note n°01/18

22 janvier 2018

**Nicolas Mazzucchi**
Chargé de recherche, Fondation pour la recherche stratégique

FONDATION pour la RECHERCHE STRATÉGIQUE

# 2018, année charnière pour l'Europe dans le cyber ?

Le discours sur l'état de l'Union européenne du Président Juncker à l'automne 2017 a mis, entre autres, l'accent sur la cybersécurité comme priorité de travail, pour la Commission aussi bien que pour l'ensemble des institutions européennes. 2018 s'annonce comme une année potentiellement charnière en matière de cybersécurité à l'échelle de l'Union. L'entrée en vigueur des règlementations clés dans le domaine de la gestion des données (Règlement général sur la protection des données, directive SRI) est une avancée essentielle dans l'harmonisation des législations sur le territoire de l'Union. En outre, l'UE est confrontée à de nombreux défis, en matière de sécurité comme d'appropriation de nouvelles technologies, ouvrant potentiellement de nouvelles failles. L'intelligence artificielle et le bitcoin, pour n'en citer que deux, représentent un défi pour le législateur européen qui se voit confronté à la nécessité d'une part d'en définir les contours juridiques et, d'autre part, de les réguler.

Toutefois cette bascule est grandement conditionnée par le vote, cette année, par le Parlement du « paquet cyber » proposé à l'automne 2017 par la Commission. Ce train de réformes qui a été approuvé par le Conseil en octobre 2017, doit encore passer à travers l'étape politique la plus complexe, celle de la représentation des citoyens, où les particularismes nationaux risquent d'être difficiles à contourner. 2018 est ainsi l'année du choix entre le renforcement des compétences de l'Union par transfert de prérogatives nationales et l'amplification du fossé entre États-membres.

## La protection des données, un enjeu de longue date

### L'entrée en vigueur du RGPD

La principale avancée européenne dans le cyberespace en ce début d'année 2018 est l'entrée en vigueur du Règlement général sur la protection des données (RGPD), prévue pour mai. Il s'agit d'une évolution majeure de l'UE sur la question de la gestion des données personnelles des citoyens de l'Union qui vient couronner les travaux menés dans de nombreuses instances, comme le G29[1], sur ces sujets. Le RGPD est une évolution majeure par rapport à la directive sur la protection des données personnelles de 1995, prenant notamment en compte les nombreuses évolutions technologiques survenues – et se profilant – dans le cyberespace.

Le RGPD se veut notamment – c'est une première dans ce domaine – un texte d'application extraterritoriale, à l'image des effets que le droit américain peut parfois produire. Il instaure ainsi des obligations pour les entités effectuant le traitement de données personnelles des citoyens européens que celles-ci soient ou non sur le territoire de l'Union. Il appartiendra d'en apprécier au cours du temps les effets réels, mais c'est une première importante dans la volonté d'une sanctuarisation d'un espace cyber européen, à l'image de ce que font d'autres pays[2]. Le RGPD est, dans sa forme, compatible avec les obligations nées de la signature d'une coopération UE-États-Unis sur le transfert des données (dite *Privacy Shield*) ce qui limite toutefois l'aspect « souverain » du règlement[3]. La coopération européenne est également renforcée avec la création d'un Comité européen de protection des données (CEPD) qui vise à se substituer à terme au G29, plus proche d'un forum de partage de bonnes pratiques que d'une véritable instance de coordination. Les données elles-mêmes devront être les plus sécurisées possibles chez les responsables de traitement, notamment par la mise en œuvre des technologies dites *privacy by design* qui sont censées inclure des systèmes de protection contre l'identification au sein du système lui-même[4].

Ces avancées sont à la fois très importantes et mineures selon les pays et les cas rencontrés. La France par exemple, au travers de la Loi Informatique et Liberté de 1978 et des diverses règlementations sur les systèmes de traitement automatisés de données, appliquait déjà le principe de la discrimination et le droit de ne pas faire uniquement l'objet d'un traitement automatisé. De même, l'obligation d'information des personnes était déjà contenue dans la directive européenne de 1995, avec une application plus limitée certes[5].

