23 octobre 2019

IRSEM
INSTITUT DE RECHERCHE STRATÉGIQUE
DE L'ÉCOLE MILITAIRE

NOTE DE RECHERCHE – n° 83

UNE CYBERDÉFENSE COLLECTIVE EN EUROPE ?

L'ARTICULATION ENTRE CYBERDÉFENSES EUROPÉENNE ET TRANSATLANTIQUE

Morgan JOUY
Assistant de recherche à l'IRSEM en 2017

RÉSUMÉ

Une défense collective dans le cyberespace pourrait apparaître pertinente au regard de la potentialité d'un conflit cyber et des menaces cybernétiques qui en émanent. Cette cyberdéfense collective semble particulièrement appropriée en Europe, car elle s'appuierait sur des réseaux de confiance préexistants et solides. Cependant le paysage institutionnel est très particulier dans cette région, où l'OTAN et l'UE partagent une majorité de membres en commun et ont de ce fait une zone d'action très similaire sur le Vieux Continent. Ceci donne lieu à certains chevauchements et doublons d'activités. Les éléments de subsidiarité ou de complémentarité entre l'UE et l'OTAN dans le domaine de la cyberdéfense sont aujourd'hui difficilement identifiables alors que la sécurité de l'OTAN et celle de l'UE sont interconnectées. Une comparaison des compétences, capacités et moyens d'actions dont disposent ces deux structures de cyberdéfense collectives est alors nécessaire pour clarifier l'articulation des deux systèmes et les pistes de renforcement de celle-ci.

SOMMAIRE

INTRODUCTION : UNE CYBERDÉFENSE COLLECTIVE POUR UN RAPPORT DE FORCE AFFIRMÉ DANS LE CYBERESPACE

L'Europe est dotée d'un paysage institutionnel très particulier en matière de sécurité et de défense collective. On y retrouve ainsi l'Organisation du traité de l'Atlantique nord (OTAN), une organisation spécialisée en sécurité et défense collectives dès sa création en 1949, mais également l'Union européenne (UE), qui, à l'inverse, a vu ses compétences dans ce domaine se construire progressivement, notamment depuis les traités de Nice (2001) et de Lisbonne (2011).

Si la guerre est toujours « une affaire d'État », on constate un « enracinement des alliances » et, plus largement, des structures de sécurité collective[1]. Hume[2], dès le milieu du XVIII[e] siècle, expose que chaque État agit dans le but d'atteindre un objectif direct (sécurité individuelle) mais aussi afin de remplir un objectif indirect, l'équilibre international (ou « équilibre des pouvoirs »). De ce fait, les alliances peuvent présenter une utilité afin de construire un équilibre entre puissances, ou du moins pour équilibrer les menaces[3]. En effet, l'intérêt d'une alliance pour un État consiste à intégrer un système collectif de sécurité, qui lui confère une puissance plus importante, et à y contribuer.

Ces mêmes théories et stratégies s'appliquent dans le cyberespace[4]. Dans la mesure où les menaces cyber sont déterritorialisées, opaques, relativement instantanées et difficilement attribuables, l'intégration d'une coopération ou d'une alliance interétatique peut se révéler particulièrement pertinente pour consolider les rapports de force.

En matière de cyberdéfense, la coopération internationale constitue un axe important pour la stratégie française. Dès 2008, un rapport parlementaire met en évidence la « préoccupation commune » que constitue la menace cyber :

> « Les attaques informatiques s'affranchissent des frontières et peuvent être dirigées simultanément contre plusieurs États. La surveillance des réseaux et la mise au point des réactions en cas d'incident justifient une coopération et une assistance internationales. De manière plus générale, la protection des systèmes d'information face aux activités illégales constitue aujourd'hui une préoccupation commune à de nombreux États[5]. »

La *Revue stratégique de cyberdéfense* parue en février 2018 affirme également que « le renforcement de la protection, de la résilience et de la coopération de l'ensemble des acteurs du cyberespace participe de manière directe au renforcement de notre sécurité nationale[6] ». Dans ce même document, l'autonomie stratégique de l'Union européenne apparaît comme une préoccupation majeure pour l'État français, ouvrant la voie à des « moyens de réponses diplomatiques aux crises cyber à l'échelle européenne » et « à l'établissement d'une capacité

1. O. Kempf, *Alliances et mésalliances dans le cyberespace*, Economica, 2014, p. 12-38.
2. D. Hume, *Essay on the Balance of Power*, 1754.
3. S. Walt, *The Origins of Alliances*, Ithaca, Cornell University Press, 1990, p. 336.
4. O. Kempf, *Alliances et mésalliances dans le cyberespace*, *op. cit.*, p. 27.
5. *Cyberdéfense : un nouvel enjeu de sécurité nationale*, Rapport d'information n° 449 (2007-2008) de M. Roger Romani, fait au nom de la commission des affaires étrangères, déposé le 8 juillet 2008.
6. *Revue stratégique de cyberdéfense*, SGDSN, Paris, 12 février 2018, p. 75.

opérationnelle supranationale »[7]. Concilier l'action de l'UE avec les prérogatives souveraines des différents États membres demeure néanmoins une préoccupation fondamentale, comme le rappelle le Parlement européen dans sa résolution « cyberdéfense » de 2018 :

> « E. considérant que, si la cyberdéfense demeure une compétence clé des États membres, l'Union européenne a un rôle vital à jouer pour offrir une plateforme de coopération européenne et pour veiller à ce que ces nouveaux efforts soient étroitement coordonnés au niveau international et dans le cadre de l'architecture de sécurité transatlantique […] ; que nous devons aller au-delà du renforcement de notre coopération et de notre coordination ; que nous devons garantir une prévention efficace en renforçant la capacité de détection, de défense et de dissuasion de l'Union ; qu'il est indispensable de disposer d'une cyberdéfense et d'une cyberdissuasion crédibles afin de garantir une cybersécurité effective dans l'Union, tout en veillant à ce que les États les moins préparés ne deviennent pas la cible facile de cyberattaques, et qu'une capacité consistante de cyberdéfense devrait être entièrement intégrée à la PSDC ainsi qu'à l'union de la défense en cours d'érection[8] ».

Il apparaît clairement dans cet extrait que l'articulation des compétences de l'UE et de ses États membres avec l'OTAN, « architecture de sécurité transatlantique », constitue également un enjeu clé. L'OTAN, alliance militaire transatlantique qui comprend aujourd'hui vingt-deux[9] États membres de l'UE, représente en effet un acteur incontournable de la sécurité européenne. Cette dernière est importante car elle engage, en cas d'agression avérée, l'implication des États-Unis et du Canada dans la défense de l'Europe prise dans son sens le plus large[10], tout comme elle implique, réciproquement, l'engagement de ses membres européens dans la défense des deux pays nord-américains.

