L'UNION EUROPÉENNE, UNE CYBERPUISSANCE EN DEVENIR ? RÉFLEXION SUR LA CYBERDÉFENSE EUROPÉENNE

Delphine Deschaux-Dutard

Armand Colin | « Revue internationale et stratégique »

2020/1 N° 117 | pages 18 à 29

ISSN 1287-1672
ISBN 9782200933326

Article disponible en ligne à l'adresse :

https://www.cairn.info/revue-internationale-et-strategique-2020-1-page-18.htm

ÉCLAIRAGES

L'Union européenne, une cyberpuissance en devenir ? Réflexion sur la cyberdéfense européenne

Delphine Deschaux-Dutard

Docteur en science politique, maître de conférences à l'Université Grenoble Alpes, chercheure au Centre d'études sur la sécurité internationale et les coopérations européennes (CESICE).

Résumé

Cet article se penche sur la façon dont l'Union européenne (UE) développe, ces dernières années, une stratégie et des outils de cyberdéfense. Dans un monde de plus en plus connecté, comment l'UE conçoit-elle son rôle dans le cyberespace ? En quoi les initiatives européennes en matière de cyberdéfense traduisent-elles le rapport ambigu de l'Union à la notion de puissance ? Après avoir présenté les aspects stratégiques et institutionnels de la cyberdéfense européenne comme autant de facteurs d'une capacité de cyberdéfense émergente, l'article explore les limites de cette capacité et propose une interrogation sur le rapport entre l'UE et la notion de cyberpuissance.

Abstract

This article focuses on how the European Union (EU) has been developing, for the past few years, strategic thinking and tools in the area of cyberdefence. In an increasingly connected world, how does the EU conceive its role in cyberspace? To what extent do European initiatives in the area of cyberdefence express the EU's ambiguous relationship with the notion of power? After assessing the strategic and institutional elements of European cyberdefence, this paper explores the limits of European initiatives and offers insight on the relationship between the EU and the idea of cyber power.

Dans son discours du 13 septembre 2017 sur l'état de l'Union, le président de la Commission européenne d'alors, Jean-Claude Juncker, déclarait : **« Au cours des dernières années, nous avons fait des progrès notables dans la sécurisation de l'Internet. [...] Mais l'Europe reste mal équipée face aux cyberattaques. Les cyberattaques sont parfois plus dangereuses pour la stabilité des démocraties et des économies que les fusils et les chars. »**[1] De fait, ces cyberattaques tendent à se multiplier depuis une décennie et affectent de plus en plus les États membres de l'Union européenne (UE), à l'instar de celles subies par l'Estonie en 2007,

1. Jean-Claude Juncker, « Discours sur l'état de l'Union 2017 », Bruxelles, 13 septembre 2017.

voire les institutions européennes elles-mêmes. De nombreux chefs d'État et de gouvernement européens, dont le président de la République française, et des responsables des institutions européennes – Commission et Parlement, notamment – avaient d'ailleurs appelé à la plus grande vigilance numérique lors des élections européennes de mai 2019 face aux risques de désinformation et de déstabilisation politique. Ils organisèrent même, en avril 2019, le premier grand exercice cybersécuritaire européen[1]. Face à un risque de cyberguerre multiforme et diffuse dont on peut de plus en plus douter qu'elle n'aura pas lieu[2], l'UE a dû, ces dernières années, commencer à se positionner en tant qu'acteur du cyberespace. Ce dernier est en effet devenu un cinquième champ de conflictualité militaire, aux côtés des espaces traditionnels de bataille comme la terre, l'air, la mer et l'espace stratosphérique[3]. Confrontée à une forme de cyberguerre froide[4] menée par des forces extérieures à l'encontre de ses États membres et de ses institutions, l'UE a ainsi initié les prémisses d'une cyberdéfense à l'échelle européenne. Comment conçoit-elle ce sujet et existe-t-il une spécificité européenne en la matière ? Le cyberespace peut-il permettre à l'UE d'avancer sur le chantier de son autonomie stratégique et de son positionnement en tant que puissance sur la scène internationale ?