Certaines des dispositions contenues dans le RGPD demeurent assez floues, surtout quant aux effets juridiques qu'elles créent. L'obligation d'information des personnes, afin de recueillir leur consentement, est renforcée mais il n'est pas fait mention du moment où cette information doit être faite, *a priori* ou *a posteriori*. Identiquement, le retrait du consentement n'étant pas rétroactif, le traitement qui avait été appliqué aux données personnelles est conservé, limitant par là le caractère de possession absolue de celles-ci. Le consentement des personnes est ainsi limité par certaines barrières juridiquement floues, comme « *la conservation des données [...] à des fins archivistiques dans l'intérêt du public* » (article 17). Dans ce cas un moteur de recherche, ayant collecté des données personnelles auprès de tiers, pourrait légitimement refuser l'effacement de celles-ci de ses résultats pour ce motif. Certes cela tendrait vers une tyrannie de la transparence, mais l'argument est *a priori* recevable.

Autre point sensible, la question de la sécurité (article 32) qui implique notamment de recourir à la pseudonymisation des données. Or une telle technique a depuis longtemps atteint ses limites et il est maintenant extrêmement facile de reconstituer l'identité d'une personne à l'aide de quelques données structurées[6]. Le *privacy by design* adopté doit donc, pour être efficace, être bien plus contraignant que la seule pseudonymisation ; l'article 25 du RGPD demeurant assez flou sur ce sujet

1. Le G29 est le groupe réunissant *ad hoc* les autorités de protection de la vie privée des États-membres de l'UE ; la CNIL en est le représentant pour la France et en assure en ce moment la présidence.

2. Certains comme la Russie ou la Chine imposent que les données des citoyens soient stockées de manière exclusive sur leur territoire national et ne puissent en sortir.

3. Les données transférées aux Etats-Unis au titre du *Privacy Shield* tombent, *de facto*, sous le coup des lois américaines dont le Patriot Act ou le Foreign Intelligence Surveillance Amendements Act of 2008.

4. https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels

5. M. Boizard (2017), « Protection des algorithmes et sécurité des personnes », *Allocution prononcée lors de la conférence WISG 2017*, Paris, 15 septembre 2017.

6. Y.-A. de Montjoye (2017), « Computational Privacy : Pouvons-nous encore protéger la vie privée à l'ère du Big Data ? », *Allocution prononcée lors de la conférence WISG 2017*, Paris, 15 septembre 2017.

pourtant technologiquement précis[7]. La cybersécurité des systèmes de traitement automatisés de données – et des objets cyber dans leur ensemble – est pourtant l'un des principaux axes d'effort de l'UE depuis quelques années.

### Les obligations de la directive SRI

Au-delà du RGPD, le principal événement réglementaire de cette année au niveau du cyberespace sera la fin du délai octroyé aux Etats-membres européens pour transposer en droit local la directive SRI (Systèmes et réseaux d'information ou NIS en anglais pour *network and information systems*). Celle-ci prévoit un renforcement drastique des mesures de cybersécurité au niveau de l'ensemble de l'Union, en harmonisant les pratiques autour de la protection des opérateurs d'importance vitale (OIV). Outre la question des OIV, la directive SRI s'intéresse également aux fournisseurs d'accès et de services numériques (au sein desquels les moteurs de recherche comme Google) qui sont également astreints à des efforts en matière de cybersécurité ainsi que de déclaration des incidents. Toutefois les fournisseurs de services sont assez limités puisque ne figurent pas, par exemple, les réseaux sociaux, lesquels ont une importance dans le cyberespace proche de celle des moteurs de recherche ou des places de marché en ligne type Amazon ou Alibaba.

La directive SRI pose un certain nombre de questions, voire de problèmes, dans les pays n'ayant pas fait le choix d'un investissement massif en termes de cybersécurité, notamment des OIV. En renforçant les devoirs des autorités nationales sur les questions de gestion de crise (au travers des CSIRT (*Computer Security Incident Response Team*), descendants des CERT (*Computer Emergency Response Team*)) et de protection en amont, l'UE oblige d'une certaine manière tous les États-membres à se mettre au même niveau. Pour un pays comme la France, l'ANSSI (Agence nationale de la sécurité des systèmes d'information) et le CERT-FR représentent déjà des outils matures, mais pour des pays plus petits et moins bien dotés[8], il s'agit d'une évolution majeure ; d'où les deux années laissées pour la transposition de la directive.