Une cyberdéfense collective apparaît pertinente au regard de la potentialité d'un conflit cyber et des menaces cybernétiques qui en découlent. Elle semble particulièrement appropriée à l'échelle régionale. Elle pourrait en effet s'appuyer sur des réseaux de confiance préexistants et solides, très importants dans le cyberespace où le concept de voisinage stratégique d'un État est remis en cause. L'intérêt d'une cyberdéfense collective pour l'Europe n'étant plus à démontrer, il s'agit désormais d'en définir les modalités précises : *quelle* cyberdéfense collective pour l'Europe ?

Tant au sein de l'UE que dans l'OTAN, on assiste à une institutionnalisation des problématiques cyber. Les deux organisations ont adapté leurs structures et administrations à ces problématiques émergentes. Chacune de ces deux entités a instauré une politique s'appuyant tant sur les décisions et textes réglementaires que sur des agences spécialisées[11]. Elles cherchent toutes deux à remplir un même objectif, de nature double : d'une part, renforcer la sécurité des réseaux et systèmes d'informations de leurs institutions ; d'autre part, améliorer la sécurité ou renforcer les capacités des États membres[12].

---

7. *Ibid.*, p. 77.
8. *Résolution du Parlement européen du 13 juin 2018 sur la cyberdéfense (2018/2004(INI))*, Strasbourg, 13 juin 2018.
9. Vingt et un membres en commun après la sortie effective du Royaume-Uni de l'Union européenne.
10. Incluant les pays de l'OTAN sur le continent européen non membres de l'UE comme l'Albanie, l'Islande, le Monténégro, la Norvège ou encore la Turquie.
11. J. Joubert & J.-L. Samaan, « L'intergouvernementalité dans le cyberespace : étude comparée des initiatives de l'OTAN et de l'UE », *Hérodote*, n° 152-153, 2014.
12. *Ibid.*

Cependant, n'ayant pas développé leurs politiques de manière conjointe, « une certaine confusion règne sur les rôles de l'OTAN et de l'UE dans le domaine [du cyberespace], notamment en ce qui concerne la sphère militaire. Il est bien difficile de voir émerger des éléments de subsidiarité ou de complémentarité des travaux de chacun[13] ». Pourtant, « la sécurité de l'Union européenne et celle de l'OTAN sont interconnectées[14] ».

Une comparaison des compétences, capacités et moyens d'action dont disposent ces deux structures de cyberdéfense collective est alors nécessaire pour clarifier l'articulation des deux systèmes.

QUELLES COMPÉTENCES POUR UNE (CYBER)DÉFENSE COLLECTIVE ?

Les compétences de l'OTAN

Les compétences de l'OTAN en matière de défense ont été définies par le traité de Washington (ou traité de l'Atlantique nord, TAN), traité fondateur signé le l4 avril 1949. Si l'OTAN reste une institution de sécurité collective, comme l'expriment ses trois premiers articles, l'Alliance atlantique assure plus spécifiquement et surtout une défense collective en cas d'agression armée tel que le prévoit son article 5, véritable clause d'assistance mutuelle[15].

Les États parties s'engagent avant tout à éviter les conflits et à régler de manière pacifique les disputes internationales (articles 1 et 2 TAN). Ils développent, de manière individuelle, mais aussi de manière collective, des capacités nécessaires pour dissuader les menaces et résister aux agressions (article 3). Enfin, la clause d'assistance mutuelle (article 5) offre deux provisions opératives définissant les compétences de l'OTAN[16] : d'une part, l'idée « qu'une attaque armée contre l'une ou plusieurs d'entre [les parties] survenant en Europe ou en Amérique du Nord sera considérée comme une attaque dirigée contre toutes les parties » ; d'autre part, que chaque État « assistera la partie ou les parties ainsi attaquées en prenant aussitôt, individuellement et d'accord avec les autres parties, telle action qu'elle jugera nécessaire, y compris l'emploi de la force armée » (article 5, TAN).

Le traitement de la menace cybernétique par l'OTAN est apparu et a évolué à la suite d'importants incidents cyber qui ont impacté l'Alliance et ses membres. C'est à la suite des cyberattaques commises lors de la guerre du Kosovo en 1999, dans laquelle l'Alliance était engagée, que l'OTAN a décidé de prendre en compte cette menace. Un audit interne a d'abord été mené par le SACEUR (*Supreme Allied Commander Europe*). Puis les chefs d'État ont pris des engagements lors du sommet de Prague en novembre 2002 afin de « renforcer

13. *Ibid.*, p. 275.
14. Commission européenne, « Questions-réponses : l'avenir de la défense européenne », Fiche d'information (en ligne), 2017.
15. B. Tertrais, « Article 5 of the Washington Treaty: Its Origins, Meaning and Future », Research Paper n° 130, NATO Defense College, 2016.
16. *Ibid.*

[leurs] capacités de défense contre les cyberattaques ». Néanmoins, le sujet n'est alors traité, à ce stade, que sous un angle purement technique. Il faut attendre l'attaque informatique de 2007 contre l'Estonie (membre de l'OTAN) pour que la menace cybernétique s'insère dans l'agenda politique[17]. Cette attaque soulève la question de l'invocabilité de l'article 5 du TAN en cas d'attaques cyber, et, le cas échéant, la réponse à adopter (contre-attaque informatique ou riposte conventionnelle). Ce n'est que l'année suivante qu'est adoptée la première Politique cyber de l'OTAN (*Cyber Defense Policy*) par le Conseil de l'Atlantique nord, signe que le cyber est devenu une préoccupation majeure pour l'organisation et ses États membres. Une menace émergente tellement importante, que, depuis le sommet de Varsovie en juillet 2016, le cyberespace est reconnu comme « domaine d'opérations dans lequel l'OTAN doit se défendre aussi efficacement qu'elle le fait dans les airs, sur terre et en mer » (§ 70 du Communiqué du sommet). Il est explicitement affirmé par l'OTAN que la clause d'assistance mutuelle peut être invoquée dans le cadre d'une attaque cybernétique contre l'un des États[18].

La cyberdéfense fait donc partie intégrante de la compétence essentielle de l'OTAN en matière de défense collective.

Les compétences de l'UE

À la différence de l'OTAN, les compétences de l'UE en matière de cyberdéfense n'ont pas évolué à la suite d'incidents cyber dirigés à son encontre, mais plutôt en prévision de cette menace émergente. L'UE a ainsi progressivement développé une posture de résilience et de réponse coordonnée.

Tout d'abord en matière de défense généralement, la Politique de sécurité et de défense commune (PSDC), définie à l'article 42 du traité de l'Union européenne (TUE), permet à l'UE de disposer de moyens civils et militaires dans la résolution de crises et conflits internationaux. Partie intégrante de la politique étrangère et de sécurité commune (PESC), la PSDC s'apparente aujourd'hui davantage à une forme de défense collective. Elle ne pourra constituer une véritable « défense commune » qu'après définition d'une politique commune adoptée à l'unanimité par le Conseil européen (article 42 § 2 TUE). En effet, la PSDC « repose sur les capacités fournies par les États membres » (article 42 § 1 TUE) et s'appuie encore essentiellement sur les budgets nationaux pour financer les dépenses en opérations (et ceci, malgré le mécanisme de financement Athéna). Enfin, la prise de décision demeure intergouvernementale, la règle de l'unanimité prévalant pour les décisions du Conseil (article 42 § 4 TUE).

