup> Ministère des Armées (France), « Droit international appliqué aux opérations dans le cyberspace », section 1.2.1.

<sup>59</sup> Sur les effets (militaires) possibles des cyberattaques, lire notamment : Estelle Hoorickx, « L'implication de la Belgique dans la cyberstratégie euro-atlantique : état des lieux et défis à relever », *Sécurité & Stratégie* 139, février 2019, 11 et 13 (<https://www.defence-institute.be/wp-content/uploads/2020/03/ss-139.pdf>).

<sup>60</sup> Service juridique du Conseil de l'UE, « Article 42(7) du TUE », tel que cité par André Dumoulin et Nicolas Gros-Verheyde, *La politique européenne de sécurité et de défense commune*, 326.

<sup>61</sup> Elie Tenenbaum, « Migrants en Biélorussie : le casse-tête stratégique des "menaces hybrides" », *Le Figaro*, 12 novembre 2021 (<https://www.lefigaro.fr/international/le-casse-tete-strategique-des-menaces-militaires-hybrides-20211112>).

La clause d'assistance mutuelle du Traité sur l'Union européenne (article 42§7 TUE)  
permet-elle de répondre adéquatement aux nouvelles menaces ?

agression armée au sens juridique du terme, mais appartient plutôt au registre des actes hostiles, voire illicites qui peuvent entraîner des contre-mesures (en plus, bien évidemment, de mesures de rétorsion)<sup>62</sup>.

Enfin, l'invocation de l'article 42§7 ne dépend pas seulement de la violation d'une règle du droit international mais également de la possibilité de pouvoir attribuer l'agression à un auteur<sup>63</sup>. La pratique montre que, depuis 2001, les États ont surtout invoqué la légitime défense en cas d'attaques menées par des acteurs non étatiques. Eu égard aux doctrines nationales et documents du service juridique du Conseil concernant l'article 42§7 TUE<sup>64</sup>, il est probable que la clause pourrait s'appliquer également au cyberspace – à condition que les actes en question puissent être attribués (in)directement à une entité étatique. En effet, s'il peut s'avérer techniquement difficile de prouver qu'une cyberattaque ou une campagne de désinformation soit le fait d'un individu, il est encore plus complexe de démontrer que celle-ci a été commanditée ou tolérée par un État, qui aura d'ailleurs tout intérêt à ne pas être démasqué pour des raisons géopolitiques évidentes. Cette difficulté d'attribution, qui est une prérogative nationale souveraine, empêche dès lors toute réaction – individuelle ou collective –, qui pourrait, en cas d'absence de preuves suffisantes, être qualifiée d'acte d'agression<sup>65</sup>. La décision d'attribution n'est en général pas prise uniquement en fonction d'informations techniques, mais également sur la base de l'évaluation du contexte stratégique et des effets de l'attaque cyber au-delà du cyberspace (c'est-à-dire notamment des effets physiques, politiques ou économiques de l'attaque), en tenant compte du contexte plus large, comme le souligne la doctrine cyber de l'Allemagne<sup>66</sup>.

Néanmoins, même lorsque l'attribution d'une cyberattaque est clairement établie, certains pays se montrent réticents à incriminer ouvertement l'État à l'origine de l'agression – ce qui est pourtant une condition préalable à l'exercice de la légitime défense collective. Ainsi par exemple, il y a quelques années, lorsque le *Bundestag* (Parlement allemand) et l'Organisation pour l'interdiction des armes chimiques (OIAC) ont été victimes de cyberattaques commanditées par la Russie et la Chine, l'UE a préféré, pour éviter une escalade juridique et politique, sanctionner des individus, dont la nature d'agents d'État *de jure* ou *de facto* était pourtant évidente, plutôt que les deux pays en question<sup>67</sup>.

## Conclusions et recommandations

---

Malgré le choc créé par l'invasion de l'Ukraine par la Russie, les États membres n'accordent pas nécessairement la même importance à la clause d'assistance mutuelle du Traité sur l'Union européenne (TUE) : certains privilégient l'option transatlantique dans le cadre de l'OTAN et d'autres – surtout les pays de l'UE qui ne sont pas membres de l'OTAN – estiment que l'article 42§7 TUE constitue une garantie de sécurité indispensable pour faire face à la menace russe,

---

<sup>62</sup> Paddeau, « Countermeasures ».