L'interconnexion de plus en plus poussée d'un certain nombre de secteurs au niveau européen, bancaire bien sûr, mais également énergie, télécommunications, etc. crée *de facto* une chaîne qui n'est forte qu'autant que le plus faible de ses maillons. La face sombre de la construction européenne apparaît ici nettement, avec un différentiel de prise en compte et de compétences selon les pays qui peut s'avérer dramatique en termes de conséquence en cas de réaction en cascade. C'est en creux ce qui ressort du *memorandum* de la Commission européenne du 13 septembre 2017 sensibilisant le Parlement sur la nécessité de voter un paquet cybersécurité rassemblant diverses compétences au niveau de l'Union[9].

## Les avancées en matière de cybersécurité et de cyberdéfense

### L'évolution de l'ENISA, vers un consensus ?

La Commission européenne a proposé au Parlement et au Conseil un paquet dit « Cybersecurity Act » qui devrait être examiné au cours de l'année 2018 visant à approfondir le rôle de l'ENISA et ses pouvoirs. A la suite du discours de J.-C. Junker sur l'état de l'Union, la Commission s'est saisie du dossier de la cybersécurité qui, au regard des ambitions sur la protection des données susmentionnées, ainsi que sur la réalisation du marché numérique unique (DSM pour *digital single market*), s'avère fondamental. L'évolution ces dernières années de l'ENISA a suivi la prise en compte du caractère de plus en plus dangereux et complexe des cyberattaques, aussi bien que de la profonde dichotomie existant entre les États-membres sur les questions de cybersécurité.

L'Agence européenne chargée de la sécurité des réseaux et de l'information a vu le jour en 2004 et elle est depuis demeurée un organisme assez discret de l'UE, se contentant de jouer le rôle d'un centre de coordination pour les différentes initiatives nationales – quand celles-ci ne la contournaient pas – et de développement des compétences techniques. De fait l'ENISA, agence au financement faible (€ 11,2 millions de budget en 2017) et aux ressources humaines limitées (moins de 80

7. Il mentionne « *l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques* » comme déterminants du niveau de protection.

8. L'ENISA (Agence européenne chargée de la sécurité des réseaux et de l'information) qui recense l'existence des doctrines cyber nationales sur l'ensemble de la planète, montre qu'une bonne partie de celles des pays de l'UE n'ont été adoptées que depuis 2015.

9. Commission européenne (2017), *Proposition de règlementation du Parlement et du Conseil sur l'ENISA, l'« agence de cybersécurité de l'Union européenne » et abrogeant la règlementation EU 526/2013 « Cybersecurity Act »*, Bruxelles, UE.

personnes), n'est pas en l'état en mesure de prendre le rôle que voudrait lui confier la Commission, à savoir une véritable agence de cybersécurité. Les avancées susmentionnées, notamment la directive SRI imposent néanmoins une coopération renforcée au niveau communautaire tendant vers la plus grande harmonisation possible.

En attendant de voir quelle va être l'évolution de l'ENISA au cours de cette année, son programme de travail repose maintenant sur 3 piliers : le conseil & formation, la coopération et l'assistance technique. C'est dans ce dernier domaine que les évolutions de l'ENISA seraient les plus importantes et c'est d'ailleurs sur ce point que les réticences sont les plus fortes de la part de certains États-membres, eu égard aux différences entre eux.

Les pays européens sont en effet divisés entre plusieurs groupes, selon leur maturité technico-règlementaire sur ce sujet, avec un petit groupe de pays (France et Allemagne en particulier) en pointe dans le domaine. La principale évolution mise en doute par ces pays, est celle concernant la volonté de faire de l'ENISA le certificateur unique en termes de cybersécurité au niveau européen. Cette orientation qui s'appuie sur la disparité des pratiques et des exigences au sein de l'Union, inquiète grandement les pays les plus avancés – donc les plus exigeants – qui se verraient *de facto* dans l'impossibilité de refuser sur leur sol des produits certifiés par l'ENISA, même si ceux-ci leur paraissent insuffisamment protégés. Cet enjeu de la certification tend à devenir de plus en plus critique, avec l'explosion programmée du marché des objets connectés[10]. La différence d'approche des pays européens vis-à-vis du principal accord international de certification – le CCRA, Common Criteria Recognition Agreement – est en elle-même révélatrice de cette dichotomie. Alors que cet accord regroupe au niveau mondial 28 pays dont l'Ethiopie et le Qatar, seuls 7 pays européens en sont pleinement partie et 6 autres le reconnaissent.