L'Union européenne, une cyberpuissance en construction ?

Si la question de savoir quel type de puissance incarne l'UE n'est pas nouvelle[5], il apparaît toutefois intéressant de l'appliquer au cas du positionnement de l'UE au sein du cyberespace. Être une cyberpuissance signifie en effet être un acteur capable d'agir sur le cyberespace en influençant les comportements des autres. Une telle ambition s'appuie nécessairement sur une stratégie et sur des moyens. Pour savoir si l'UE ambitionne un statut de cyberpuissance, il

1. Cet exercice a réuni le Parlement européen, la Commission européenne, les États membres et l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA). Voir Commission européenne, « EU Member States test their cybersecurity preparedness for fair and free 2019 EU elections », Communiqué de presse, Bruxelles, 5 avril 2019.
2. Quoi qu'en dise Thomas Rid, *Cyberwar Will Not Take Place*, Oxford, Oxford University Press, 2013.
3. Voir Daniel Ventre, *Cyberattaque et cyberdéfense*, Paris, Lavoisier, 2011.
4. La cyberguerre froide désigne un état du cyberespace dans lequel les États se munissent d'un arsenal cybernétique – tant défensif qu'offensif – et recourent – souvent indirectement *via* des acteurs non étatiques – à des cyberattaques dans le cadre de manœuvres de déstabilisation sans franchir le seuil qui caractériserait une cyberguerre ouverte. Plus généralement sur la notion de cyberguerre, voir Nicolas Arpagian, *La Cyberguerre. La guerre numérique a commencé*, Paris, Vuibert, 2009. Sur les aspects stratégiques, voir Olivier Kempf, « Cyber et surprise stratégique », *Stratégique*, vol. 106, n° 2, 2014.
5. Voir notamment Bastien Nivet, *L'Europe puissance, mythes et réalité. Une étude critique du concept d'Europe puissance*, Bordeaux, Presses universitaires de Bordeaux, 2019.

convient donc de se pencher sur la place qu'occupe le cyberespace dans sa réflexion stratégique.

Une cyberdéfense encore marginale dans l'architecture normative stratégique européenne

L'UE a développé un intérêt pour le cyberespace dès la fin des années 1990, à la suite de cyberattaques menées par des *hackers* serbes à l'encontre du site Internet du Commandement suprême des forces alliées en Europe (SHAPE) de l'Organisation du traité de l'Atlantique Nord (OTAN)[1]. La plupart des États de l'Union étant membres de l'OTAN, l'UE a, à son tour, commencé à se pencher sur le cyberespace. La Commission européenne a ainsi lancé une série de directives au début des années 2000 visant à protéger les droits fondamentaux des citoyens européens et leurs libertés dans le cadre des activités économiques et commerciales en ligne. Cette dimension économique a longtemps prévalu dans les normes européennes relatives au domaine cybernétique. La stratégie européenne de sécurité de 2003 ne faisait, par exemple, aucune mention des cybermenaces.

L'**UE** a développé un **intérêt** pour le **cyberespace** dès la fin des années **1990**

Les cyberattaques à l'encontre de l'Estonie et de la Géorgie en 2007-2008 ont impulsé une nouvelle étape de réflexion et, en février 2013, l'UE s'est dotée d'une stratégie de cybersécurité – dont le sous-titre plaide pour un cyberespace ouvert, sûr et sécurisé[2]. Cette stratégie vise la résilience de l'Union aux cyberattaques, et fait de la cyberdéfense l'une des cinq priorités à développer au niveau européen. L'UE s'est ainsi équipée, ces dernières années, de documents stratégiques visant à l'inscrire de plain-pied en tant qu'acteur de la régulation du cyberespace, y compris dans les domaines militaires et diplomatiques. Un cadre d'action pour une réponse diplomatique conjointe de l'UE face aux activités cybermalveillantes – appelé également « boîte à outils cyberdiplomatique » – a notamment été adopté par le Conseil européen en juin 2017, en vue de coordonner les réponses aux cyberattaques et de permettre l'adoption de sanctions à l'encontre des attaquants. Cette capacité