Une clause de défense mutuelle offre néanmoins la possibilité d'une défense collective depuis le traité de Lisbonne (article 47 § 7 TUE). Similaire à la deuxième provision opérative de l'article 5 du TAN, elle dispose qu'« au cas où un État membre serait l'objet d'une

17. J. Joubert & J.-L. Samaan, « L'intergouvernementalité dans le cyberespace : étude comparée des initiatives de l'OTAN et de l'UE », *op. cit.*
18. *Ibid.*

agression armée sur son territoire, les autres États membres [de l'Union européenne] lui doivent aide et assistance par tous les moyens en leur pouvoir ».

Si l'Union européenne a progressivement pris conscience de l'émergence du risque cyber depuis les années 1990, ce n'est qu'en février 2013 qu'elle se déclare compétente en matière de cyberdéfense. C'est par la *Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé*[19], publiée conjointement par la Commission et la haute représentante pour les affaires étrangères et la politique de sécurité, que l'Union s'est auto-attribuée, à l'aune de la PSDC, sa compétence en matière de cyberdéfense. Précisément, c'est la priorité trois (sur cinq) qui lui confère cette attribution et en définit les contours :

> « **2.3 Développer une politique et des moyens de cyberdéfense s'inscrivant dans le cadre de la politique de sécurité et de défense commune (PSDC)**
>
> Les efforts de cybersécurité dans l'UE ont aussi une dimension de cyberdéfense. Pour accroître la résilience des systèmes de communication et d'information préservant les intérêts des États membres en matière de défense et de sécurité nationale, le développement des moyens de cyberdéfense doit être axé sur la détection, l'intervention et la récupération en cas de cybermenace sophistiquée.
>
> Comme ces menaces sont multiformes, il faut développer des synergies entre les approches civile et militaire de la protection des cyberinfrastructures critiques. Ces efforts doivent être étayés par de la R et D et une coopération étroite entre les pouvoirs publics, le secteur privé et les universités dans l'UE » (p. 12).

Cette Cyberstratégie, révisée en 2017, vise alors surtout la résilience dans son ensemble, et non nécessairement la suppression de la menace par une action opérationnelle contre un agresseur potentiel[20]. Menée par le SEAE, elle a été élaborée en consultation étroite avec la DG CNECT (Réseaux de communication, contenu et technologies), mais aussi la DG GROW (Marché intérieur, industrie, entrepreneuriat et PME) et la DG HOME (Migration et affaires intérieures). Cette stratégie est complétée par la directive *Network and Information System Security* (NIS) du 6 juillet 2016, qui détermine les normes auxquelles les entreprises doivent souscrire pour renforcer la cybersécurité civile au sein de l'UE. La stratégie dans son ensemble se concentre de ce fait davantage sur la sécurité intérieure de l'Union, une préoccupation répondant moins à des enjeux de sécurité intérieure qu'à des impératifs économiques[21]. La cyberdéfense au niveau de l'UE n'en est donc qu'à ses balbutiements, malgré la reconnaissance manifeste par la Commission de l'importance de la coopération en matière de cyberdéfense dans le *Document de réflexion sur l'avenir de la défense européenne* (2017).

Par ailleurs, cette stratégie ne fait pas explicitement référence à la clause d'assistance mutuelle (47 § 7 TUE) mais seulement à la clause de solidarité (article 222 du traité sur le fonctionnement de l'Union européenne [TFUE]) qui peut être invoquée au motif d'« un

19. *Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé*, Communication conjointe au Parlement européen, au Conseil, au CESE et au Comité des Régions, [JOIN(2013) 1 final], Bruxelles, 7 février 2013.

20. D. Deschaux-Dutard, « Cybersécurité et cyberdéfense : Éléments d'introduction du point de vue de la science politique », dans *Cyber, Nano : Nouvelles technologies et nouveaux enjeux sécuritaires*, Cours dans le cadre du master Sécurité internationale et défense de la faculté de droit de Grenoble, 2017.

21. *Ibid.*

cyberincident ou [d']une cyberattaque particulièrement sérieux[22] ». En revanche, il est intéressant de noter que dans sa « résolution cyberdéfense » de 2018, le Parlement européen a quant à lui affirmé l'applicabilité des deux clauses. On y distingue ainsi les contours d'une stratégie de cyberdéfense collective pour l'UE.

QUELS MOYENS ? UNE CARTOGRAPHIE DES CAPACITÉS DE L'UE ET L'OTAN

Les capacités de résilience : analyse et veille des menaces, sécurité des systèmes et moyens de réponse

Depuis le sommet de Varsovie de juillet 2016, les États membres de l'OTAN se sont engagés à améliorer leurs défenses informatiques afin de garantir un haut niveau de résilience collective pour l'ensemble de l'Alliance. Au-delà des efforts individuels des États membres, l'OTAN dispose de capacités spécifiques en matière de cyberdéfense :

- Au siège de l'OTAN, la **Division Défis de sécurité émergente** est l'instance d'analyse stratégique qui assure une approche coordonnée des risques de défense et de sécurité émergents[23]. La préoccupation « cyber » figure parmi d'autres défis sécuritaires internationaux comme le terrorisme, la prolifération des armes de destruction massive ou l'insécurité énergétique[24].

- L'**Agence d'information et de communication de l'OTAN** (NCIA) soutient les opérations de l'organisation, assure la connexion des systèmes d'information et de communication, et défend également les réseaux de l'OTAN.

- La **Capacité de réaction aux incidents informatiques** (NCIRC), située au Grand quartier général des puissances alliées en Europe (SHAPE), assure la protection des réseaux de l'OTAN. Composée d'environ 200 experts, cette capacité veille continuellement à prévenir et, le cas échéant, à réagir aux incidents cyber. Cette capacité revêt aussi un rôle d'analyse des défis à venir[25].

- Enfin, la mise en place d'un **Centre des cyberopérations** (CyOC) a été décidée en 2018 par les chefs d'État rassemblés au sommet de Bruxelles. Ce Centre, intégré dans le cadre de la structure de commandement renforcée de l'OTAN, devrait être pleinement opérationnel d'ici 2023. Il permet à l'Alliance de disposer de réelles capacités de réponses cyber aux côtés des capacités conventionnelles (terre, air, mer), mises à disposition par les États membres. De même, dans le cadre de ses missions et opérations, l'OTAN pourra bénéficier de capacités informatiques nationales[26].

22. *Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé*, *op. cit.*, p. 20-21.
23. S. Lille, « L'OTAN crée une nouvelle division liée à la sécurité », site du ministère des Armées, 6 août 2010.
24. J. Joubert & J.-L. Samaan, « L'intergouvernementalité dans le cyberespace : étude comparée des initiatives de l'OTAN et de l'UE », *op. cit.*, p. 266.
25. OTAN, « Cyberdéfense de l'OTAN », Fiche d'information, février 2018.
26. OTAN, Cyber Defence.