Il ressort donc une crainte sur la question de la certification unique, celle de voir une harmonisation des exigences européennes par le bas. Les pays les plus avancés dans ce domaine, à commencer par la France qui ne souhaite pas perdre le contrôle qu'elle exerce *via* l'ANSSI en ce domaine, s'opposent à une centralisation de la certification au niveau de l'ENISA. L'opposition à cette évolution se lit à plusieurs niveaux en France qu'il s'agisse des entreprises spécialisées dans le domaine de la cybersécurité qui déplorent un alignement probable par le bas[11], aux députés de la commission des Affaires étrangères, auteurs d'un rapport sur les enjeux du marché numérique unique[12] [13]. La question, très sensible, de la certification des produits en termes de cybersécurité a fait l'objet de nombreux débats politiques – par exemple le rapport Bockel de 2012 qui pointait directement les routeurs cœur de réseau chinois comme dangereux – et s'inscrit dans le cadre plus global d'une faiblesse des BITC européennes. La certification cherche ainsi à répondre, de manière trop limitée certes, au retard industriel européen dans le domaine des produits cyber puisqu'elle constitue une forme de contrôle *a posteriori* de leur efficacité.

L'évolution potentielle de l'ENISA doit être considérée différemment d'autres orientations européennes comme la directive SRI par exemple. Cette dernière tend à responsabiliser les pays-membres sur la question des OIV en leur donnant, d'une certaine manière, les moyens juridiques pour un contrôle accru des opérateurs. Si des États comme la France, au travers de l'ANSSI, avaient depuis longtemps mis ces préceptes en application, une harmonisation était nécessaire. Toutefois l'évolution proposée de l'ENISA, sur le volet certification du moins, touche d'assez près à la souveraineté nationale d'un domaine qui est, par essence, dual, surtout dans un contexte stratégique qui impose de traiter également de nouvelles menaces.

### *Fake news* et guerre hybride, un nouveau front

L'une des grandes évolutions dans la prise en compte des menaces ces dernières années, a été la focalisation sur les actions de désinformation. Apparue il y a des années sous la plume du chef d'état-major des armées russes, le général V. Gerasimov, la notion de « guerre

10. Selon Gartner il y avait 8,4 milliards d'objets connectés en 2017 dans le monde et le chiffre avancé pour 2020 se monte à plus de 20 milliards.

11. https://sd-magazine.com/securite-numerique-cybersecurite/cyber-act-european-oui-a-nimporte-condition

12. E. Bothorel, C. Le Grip (2017), *Rapport d'information sur le marché unique du numérique,* Paris, Commission des Affaires étrangères de l'Assemblée nationale.

13. En Allemagne la position est plus nuancée, toutefois le numéro de fin d'année dernière de *BSI Magazine* (2017/2), édité par l'autorité allemande de cybersécurité, met l'accent sur des éléments tels que « *la préservation de la souveraineté dans le cyberespace* » et « *le savoir-faire national en matière de certification* ».

hybride » a, depuis 2014, fait florès au sein des gouvernements et des états-majors occidentaux. Considérée par certains comme une nouvelle approche du fait militaire, elle n'est au fond que la réaffirmation de la combinaison des moyens cinétiques et non-cinétiques au service d'une action globale. Dans ce cadre, la Russie qui a maintenu depuis le siècle précédent un savoir-faire certain quant aux actions dites informationnelles, dispose d'une compétence qui inquiète tant les dirigeants nationaux que les instances européennes. Malgré l'emploi du terme, il ne semble donc pas qu'il faille considérer cette forme de conflictualité ni comme une nouveauté, ni comme une révolution malgré des évolutions certaines[14].

Des accusations se sont multipliées pour dénoncer le rôle, supposé, de tel ou tel dans la manipulation des opinions lors de grands rendez-vous démocratiques ; en Europe principalement le vote sur le *Brexit* ou l'élection présidentielle française. Si dans le mode opératoire les *Macronleaks* de 2017 diffèrent assez peu du *Climategate* de 2009[15] – notamment par une combinaison d'action d'espionnage pour dérober les mails et de subversion pour diffuser certains contenus –, la perception de la menace sous-jacente n'est plus du tout la même. De cette crainte généralisée est née la prise en compte, y compris par les instances communautaires, de lutter contre le double phénomène de la « guerre hybride » (promue par un acteur étatique) et des « *fake news* » (dont les auteurs peuvent appartenir à différentes sphères). Il s'agit dans ces deux cas – guerre dite hybride et *fake news* - d'un phénomène cyber touchant avant tout à la couche sémantique du cyberespace. La mise en forme et la diffusion par des canaux appropriés d'informations destinées à tromper l'adversaire ou modifier son comportement, sont avant tout de la désinformation, au sens militaire du mot. Il s'agit donc d'agir tant sur le message lui-même que sur le *medium* et sur les opinions visées, afin de contrer la menace.