<sup>63</sup> La complexe controverse selon laquelle la légitime défense peut également être invoquée vis-à-vis d'acteurs non étatiques ne sera pas abordée dans la présente note.

<sup>64</sup> Service juridique du Conseil de l'UE, « Article 42(7) du TUE », tel que cité par André Dumoulin et Nicolas Gros-Verheyde, *La politique européenne de sécurité et de défense commune*, 326.

<sup>65</sup> Wood, « International Law and the use of force: What happens in practice? », 350.

<sup>66</sup> Gouvernement fédéral allemand, « On the Application of International Law in Cyberspace », 15.

<sup>67</sup> Règlement d'exécution (UE) 2020/1125 du Conseil du 30 juillet 2020 mettant en œuvre le règlement (UE) 2019/796 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres (<https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32020R1125>).

La clause d'assistance mutuelle du Traité sur l'Union européenne (article 42§7 TUE)  
permet-elle de répondre adéquatement aux nouvelles menaces ?

notamment. Quoi qu'il en soit, la clause d'assistance mutuelle du Traité de l'UE constitue un outil utile, voire essentiel, à la mise en place d'une Europe de la défense davantage souveraine et autonome, processus que la guerre en Ukraine a accéléré.

L'invocation et le déclenchement de l'article 42§7 TUE en cas d'attaques cyber ou hybrides n'est néanmoins pas chose aisée. Le recours à cette clause doit en effet répondre à des critères liés au droit encadrant la légitime défense, qui ne sont pas facilement applicables aux nouvelles menaces issues de la guerre hybride, aussi appelée « guerre ambiguë ». Par ailleurs, les États membres ne disposent pas actuellement d'une définition uniforme ou précise concernant les nouvelles formes de menaces ou d'attaques, et ce malgré l'adoption récente de la boussole stratégique. L'absence d'une définition commune est une lacune importante que les acteurs européens doivent combler dans un avenir proche. S'il ne semble pas nécessaire de déterminer des « critères rigides d'application »<sup>68</sup> pour la clause d'assistance mutuelle, les États membres devraient non seulement acquérir une compréhension commune des nouveaux phénomènes de sécurité, y compris les problématiques cyber et hybrides, mais également l'exposer clairement dans un document politico-stratégique, pour que l'article 42§7 TUE puisse, le cas échéant, être déclenché de manière rapide et efficace. Il convient, pour ce faire, de se mettre d'accord sur les critères selon lesquels une cyberattaque ou une campagne hybride peut être qualifiée d'agression armée en tenant notamment compte de son ampleur et de sa gravité. Les États membres de l'UE pourraient ainsi se mettre politiquement d'accord, comme l'a fait déjà l'OTAN avec son article 5, sur le fait que la clause d'assistance mutuelle puisse être déclenchée en cas de cyberattaque et/ou d'une attaque dans l'espace d'une certaine ampleur vis-à-vis d'un ou de plusieurs de ses États membres. La boussole stratégique laisse en tout cas sous-entendre que l'assistance mutuelle pourrait aussi être invoquée pour faire face aux menaces hybrides<sup>69</sup>.

Si l'article 42§7 TUE offre une base juridique précieuse pour une réponse collective à une agression armée, elle doit être traitée comme une mesure de dernier recours. Elle ne devrait donc pas servir de base juridique pour agir ou réagir à des attaques dont la portée et les effets n'équivalent pas à une agression armée. En effet, dans ce cas de figure, la diplomatie, les rétorsions et les contremesures restent les options à privilégier.



**INSTITUT ROYAL  
SUPERIEUR**  
150 ans *think tank*  
de **D E F E N S E**

Les vues exprimées dans ce document sont celles des auteures et ne reflètent pas nécessairement les positions de l'Institut royal supérieur de défense, de la Défense belge ou celles du gouvernement belge.

[www.defence-institute.be](http://www.defence-institute.be)  
© IRSD – Tous droits réservés

Sources image : [maxpixel.net](http://maxpixel.net)



**LA DÉFENSE**

<sup>68</sup> Nicolas Gros-Verheyde, « À défaut d'article 5 de l'OTAN ».

<sup>69</sup> Conseil de l'UE, « Boussole stratégique » (2022), 22.