À l'échelle de l'UE, un ensemble de moyens institutionnels existe également pour assurer la résilience dans le cyberespace. Si des parallélismes peuvent être établis avec les agences de l'OTAN, l'organisation institutionnelle est fondée sur une conception différente : elle est en premier lieu construite autour de la cybersécurité, et non spécifiquement de la cyberdéfense. La Cyberstratégie de 2013 fait de la résilience et de la cybersécurité les pierres angulaires de l'action européenne. Ainsi, dans les trois aspects mentionnés ci-dessous, il apparaît nécessaire d'appréhender les moyens de cyberdéfense comme une capacité incluse dans les structures plus larges de cybersécurité :

• Le rôle d'analyse et de veille stratégique au niveau de l'UE est tout d'abord assuré par le **Centre de l'UE pour l'analyse des renseignements (INTCEN)** à Bruxelles (Belgique), créé en 2011. Cette structure a un triple rôle : « fournir au haut représentant, au SEAE et aux États membres des analyses de renseignement, des alertes précoces et une sensibilisation à des situations géographiques particulières[27] ». L'**Institut européen pour les études de sécurité (EUISS)** à Paris (France), un *think tank* autonome relevant de la PSDC, contribue également à l'analyse en source ouverte et à la prévision des risques dans le domaine cyber. De nombreuses publications de cet organisme ont pour objet d'étude la cyberdéfense européenne.

• L'**ENISA**, à Heraklion (Grèce), est l'Agence européenne chargée de la sécurité des réseaux et de l'information. Elle fournit des recommandations et soutient l'élaboration et la mise en œuvre de politiques dans le cyber.

• La capacité de réaction de l'Union est assurée depuis 2012 par une **équipe permanente d'intervention en cas d'urgence informatique (le CERT-UE)**. Elle coopère avec les capacités de réaction des États membres et le secteur privé, afin de répondre aux incidents cyber en tout genre.

L'UE ne dispose cependant pas, à l'image du CyOC de l'OTAN, d'une capacité de réponse opérationnelle spécifique au cyber aux côtés des capacités conventionnelles. En l'absence d'une telle capacité, l'**État-major de l'UE (EMUE)** peut fournir une expertise militaire et opérationnelle. L'EMUE est la structure militaire intégrée à l'UE. Elle est rattachée au SEAE, et entièrement multinationale et interarmées. Deux de ses divisions apportent une expertise en matière de cyberdéfense. En premier lieu, la Division politique et plans (CON/CAP) est responsable des doctrines, concepts de la planification stratégique et plans de développement capacitaires[28]. Ensuite, la Division des systèmes d'information et de commandement (CIS) propose une expertise relative aux communications et aux systèmes d'information tant à un niveau stratégique qu'opérationnel. Il n'existe cependant pas de centre unique pour piloter la planification et la conduite opérationnelle dans le domaine cyber. Il revient alors aux structures de planification existantes d'intégrer la conduite opérationnelle cyber dans leurs opérations. Les cinq quartiers généraux installés au sein des États membres[29] assurent les opérations exécutives, et la Capacité militaire de planification et de conduite (MPCC) est en charge des opérations

27. Représentation permanente de la France auprès de l'Union européenne (RPUE), *Structures, acteurs et outils de la PSDC*, 2019.
28. Pour rappel, le cyber étant reconnu comme un domaine d'opération depuis 2016.
29. Mont-Valérien (France), Northwood (Royaume-Uni), Postdam (Allemagne), Rome (Italie), Larissa (Grèce).

à mandat non exécutif. La division aujourd'hui entre le MPCC et les cinq quartiers généraux pourrait compliquer le déploiement de réponses opérationnelles cyber cohérentes aux côtés de forces conventionnelles.

Assurer le facteur technique : développement capacitaire & interopérabilité

Une cyberdéfense ne peut être efficace et crédible que si elle dispose de capacités informatiques garantissant un haut niveau de résilience. L'Union et l'Alliance ont toutes les deux une plus-value dans le renforcement capacitaire afin d'atteindre la normalisation et l'interopérabilité dans ce domaine.

Aujourd'hui, les vulnérabilités de l'UE résultent notamment de la fragmentation des stratégies et des capacités nationales[30]. La coopération interinstitutionnelle est vitale afin de garantir une efficacité des mécanismes, tout autant que l'émergence d'une culture stratégique en matière de cyberdéfense. Les priorités militaires dans le domaine du cyberespace doivent être partagées au sein de l'Union[31]. L'**Agence européenne de défense (AED)** est le moteur au niveau de l'UE du soutien dans le développement de capacités des États membres. Elle participe ainsi à la coordination et l'action commune par le développement de capacités militaires jointes et standardisées. L'AED définit notamment un *Cyber Defence Strategic Research Agenda* (CSRA) afin de cibler et mutualiser les efforts en recherche et technologies nécessaires à la réalisation d'une cyberdéfense européenne résiliente[32].

L'UE dispose en effet d'un avantage particulier dans ce domaine, la recherche et développement étant une de ses compétences partagées (article 4 du TFUE). Ainsi, au-delà de l'AED, **les programmes européens pour la recherche et le développement**[33] peuvent également influer sur la base industrielle et technologique de défense européenne et pousser au développement capacitaire en matière de sécurité de l'environnement cybernétique et d'innovations technologiques. Une communication conjointe au Parlement européen et au Conseil reconnaît d'ailleurs que « le haut niveau de résilience requis en matière de cyberdéfense nécessite un ciblage spécifique des efforts en matière de recherche et de technologie[34] ».

L'OTAN, ne bénéficiant pas de compétences aussi vastes que l'UE, dispose de moyens moins larges pour influer sur le développement de capacités de ses membres. L'Alliance reste toutefois active dans ce domaine, notamment dans le cadre du processus de planification de défense. Celle-ci vise à assurer que l'OTAN dispose d'un ensemble de capacités suffisant pour garantir la sécurité de ses États membres. L'OTAN fixe ainsi des objectifs pour

30. E. Nagyfejo, *Transatlanic collaboration in response to cyber crime: how does strategic culture affect EU-US collaboration in the fight against cyber crime?*, thèse doctorale, Université de Warwick, déposée septembre 2016 ; *Résolution du Parlement européen du 13 juin 2018 sur la cyberdéfense (2018/2004(INI))*, Strasbourg, 13 juin 2018.

31. D. Deschaux-Dutard, « Cybersécurité et cyberdéfense : Éléments d'introduction du point de vue de la science politique », *op. cit.*

32. AED, *Cyber Defense*.

33. Comme « Horizon 2020 » pour la période 2014-2020 ou « Horizon Europe » pour la période 2021-2027.

34. *Résilience, dissuasion et défense : doter l'UE d'une cybersécurité solide*, Communication conjointe au Parlement européen et au Conseil [JOIN(2017) 450 final], Bruxelles, 13 septembre 2017, p. 12.

la mise en œuvre des capacités nationales. Elle pousse donc certains États à développer leurs capacités à un niveau suffisant et renforce la résilience de l'Alliance. L'OTAN a également mis en place des initiatives dites de « défense intelligente », visant à unir les efforts des pays volontaires pour développer et maintenir des capacités qui seraient autrement trop coûteuses si elles étaient développées et maintenues seules. Différents projets dans le domaine de la cyberdéfense ont été menés, comme la plateforme d'échange d'information sur les logiciels malveillants (MISP) ou le projet de développement d'une capacité multinationale de cyberdéfense (MNCD2).