1. Voir Vincent Joubert et Jean-Loup Samaan, « L'intergouvernementalité dans le cyberespace : étude comparée des initiatives de l'OTAN et de l'UE », *Hérodote*, n° 152-153, 2014/1-2.
2. Service européen pour l'action extérieure (SEAE), « Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace », 7 février 2013.

a été approfondie en mai 2019, démontrant une réelle volonté européenne d'exister en tant qu'acteur diplomatique dans le cyberespace.

La cyberdéfense repose, quant à elle, sur le volet militaire de l'action extérieure de l'UE dans le domaine cybernétique. La stratégie de cybersécurité européenne inclut pour la première fois la cyberdéfense dans les activités de défense de l'UE, réunies dans le cadre de la politique de sécurité et de défense commune (PSDC). Ce document stratégique invoque d'ailleurs la possibilité d'utiliser la clause de solidarité contenue dans le traité sur le fonctionnement de l'UE (TFUE, article 222) en cas de cyberattaque : « Un cyber incident ou une cyberattaque particulièrement sérieux pourrait constituer une raison suffisante pour qu'un État membre invoque la clause de solidarité »[1]. Enfin, la stratégie de cybersécurité de l'UE définit quatre priorités en matière de cyberdéfense européenne : le développement de capacités et d'un cadre pour une politique de cyberdéfense en coordination avec les États membres, la promotion du dialogue civilo-militaire sur les questions cyber et le dialogue avec des partenaires internationaux tels que l'OTAN. Pour autant, la stratégie demeure assez vague et a nécessité l'adoption de normes complémentaires pour faire progresser la cyberdéfense à l'échelle européenne, depuis le cadre stratégique d'action pour la cyberdéfense de l'UE, adopté par le Conseil en 2014, jusqu'à la communication conjointe publiée par les institutions européennes en juin 2018 et intitulée « Augmenter la résilience et renforcer les capacités pour faire face aux menaces hybrides ».

Ainsi semble-t-il de plus en plus évident, d'un point de vue stratégique, que l'UE commence à se positionner comme un acteur de sécurité du cyberespace, même si les dimensions économiques et liées aux libertés politiques marquent encore largement la réflexion européenne en la matière. Une stratégie n'étant opérante que si on lui alloue des moyens, l'UE développe aussi quelques outils de cyberdéfense afférents.

Des outils de cyberdéfense émergents

L'UE s'est dotée de plusieurs types d'outils allant de pair avec cette stratégie en matière de cyberdéfense. Tout d'abord, il existe des outils juridiques prévus par les traités européens, tels que la clause de défense mutuelle – l'article 42§7 du Traité sur l'Union européenne invoqué par François Hollande à la suite des attentats de novembre 2015 à Paris[2] – ou encore la clause de solidarité (article 222 du TFUE)[3]. Bien que ces deux clauses ne fassent pas

1. *Ibid*. Notre traduction.
2. Cette clause dispose : « 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. »
3. Cette clause dispose notamment : « 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