Renforcer le facteur humain : les capacités d'éducation-formation

Outre la question technique, la défense est également une question de personnes. Tant dans le domaine de la cybersécurité qu'en matière de cyberdéfense, la dimension éducation-formation est donc essentielle pour assurer une préparation optimale aux menaces potentielles et pour déployer une réponse efficace.

À ce titre, diverses antennes de l'OTAN déploient des activités de cyberéducation, de formation et d'exercices afin de renforcer les capacités humaines de ses membres :

• Le **Centre d'excellence pour la cyberdéfense en coopération (CCD-COE)** à Tallinn (Estonie) est un organisme de recherche et de formation en matière de cyberdéfense. Créé hors du système OTAN, il ne fait donc pas partie de la structure de commandement. Le CCD est cependant, depuis octobre 2008, accrédité par l'OTAN comme un Centre d'excellence (COE) et une organisation militaire internationale. Depuis janvier 2018, le CCD-COE est plus spécifiquement responsable de la coordination de l'éducation et de la formation en matière de cyberdéfense pour toutes les agences otaniennes. À ce titre, le CCD-COE est greffé *de facto* au sein du Commandement allié Transformation (ACT).

L'OTAN, et d'autres acteurs variés, reste très attentif à l'expertise et aux conseils du CCD-COE[35]. Ce centre est à l'origine des deux Manuels de Tallinn, des documents influents dans l'*opinio juris* internationale et en particulier au sein de l'Alliance elle-même, sans pour autant être des politiques officielles de l'Alliance.

• Sous l'égide de la NCIA, une **Académie de la NCIA** a ouvert ses portes à Oeiras (Portugal) en septembre 2019 afin d'assurer la formation de civils et militaires à la cyberdéfense, notamment la défense des connexions des systèmes d'information et réseaux. L'École des systèmes d'information et de communication de l'OTAN (NCISS), qui était située auparavant à Latina (Italie), a été intégrée à cette Académie.

• Un **Cyberpolygone de l'OTAN** à Tartu (Estonie) permet aux experts de s'entraîner et développer leurs capacités lors d'exercices réalistes. L'exercice « Cyber Coalition », l'un des plus grands exercices cyber de l'OTAN, est facilité par cette instance chaque année[36].

35. OTAN, « NATO Cyber Defence », *Fact Sheet*, juillet 2016.
36. OTAN, « Cyberdéfense de l'OTAN », *op. cit.*

• L'**École de l'OTAN** à Oberammergau (Allemagne) conduit des formations relatives au cyber dans des domaines variés : opérations, stratégies, politiques, doctrines et procédures.

• Enfin, le **Collège de défense de l'OTAN** (Rome) propose une réflexion stratégique sur les questions politico-militaires, comprenant les questions de cyberdéfense.

Au niveau de l'UE, l'**AED** propose également des modules d'éducation et formation à la cyberdéfense nationale et européenne. L'objectif principal de ces modules est d'assurer l'intégration de la cyberdéfense dans le processus de planning opérationnel. Par ailleurs, dans un esprit de formation, l'AED mène des dialogues et des actions de coordination entre les États membres et d'autres partenaires internationaux. L'AED contribue donc aussi à la valorisation de l'expertise de l'UE dans ce domaine. Ainsi, ces échanges renforcent la cyberdéfense de l'Union en dissuadant « par déni » des adversaires belliqueux potentiels[37]. Le **Collège européen de sécurité et de défense** joue également un rôle important en termes de formation aux questions cyber, mais s'adresse à un public plus large. Le contenu pédagogique du Collège comprend des éléments de formation relatifs à tous les aspects cyber, mais aussi sur d'autres questions comme les menaces hybrides qui peuvent impliquer des questions cyber dans des activités militaires plus larges.

Concernant des exercices réalistes et préparations aux attaques cyber, l'**ENISA** est active dans ce domaine ; elle déploie essentiellement des exercices de cybersécurité, à l'image de l'exercice « Blue OLEx » organisé en France en 2019. Il faut cependant se tourner vers l'**EMUE** pour les exercices de renforcement des capacités en matière de cyberdéfense. L'EMUE conduit aussi dans ce cadre des consultations étroites et des activités de coordination avec l'OTAN et d'autres organisations internationales.

Capacités diplomatiques : allier le *soft* et *hard power*

Le 19 juin 2017, le Conseil de l'Union européenne a adopté le *Cyber Diplomacy Toolbox* (CDT). Ce CDT se veut être une réponse diplomatique conjointe aux cyberactivités malicieuses[38]. Pour Van der Meer[39], cette « boîte à outils » a été conçue comme un outil dissuasif important en identifiant les conséquences potentielles d'une réponse diplomatique commune ; une initiative de « *soft power* collectif » qui vient équilibrer et compléter les développements de capacités défensives et offensives des États membres de l'UE ou au sein de l'OTAN[40]. Par ailleurs, depuis le 17 mai 2019, le Conseil européen est désormais en mesure d'imposer des « mesures restrictives ciblées visant à dissuader et contrer les cyberattaques ayant des effets importants qui constituent une menace extérieure pour l'Union ou ses États membres » (Décision 019/797 du Conseil). Le régime de sanction est en effet défensif face aux attaques et tentatives de cyberattaques.

37. J. Joubert, « La dissuasion au défi du cyberespace », *Les Champs de Mars*, n° 25, 2013.
38. P. Pawlak & E. Moret, « The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime? », Issue Brief n° 24, EUISS, 2017
39. S. Van der Meer, « EU Creates a Diplomatic Toolbox to Deter Cyberattacks », *Council on Foreign Relations* (blog), 20 septembre 2017.
40. *Ibid.*

Par ailleurs, l'AED apporte sa contribution à l'émergence d'un discours européen sur le cyber au niveau international[41]. Disposer d'une culture stratégique au niveau européen contribuerait non seulement à renforcer la cyberdéfense en interne, mais également à la consolider en externe. Ce discours européen est un deuxième élément important dans le cadre de la dissuasion « par déni » mentionnée plus haut[42]. À cet effet, la Cyberstratégie de l'UE[43] demande à l'AED de mener « le dialogue et la coordination entre les acteurs civils et militaires dans l'UE », mais aussi avec des partenaires internationaux autres que l'OTAN.