expressément référence à la cyberdéfense, elles pourraient être invoquées dans le cas d'une cyberattaque qui franchirait le seuil du cyberconflit armé, c'est-à-dire qui aurait des conséquences létales et causerait des dommages de même nature qu'une agression par des armes conventionnelles[1]. Pour autant, l'utilisation de la clause de défense mutuelle soulèverait la difficile question de l'attribution de la cyberattaque à un acteur étatique ou non étatique, bénéficiant du soutien plus ou moins identifié d'un État tiers. Une telle attribution nécessiterait, au préalable, un consensus au sein du Conseil européen, ce qui ne manquerait pas de produire des difficultés. Par exemple, pourrait-on à coup sûr obtenir un consensus entre États européens si une cyberattaque massive, avec des conséquences létales, pointait vers une responsabilité russe ? Rien n'est moins sûr. C'est donc davantage la clause de solidarité qui semble apporter une piste pour la cyberdéfense à court terme, dans la mesure où une cyberattaque de grande ampleur, mais dont le seuil ne permettrait pas de la qualifier comme une agression armée, s'apparenterait au cas d'une catastrophe naturelle permettant aux États membres de demander de l'aide aux institutions de Bruxelles ainsi qu'à leurs partenaires européens. En matière opérationnelle, cela se traduirait par une aide logistique et matérielle, apportée par les institutions bruxelloises et les autres États membres, à l'État touché, pour lui permettre, par exemple, de rétablir les réseaux informatiques affectés en dépêchant des équipes de réponse informatique rapide (CERT), d'attribuer la provenance de l'attaque, etc.

Pourrait-on à coup sûr obtenir un **consensus** entre États européens si une **cyberattaque** massive, avec des **conséquences létales**, pointait vers une **responsabilité russe** ?

Un deuxième type d'outil permet de développer progressivement des capacités européennes de cyberdéfense. Il s'agit de la coopération structurée permanente (CSP), outil institutionnel de coopération entre un groupe d'États

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. »

1. Voir Erica Moret et Patryk Pawlak, « The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime? », *Brief*, n° 24, European Union Institute for Security Studies (EUISS), juillet 2017.

volontaires lancé en décembre 2017, et qui compte aujourd'hui 43 projets, dont plus d'un tiers porte sur des questions relatives au cyberespace. Cette coopération va par exemple permettre de créer des équipes de réaction rapide et d'assistance mutuelle (*Cyber Rapid Response Teams and Mutual Assistance in Cybersecurity*) donnant l'opportunité à la fois de développer les exercices et entraînements et de mieux coordonner les réponses aux cyberattaques qui auraient des implications militaires. Conduit par la Lituanie, ce projet n'est pas sans rappeler le cas des groupements tactiques de l'UE, unités militaires multinationales mises sur pied en 2007, mais qui demeurent des unités de papier, puisqu'elles n'ont jamais encore pu être déployées sur des théâtres d'opération militaire. Le mécanisme de prise de décision à l'unanimité, qui prévaut également dans le cadre de la CSP, tend en effet à bloquer le recours à ce type d'outils en nécessitant, là encore, un consensus souvent introuvable.

À ces outils juridiques et institutionnels vient enfin s'ajouter un troisième type, relevant de la cyberdiplomatie. L'UE conduit non seulement plusieurs cyberdialogues avec des partenaires stratégiques tels que les États-Unis, la Chine, l'Inde ou encore l'OTAN, mais peut aussi, depuis mai 2019, prononcer des sanctions. Les cyberattaques pouvant faire l'objet de sanctions européennes sont celles provenant ou étant conduites depuis l'extérieur du territoire de l'UE ; utilisant une infrastructure hors UE ; conduites par des personnes ou des entités établies ou opérant hors UE ; conduites avec l'aide de personnes ou d'entités opérant hors UE. Les sanctions concerneront, en l'espèce, des personnes ou entités responsables de cyberattaques ou de tentatives de cyberattaques, et / ou apportant un soutien financier, technique ou matériel à ce type d'attaques, ou étant impliquées de toute autre manière dans celles-ci[1]. Si la teneur de ces sanctions n'est pas encore établie de façon claire, elles pourraient par exemple se matérialiser sous la forme d'interdiction de voyager ou de gels d'avoirs pour les cyberattaquants. Elles viennent néanmoins se heurter à la même problématique que les outils précédents, soit la nécessité d'un consensus parfois impossible entre États membres pour déterminer les responsables de la cyberattaque incriminée.

Bien que l'UE développe à la fois une stratégie et des outils de cyberdéfense, ceux-ci se heurtent à la volonté et aux priorités stratégiques – souvent divergentes – des États membres. Dès lors, l'UE est-elle capable d'incarner une forme de puissance dans le cyberespace ?

1. Conseil européen – Conseil de l'Union européenne, « La cybersécurité en Europe : des règles plus strictes et une meilleure protection », en ligne sur *consilium.europa.eu*.

La cyberdéfense européenne : quelle forme de puissance ?

L'UE tend à développer divers attributs de la puissance. Sa Stratégie globale de sécurité, publiée en juin 2016, en offre quelques pistes. Si l'Union n'est pas une puissance coercitive en devenir, elle semble néanmoins vouloir aller au-delà du seul *normative power* visant à modeler l'environnement international par l'influence de ses normes[1]. À cet égard, le concept de cyberpuissance est défini par Joseph Nye comme « la capacité à créer l'avantage à influencer les événements dans d'autres environnements opérationnels et à travers les instruments de la puissance »[2]. Cette capacité passe à la fois par des instruments physiques et des moyens d'information, qui peuvent être utilisés autant à l'intérieur qu'à l'extérieur du cyberespace. Pour Alexander Klimburg, la cyberpuissance s'appuie sur trois dimensions : la capacité à coordonner les aspects politiques et opérationnels de la cybersécurité à travers des structures gouvernementales ; la cohérence de la politique de cybersécurité au sein des alliances internationales et des cadres juridiques ; et la coopération entre les différents acteurs étatiques et non étatiques[3]. Si l'on tente d'appliquer ces définitions au cas de l'UE, force est de constater qu'elle développe bien des outils et des éléments stratégiques visant à influencer les comportements dans le cyberespace et à projeter ses normes[4], mais demeure loin d'une réelle projection de puissance, tant sont encore nombreuses les limites matérielles et stratégiques à son action en matière de cyberdéfense. Comme le soulignent Alexander Klimburg et Heli Tiirmaa-Laar, il manque pour l'heure à l'UE un concept permettant de projeter aussi bien une puissance coercitive (*hard power*) qu'une puissance d'influence (*soft power*) à travers une approche intégrée du cyberespace, qui lui donnerait pourtant l'opportunité de contribuer à définir

L'**Union** semble vouloir aller **au-delà** du seul ***normative power***

1. Voir sur cette question Bastien Nivet et Delphine Deschaux-Dutard, « L'Union européenne et ses dépenses militaires : mise en danger ou *hyper soft power* ? », *La Revue internationale et stratégique*, n° 96, IRIS Éditions – Armand Colin, hiver 2014.
2. Traduction de l'auteur. Joseph Nye, « Cyber Power », Belfer Center for Science and International Relations, Harvard Kennedy School, mai 2010, p. 4.
3. Alexander Klimburg, « Ruling the Domain: (Self) Regulation and the Security of the Internet », 11th Meeting of the ICANN Studienkreis, Budapest, 28-29 avril 2011.
4. Le Règlement général sur la protection des données (RGPD) adopté par le Parlement européen en avril 2016 et entré en vigueur le 25 mai 2018 peut d'ailleurs être lui aussi perçu comme une façon pour l'UE de promouvoir dans le cyberespace les standards européens de protection des données, même si la large marge de manœuvre laissée aux États et aux différents acteurs dans l'application de cette certification peut en limiter l'efficacité.

ce nouvel espace de conflictualité en y projetant ses valeurs fondamentales[1]. Même la nouvelle capacité à prononcer des sanctions européennes afin de prévenir ou condamner une cyberattaque relève davantage de la puissance symbolique que d'une réelle capacité à modeler le cyberespace en fonction des préférences de l'UE, tant la souveraineté demeure le maître-mot des États membres en matière de cyberdéfense[2].