L'ARTICULATION DES DEUX CYBERDÉFENSES

L'analyse des compétences et moyens de l'UE et de l'OTAN démontre la construction progressive de leurs architectures de cyberdéfense. Néanmoins, de nombreux doublons et zones grises sont rapidement identifiables et peuvent entraîner des incertitudes. Une prise de conscience de l'importance de la coordination des deux institutions apparaît dès lors nécessaire, et fait petit à petit son chemin. L'objectif est donc la recherche de la complémentarité ou du moins une coordination plus étroite des deux. Celles-ci favoriseraient l'émergence d'une cyberdéfense collective renforcée et plus résiliente en Europe. Il s'agirait notamment d'être en mesure de clarifier les périmètres d'action respectifs de l'UE et de l'OTAN, spécifiquement pour les pays membres des deux systèmes. Par exemple, dans l'hypothèse où l'un de ces États subirait une cyberattaque de l'ampleur d'une agression armée, le choix politique entre le recours à l'article 5 TAN ou l'article 42.7 TUE pourrait en être facilité.

Une articulation limitée entre l'Union et l'Alliance

Au même titre que la défense plus généralement, la *cyber*défense de l'Union ne peut se concevoir sans prendre en compte celle de l'Alliance. La résolution « cyberdéfense » de 2018 rappelle d'ailleurs l'importance du « cadre de l'architecture de sécurité transatlantique » dans ce contexte.

La cybersécurité et la cyberdéfense constituent ensemble l'un des sept domaines de coopération renforcée entre l'OTAN et l'UE depuis la Déclaration commune sur le renforcement de la coopération pratique, signée à Varsovie en juillet 2016. Quelques mois auparavant, en février, un accord technique entre les deux institutions avait également été signé afin de renforcer leur coopération en matière de cyberdéfense. Spécifiquement, cet accord entre la capacité de réaction aux incidents informatiques de l'OTAN (NCIRC) et le CERT-UE visait à renforcer la protection contre les cyberattaques par le partage notamment de pratiques de référence. Il existe donc une coordination renforcée entre les deux institutions

41. A. Barrinha, *The EDA and the discursive construction of European defence and security,* dans N. Karampekios & I. Oikonomou, *The European Defence Agency: arming Europe*, Londres, Routledge, 2015.
42. J. Joubert, « La dissuasion au défi du cyberespace », *op. cit.*
43. *Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé*, *op. cit.*, p. 12.

dans ce domaine, se traduisant par l'échange d'informations, de meilleures pratiques, des formations et exercices conjoints, l'objectif ultime étant l'interopérabilité des capacités. Ces éléments ont d'ailleurs été rappelés dans la plus récente déclaration conjointe sur la coopération entre l'UE et l'OTAN signée l'année dernière, le 10 juillet 2018.

Cependant, cette coordination reste limitée. Comme l'ont exprimé J. Joubert et J.-L. Samaan[44], il est difficile d'identifier les éléments de complémentarité ou de subsidiarité entre les deux. La cybridisation de la défense collective en Europe se limite essentiellement à des exercices et formations, et les moyens capacitaires manquent encore. Par ailleurs, malgré la volonté d'établir des chaînes de commandement et des systèmes de réponses à travers les institutions, celles-ci peinent à être mises en place, tant au niveau de l'UE[45] qu'au niveau de l'OTAN[46]. Les deux organisations connaissent la même difficulté que peut présenter l'intergouvernementalisme. La souveraineté nationale peut alors apparaître comme un frein au développement d'une cyberdéfense commune avec des capacités mutuelles[47]. Si l'OTAN commence à développer ses capacités de cyberdéfense aux côtés de ses capacités conventionnelles, ce n'est qu'un développement naissant. Pour l'UE, comme plus largement dans le projet d'une « Europe de la défense », l'institution n'arrive pas à développer des capacités conventionnelles propres du fait des volontés politiques nationales divergentes[48]. La PSDC reste une politique intergouvernementale dont l'unanimité est la règle (article 42 § 4 TUE).

Si beaucoup d'efforts ont été faits pour adapter les structures de sécurité et de défense collective en Europe aux menaces émergentes du cyberespace, il persiste encore plusieurs défaillances dans l'architecture régionale : complexité de structures se chevauchant, dédoublement de certaines activités et manque de subsidiarité claire entre l'OTAN et l'UE, difficile développement capacitaire et manque d'interopérabilité, absence de définition de doctrines claires, etc. La cyberdéfense collective reste encore en construction.

Une complémentarité possible dans une approche plus globale à la cyberdéfense collective

Pourtant, l'UE et l'OTAN présentent plusieurs points communs dans des domaines plus larges que des exercices opérationnels, la recherche de l'interopérabilité ou le renforcement des capacités. En termes de mesures de confiance, de références, en termes d'applicabilité du droit international, de relations avec le secteur privé ou avec d'autres partenaires internationaux, l'UE et l'OTAN partagent des approches très similaires. Ces éléments constituent des pistes de réflexion potentielles vers le développement des synergies communes ou complémentaires.

44. J. Joubert & J.-L. Samaan, « L'intergouvernementalité dans le cyberespace : étude comparée des initiatives de l'OTAN et de l'UE », *op. cit.*, p. 275.
45. D. Fiott, « The cybridisation of EU defence », Issue Alert n° 24, EUISS, 2017.
46. J. Joubert & J.-L. Samaan, « L'intergouvernementalité dans le cyberespace : étude comparée des initiatives de l'OTAN et de l'UE », *op. cit.*
47. *Ibid.*, p. 272-274.
48. D. Fiott, « The cybridisation of EU defence », *op. cit*.

En premier lieu, la cyberdéfense européenne doit promouvoir la coopération et l'échange dans le but de réduire le risque de conflits. Pour ce faire, les mesures de confiance (MDC) constituent des outils particulièrement efficaces. Ceci est notamment vrai au regard du cyberespace, caractérisé par une certaine opacité. L'OSCE par exemple, par sa décision n° 1202 (2016) a mis en place un cadre élaboré de MDC destiné à réduire les conflits interétatiques découlant de l'utilisation des technologies de l'information et des communications (TIC). Il serait pertinent pour l'OTAN et l'UE de s'inspirer de ces MDC spécifiques au cyberespace. Au-delà de la mise en place d'un cadre élaboré de MDC au sein des membres de leurs institutions, des coopérations autour des MDC dans un premier temps entre l'UE et l'OTAN, et ensuite éventuellement avec d'autres organisations régionales en Europe (comme l'OSCE justement) et au-delà seraient de nature à renforcer l'efficacité de la cyberdéfense européenne.

En deuxième lieu, il est important pour la cyberdéfense européenne d'entretenir des liens étroits avec le secteur privé, notamment industriel, un acteur incontournable dans le cyberespace. En effet, dans la mesure où la majorité des réseaux sont détenus et gérés par des acteurs privés, il est difficile de concevoir une cyberdéfense qui ne repose pas sur un ensemble de capacités, civiles et militaires, publiques et privées[49]. Une complémentarité entre l'OTAN et l'UE peut aussi être développée à cet égard, notamment au niveau industriel. Pour D. Fiott[50], c'est la base industrielle et technologique de défense européenne qui tient la clé de l'interopérabilité européenne et l'harmonisation des capacités de cyberdéfense. Des éléments de politique industrielle (soutenir l'investissement, soutenir la R&D, faciliter l'accès au marché ou aux financements, favoriser l'émergence d'une main-d'œuvre spécialisée) sont donc des outils à ne pas négliger dans le cadre de la mise en place d'une politique de cyberdéfense efficace.

L'UE, comme décrit plus haut, dispose de moyens particulièrement puissants à ce titre grâce à ses compétences élargies. Le « Cyberpartenariat OTAN-industrie » (NCIP), mis en place en 2014[51], pourrait alors se rapprocher des activités de l'UE dans ce domaine, notamment celles dans le contexte de « Horizon 2020 »/« Horizon Europe ». Une coopération avec l'AED et son CSRA ou encore la Banque européenne d'investissements, capable d'apporter un financement à certains projets de cybersécurité/cyberdéfense, pourrait également être porteur. Ce rapprochement aurait pour but d'harmoniser certains efforts pour accélérer les progrès et l'innovation. En outre, au-delà de l'aspect industriel, l'UE et l'OTAN peuvent également travailler de concert avec le secteur privé au niveau opérationnel pour promouvoir le partage d'information (entre secteur privé et gouvernement, mais aussi au sein du secteur privé), ainsi que pour l'adoption de standards communs fondés sur les meilleures pratiques identifiées. En effet, sur ce dernier point, la standardisation des pratiques de sécurité et des moyens de réponse permet une cybersécurité – et donc aussi par extension une cyberdéfense – plus robuste. Cette normalisation devrait être généralisée à tous les acteurs impliqués.

49. Observatoire du monde cybernétique, « Industrie de la cybersécurité : quelles synergies public-privé ? », Lettre n° 40, juillet 2015.
50. D. Fiott, « The cybridisation of EU defence », *op. cit.*
51. OTAN, « Cyberdéfense de l'OTAN », *op. cit.*

Par ailleurs, la cyberdéfense européenne a également un rôle à jouer dans les discussions et négociations internationales sur le droit international applicable au cyberespace. En effet, si beaucoup de discussions ont eu lieu sur l'applicabilité du droit dans le cyberespace, notamment dans le cadre de l'ONU au travers de son Groupe d'experts gouvernementaux (UNGGE)[52], il n'existe pas de position communément adoptée au niveau international et il reste encore beaucoup à faire[53]. L'UE et l'OTAN reconnaissent tous les deux l'applicabilité du droit international dans le cyberespace. Une coordination plus étroite des deux instances sur les normes et mesures répressives possibles dans le cyberespace constituerait donc déjà un progrès important pour la région européenne. Par ailleurs, dans le cadre des discussions internationales sur cette question, l'UE peut être un influenceur de taille et jouer un rôle considérable dans les négociations étant membre observateur très actif au sein de l'ONU, dotée d'une force de coordination des positions de ses États membres. L'UE pourrait défendre, avec ces derniers, les valeurs qu'elle promeut pour un cyberespace « ouvert, sûr et sécurisé », comme l'indique le titre de sa doctrine de cybersécurité[54], l'applicabilité du droit international dans le cyberespace étant l'une des pierres angulaires de celle-ci. Tout en reconnaissant que le traité fondateur ne confère pas de compétence à l'OTAN pour défendre des positions au nom de ses États membres au même titre que l'UE depuis le traité de Lisbonne, l'influence diplomatique de l'UE sera d'autant plus importante dans les négociations que les États membres de l'OTAN et de l'UE arrivent auparavant à s'accorder sur les règles applicables en Europe.

Enfin, l'OTAN et l'UE doivent également travailler étroitement avec les États tiers. Une cyberdéfense efficace nécessite d'entretenir un dialogue accru avec les États tiers afin de contribuer à la minimisation des risques de conflits. Les mesures de confiance sont donc également à mettre en œuvre avec des États extérieurs à l'Union et à l'Alliance (des États particulièrement actifs dans le cyberespace par exemple). Par ailleurs, des partenariats stratégiques plus poussés peuvent également être envisagés. Les relations étroites que les États-Unis et le Canada ont en commun avec l'Europe pourraient servir de base à un partenariat renforcé entre ces régions. L'Australie par exemple a un programme de coopération avec l'UE (août 2017) ainsi qu'avec l'OTAN (août 2019) comprenant tous les deux plusieurs aspects relevant du cyber, notamment la lutte contre les menaces de tout genre dans ce domaine. Une approche coordonnée UE/OTAN avec certains partenaires dans le domaine de la cyberdéfense pourrait présenter de nombreux bénéfices.

Ainsi, une cyberdéfense collective pour l'Europe doit être globale dans son approche. Étendre son action au-delà de considérations opérationnelles constitue le meilleur moyen d'assurer une robustesse des défenses dans l'espace cybernétique. Une approche coordonnée dans ce cadre, avec en particulier une articulation claire des deux systèmes de cyberdéfense collective, renforcera les objectifs recherchés et représentera un rapport de force affirmé.

---

52. F. Delerue, « Cyber Operations and the Prohibition of the Threat of Force », *Opinio Juris, Emerging Voices Symposium*, juillet 2014.

53. F. Delerue & A. Gery, « Le droit international dans la "stratégie nationale de la cyberdéfense" », Note de recherche n° 58, IRSEM, 2018.

54. *Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé*, *op. cit.*

CONCLUSION

Le cyberespace représente donc un nouveau domaine pour l'action collective en Europe. Une cyberdéfense collective permet à l'ensemble de la région et aux États qui la composent de s'armer plus efficacement contre la menace cyber. L'OTAN et l'UE œuvrent à la construction de celle-ci, mais elle n'est pas encore aboutie. Ces deux institutions, par leur composition et le fait qu'elles partagent une majorité de membres en commun, ont une zone d'action en Europe très similaire, ce qui donne lieu à certains chevauchements et doublons des activités. Afin que leurs actions soient les plus efficaces possibles, elles devraient toutes les deux trouver un fonctionnement complémentaire avec des éléments clairs de subsidiarité l'une avec l'autre. En l'absence de complémentarité, une approche coordonnée reste un minimum pour conserver la crédibilité de la cyberdéfense collective en Europe. L'adhésion commune de 22 États doit constituer une force importante dans cette démarche de rapprochement et de coordination.

Enfin, cette cyberdéfense, quelle qu'en soit la forme, doit être globale dans son approche. Sans se limiter aux réponses opérationnelles ou éléments capacitaires, elle doit contribuer plus généralement à la paix et la sécurité internationale par la promotion de mesures de confiance avec tous les acteurs internationaux (États, organisations, entreprises), par la participation aux discussions sur l'applicabilité du droit international au cyberespace et par la poursuite de synergies conjointes avec le secteur privé. L'aspect dual du cyberespace implique que la réglementation civile relative au cyber est également prescriptrice pour les applications militaires. L'UE, dotée d'une capacité régulatrice bien supérieure à celle de l'OTAN, joue ainsi un rôle déterminant pour la cyberdéfense, même si sa préoccupation première se porte sur la cybersécurité.