Cyberdéfense européenne et divergences stratégiques entre États

En effet, les États européens tendent à diverger aussi bien dans leur perception de la cybermenace que dans l'acception de l'autonomie stratégique européenne prise plus largement. Plus précisément, concernant la construction de capacités de cyberdéfense, trois groupes d'États se dégagent[3]. Le premier se compose des États qui investissent le plus dans la cyberdéfense au niveau national et ont mis en place des commandements militaires cyber en vue de disposer de l'ensemble du spectre des instruments permettant de prévenir et de répondre à des cyberattaques ayant des implications militaires. Il s'agit essentiellement des pays qui ont joué historiquement un rôle moteur dans la politique européenne de défense : la France, le Royaume-Uni et l'Allemagne. Tous trois se sont dotés de stratégies nationales de cyberdéfense ainsi que d'institutions dédiées. La France, par exemple, dispose de deux commandements cyber, dont le dernier créé à Rennes en octobre 2019. Un deuxième groupe d'États compte les pays nordiques – Suède, Finlande, pays baltes –, qui se concentrent, pour l'heure,

Les **États européens** tendent à diverger aussi bien dans leur **perception** de la cybermenace que dans l'**acception** de l'**autonomie stratégique** européenne

1. Alexander Klimburg et Heli Tirmaa-Klaar, « Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU », Parlement européen, 15 avril 2011. Voir aussi Myriam Dunn Cavelty, « Europe's cyber-power », *European Politics and Society*, vol. 19, n° 3, 2018.
2. Voir Bastien Nivet, « Les sanctions internationales de l'Union européenne : *soft power*, *hard power* ou puissance symbolique ? », *La Revue internationale et stratégique*, n° 97, IRIS Éditions – Armand Colin, printemps 2015.
3. Voir George Christou, *Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy*, Londres, Palgrave Macmillan, 2016.

davantage sur leurs stratégies de sécurité et ont décidé de se reposer sur les capacités de cyberdéfense développées par l'OTAN. Enfin, les autres États européens, soit la majorité d'entre eux, constituent un troisième groupe plus en retard en matière de cybersécurité et de cyberdéfense. L'investissement des membres de l'UE dans le domaine cyber reste ainsi très contrasté, et se traduit par une absence de consensus sur l'idée d'accroître le rôle de l'UE dans ce domaine[1].

À ces divisions entre États membres s'ajoute une fragmentation institutionnelle en matière de cyberdéfense : si la cybersécurité relève largement d'une gouvernance conçue sous la forme d'un partage des tâches entre la Commission européenne, l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA, basée à Héraklion), les États et les acteurs privés, la cyberdéfense demeure majoritairement l'apanage des gouvernements nationaux, même si l'Agence européenne de défense (AED) et l'État-major de l'UE y dédient certains de leurs personnels[2]. À cela s'ajoute l'existence d'une politique de cyberdéfense substantielle développée par l'OTAN.

L'Union européenne, l'OTAN et la cyberdéfense : complémentarité ou rivalité ?

Si l'un des leitmotivs des institutions bruxelloises est d'éviter les duplications inutiles avec l'OTAN, les deux organisations tendent à poursuivre des activités similaires dans le cyberespace, bien que fondées sur des présupposés différents puisqu'elles ne sont pas de même nature : l'UE est une organisation internationale dotée d'un projet politique structurant, tandis que l'OTAN est une alliance militaire. L' Alliance atlantique constitue, par ailleurs, l'organisation internationale la plus avancée en matière de cyberdéfense. Dotée d'une structure de commandement cyber dès 2008, son concept stratégique de 2010 lui a permis de poser les bases de sa vision en matière de cyberdéfense : l'OTAN considérant les cybermenaces comme une forme de menace directe sur la sécurité transatlantique, elle a ainsi intégré la cyberdéfense à sa mission de défense collective de ses membres en 2014. Elle s'est aussi équipée d'outils et de services visant à prévenir et répondre aux cyberattaques dirigées contre ses infrastructures employées dans le cadre des opérations militaires otaniennes. L'OTAN conçoit également son rôle en matière de cyberdéfense de façon beaucoup plus proactive que ne le fait l'UE, qui se présente plutôt comme un facilitateur de communication entre ses membres. Les deux organisations ont, en outre, mis en place des cyberexercices communs et, au cours des dernières

1. Ce manque de consensus existe aussi dans une certaine mesure au sein de l'OTAN. Voir Vincent Joubert et Jean-Loup Samaan, *op. cit*.