Aujourd'hui, les États membres de l'OTAN semblent disposer de plus d'outils pour réagir à un niveau opérationnel en cas de cyberattaques belliqueuses, notamment grâce à la mise en route du Centre des cyberopérations intégré dans le cadre de la structure de commandement renforcée. Pourtant, l'opportunité réelle réside dans l'UE, qui agit sur l'ensemble du spectre cybersécurité-cyberdéfense. Puissance diplomatique, disposant d'un *soft power* européen important, elle doit aujourd'hui renforcer ses compétences et moyens dans ce domaine, spécifiquement en cyberdéfense alors que la viabilité de l'Alliance est interrogée par le président américain, Donald Trump. Par ailleurs, avec la sortie imminente du Royaume-Uni de l'Union, principal facteur de blocage dans le développement d'une politique de défense européenne, une nouvelle dynamique vers une politique commune (ou du moins des éléments de défense commune) semble possible. Dans ce contexte particulier, l'UE a plus que jamais l'opportunité de développer une culture stratégique propre, lui permettant d'affirmer son autonomie stratégique et de se construire un *hard power* européen dans le cyberespace.

BIBLIOGRAPHIE

Ouvrages et articles

AED, *Cyber Defense* (en ligne).

BARRINHA A., *The EDA and the discursive construction of European defence and security,* dans KARAMPEKIOS N. & OIKONOMOU I., *The European Defence Agency: arming Europe*, Londres, Routledge, 2015, p. 27-42.

COMMISSION EUROPÉENNE, « Questions-réponses : l'avenir de la défense européenne », Fiche d'information, 2017 (en ligne).

DELERUE F., « Cyber Operations and the Prohibition of the Threat of Force », *Opinio Juris, Emerging Voices Symposium*, juillet 2014.

DELERUE F. & GERY A., « Le droit international dans la "stratégie nationale de la cyberdéfense" », Note de recherche n° 58, IRSEM, 2018.

DESCHAUX-DUTARD D., « Cybersécurité et cyberdéfense : Éléments d'introduction du point de vue de la science politique », dans *Cyber, Nano : Nouvelles technologies et nouveaux enjeux sécuritaires*, Cours dans le cadre du master Sécurité internationale et défense de la faculté de droit de Grenoble, 2017, p. 27.

FIOTT D., « The cybridisation of EU defence », Issue Alert n° 24, EUISS, 2017.

JOUBERT J., « La dissuasion au défi du cyberespace », *Les Champs de Mars*, n° 25, 2013, p. 75-90.

JOUBERT J. & SAMAAN J.-L., « L'intergouvernementalité dans le cyberespace : étude comparée des initiatives de l'OTAN et de l'UE », *Hérodote*, n° 152-153, 2014, p. 261-275.

HUME D., *Essay on the Balance of Power,* 1754.

KEMPF O., *Alliances et mésalliances dans le cyberespace*, Economica, 2014, p. 191.

LILLE S., « L'OTAN crée une nouvelle division liée à la sécurité », site du ministère des Armées, 6 août 2010.

NAGYFEJO E., *Transatlanic collaboration in response to cyber crime: how does strategic culture affect EU-US collaboration in the fight against cyber crime?*, thèse doctorale, Université de Warwick, déposée septembre 2016.

OBSERVATOIRE DU MONDE CYBERNÉTIQUE, « Industrie de la cybersécurité : quelles synergies public-privé ? », Lettre n° 40, juillet 2015.

OTAN, « NATO Cyber Defence », *Fact Sheet*, juillet 2016.

OTAN, « Cyberdéfense de l'OTAN », Fiche d'information, février 2018.

PAWLAK P. & MORET E., « The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime? », Issue Brief n° 24, EUISS, 2017.

REPRÉSENTATION PERMANENTE DE LA FRANCE AUPRÈS DE L'UNION EUROPÉENNE (RPUE), *Structures, acteurs et outils de la PSDC*, 2019 (en ligne).

TERTRAIS B., « Article 5 of the Washington Treaty: It's Origins, Meaning and Future », Research Paper n° 130, NATO Defense College, 2016, p. 1-8.

VAN DER MEER S., « EU Creates a Diplomatic Toolbox to Deter Cyberattacks », *Council on Foreign Relations* (blog), 20 septembre 2017.

WALT S., *The Origins of Alliances*, Ithaca, Cornell University Press, 1990, p. 336.

Documents officiels

Cyberdéfense : un nouvel enjeu de sécurité nationale, Rapport d'information n° 449 (2007-2008) de M. Roger Romani, fait au nom de la commission des affaires étrangères, déposé le 8 juillet 2008.

Rapport du Groupe d'experts gouvernementaux (GGE) chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale, document des Nations unies A/68/98, 2013.

Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé, Communication conjointe au Parlement européen, au Conseil, au CESE et au Comité des Régions, [JOIN(2013) 1 final], Bruxelles, 7 février 2013.

Rapport du Groupe d'experts gouvernementaux (GGE) chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale, document des Nations unies A/70/174, 2015.

Mesures de confiance de l'OSCE visant à réduire les risques de conflit découlant de l'utilisation des technologies d'information et de communication, Décision n° 1202 du Conseil permanent de l'OSCE, fait lors de la 1092e séance plénière le 10 mars 2016,

Communiqué du sommet de Varsovie publié par les chefs d'État et de gouvernement participant à la réunion du Conseil de l'Atlantique nord tenue à Varsovie les 8 et 9 juillet 2016, Varsovie, 9 juillet 2016 [consulté le 27 juillet 2018].

Résilience, dissuasion et défense : doter l'UE d'une cybersécurité solide, Communication conjointe au Parlement européen et au Conseil [JOIN(2017) 450 final], Bruxelles, 13 septembre 2017.

Revue stratégique de cyberdéfense, SGDSN, Paris, 12 février 2018.

Résolution du Parlement européen du 13 juin 2018 sur la cyberdéfense (2018/2004(INI)), Strasbourg, 13 juin 2018.

Déclaration conjointe du président du Conseil européen, du président de la Commission européenne et du secrétaire général de l'Organisation du traité de l'Atlantique nord sur la coopération entre l'UE et l'OTAN, Bruxelles, 10 juillet 2018.

Décision (PESC) 2019/797 du Conseil du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres, Bruxelles, 17 mai 2019.

Cet article s'inspire des recherches menées dans le cadre du mémoire « La cyberguerre en Europe : une cyberdéfense collective ? » (2018) rédigé dans le cadre du diplôme de Master 2, Droit international, Sécurité internationale et défense de l'Université Grenoble-Alpes.

Morgan Jouy est diplômé en administration publique, en relations internationales et en droit international. Ses intérêts portent notamment sur le multilatéralisme, la cyberdéfense, la non-prolifération et le désarmement. Il a été assistant de recherche à l'IRSEM en 2017.

Contact : morgan.jouy@sciencespo.fr