2. Voir Jaap de Hoop Scheffer, Lorenzo Pupillo, Melissa Griffith, Steven Blockmans et Andrea Renda, *Strengthening the EU's Cyber Defence Capabilities. Report of a CEPS Task Force*, Bruxelles, CEPS, novembre 2018, p. 36.

années, fait plusieurs déclarations conjointes visant à faciliter l'échange d'informations et de pratiques dans le domaine cybernétique. Dès lors, comment l'UE peut-elle parvenir à développer sa propre forme de cyberdéfense et, plus largement, se concevoir comme une cyberpuissance quand la majorité de ses États membres, également membres de l'OTAN, ne peuvent envisager de dépenser des budgets contraints pour les deux organisations et préfèrent donc miser, pour une large part, sur les infrastructures de cyberdéfense de l'Alliance atlantique ?

Quelle cyberpuissance pour l'UE ?

Si l'Union européenne veut devenir un acteur international reconnu dans le cyberespace et faire face aux risques de cyberguerre, tout en restant fidèle à son approche traditionnellement non coercitive et collaborative de la sécurité internationale, elle doit se poser la question de savoir quel type de cyberpuissance elle souhaite développer, dans la mesure où les États ont, depuis une décennie, largement inscrit le cyberespace dans leurs priorités stratégiques. Dès lors, si l'UE aspire à une autonomie stratégique, il semble important qu'elle continue de se doter d'outils propres – comme les sanctions – lui permettant de prévenir les cyberattaques et d'influencer les comportements de potentiels cyberagresseurs. Mais en l'absence d'une politique étrangère européenne cohérente et d'une politique européenne de défense plus substantielle, il semble difficile d'aller plus loin qu'un rôle de facilitateur en matière de cyberdéfense. Certains auteurs plaident en faveur d'une forme de *cyber soft power* pour l'UE, construit autour de la notion de résilience[1], qui ne contredit pas pour autant l'ambition de développer ses propres capacités de cyberdéfense[2]. En revanche, serait-il opportun pour l'UE, qui se définit comme un acteur promouvant la paix sur la scène internationale, de créer des armes cyber offensives, comme le font de nombreux États-nations, créant davantage de vulnérabilité dans un cyberespace déjà largement marqué par la course aux

Si l'**UE** aspire à une **autonomie stratégique**, il semble important qu'elle continue de se **doter** d'**outils propres**

1. Voir notamment Myriam Dunn Cavelty, *op. cit.*, 2018 ; et Annegret Bendiek, « The EU as a Force for Peace in International Cyber Diplomacy », *SWP Comments*, German Institute for International and Security Affairs, avril 2018.
2. Voir Wolfgang Röhrig et Rob Smeaton, « Cyber Security and Cyber Defence in the European Union. Opportunities, Synergies and Challenges », *Cybersecurity Review*, été 2014.

armements ? La question rejoint, au fond, celle du projet européen lui-même. Dans un monde où le multilatéralisme est de plus en plus remis en cause par l'action unilatérale des grands États, la plus-value de l'UE n'est-elle pas la force de son projet politique et des habitudes de communication entre États qu'elle a instaurées ? Ainsi devrait-elle miser sur un *cyber smart power* combinant des outils cyberdiplomatiques qui lui permettent de diffuser ses normes, tout en se dotant d'une architecture légère mais cohérente de cyberdéfense, sans redondance avec celle de l'OTAN, lui permettant de se prémunir contre les cyberconflits. Une cohérence qui reste encore à trouver. ■