L'Union européenne s'est ainsi engagée dans la mise en place d'outils et de pôles de réflexion pour disposer d'une stratégie et de moyens d'actions pour contrer ces deux phénomènes. Le renforcement du rôle de l'ENISA comme « agence de cybersécurité européenne » est censé prendre en compte ces problématiques, notamment sur les volets formation et conseil ainsi que coopération transnationale. En effet l'harmonisation d'un niveau basique de cybersécurité au sein de l'ensemble du territoire de l'Union, amènerait mécaniquement à une augmentation de la résilience vis-à-vis de ces phénomènes, pour autant que ce niveau soit suffisamment élevé.

Concernant le problème spécifique des *fake news*, le groupe d'experts mis en place au sein de la Commission fin 2017 devrait livrer ses premières recommandations au premier semestre 2018. La problématique incriminée qui est de nature complexe — à cause de la nature même du cyberespace, mondialement interconnecté –, devrait donner lieu à plusieurs approches vis-à-vis des contenus aussi bien que des contenants. La prise en compte de cette question des *fake news* ne peut ainsi se décoreller de la cybersécurité elle-même, dans le sens où les couches logicielle et sémantique, voire matérielle selon les cas, sont concernées. Toutefois la directive SRI qui pourrait avoir un certain impact, notamment sur l'aspect « intrusion/vol de données », est limitée à des catégories d'acteurs n'incluant, malheureusement pas, les réseaux sociaux et *media* en ligne.

Opportunément, la Finlande, membre de l'UE mais hors de l'OTAN, a décidé de créer un centre d'excellence européen, sur le modèle des centres d'excellence de l'OTAN, dédié à la lutte contre la guerre hybride[16]. La création de celui-ci se fonde sur une déclaration conjointe le 8 juillet 2016 du Secrétaire général de l'OTAN, du Président du Conseil européen et du Président de la Commission européenne, sur la nécessité de coopérer dans la lutte contre les menaces hybrides. Le centre qui a été officiellement ouvert le 1er septembre 2017 a, très rapidement, organisé des évènements conjoints UE-OTAN afin d'harmoniser les définitions et les pratiques des deux organisations. Si l'UE et l'OTAN ne sont pas membres officiellement du centre d'Helsinki[17], c'est bien autour de leur coopération renforcée que se définit l'essentiel de son activité. Ce centre

14. E. Tenenbaum (2015), *Le piège de la guerre hybride,* Focus stratégique n° 63, Paris, IFRI.

15. Celui-ci avait consisté dans le vol et la diffusion de courriels sélectionnés de scientifiques anglais membres du GIEC (Groupe d'experts intergouvernemental sur l'évolution du climat), censés prouver que le consensus sur le changement climatique n'existait pas et, *in fine,* que le GIEC manipulait les opinions ; voir F.-B. Huyghe, O. Kempf, N. Mazzucchi (2015), *Gagner les cyberconflits,* Paris, Economica.

16. https://www.hybridcoe.fi/

17. Les membres, au titre du Memorandum of Understanding organisant le centre, sont : l'Allemagne, l'Espagne, l'Estonie, les États-Unis, la Finlande, la France, la Lettonie, la Lituanie, la Norvège, la Pologne, le Royaume-Uni et la Suède ; tous membres de l'UE et de l'OTAN sauf la Finlande et la Suède.

qui n'est pas à proprement parler une initiative européenne, doit néanmoins être inclus dans le périmètre des actions menées par l'Union, notamment au titre de sa montée en puissance au cours de l'année 2018. Au-delà de cette initiative soutenue par l'UE, l'approche des questions cyber au sein de la PSDC (politique de sécurité et de défense commune) est en pleine évolution depuis quelques années.

### Cyber et PSDC

Les questions cyber sont en effet très présentes au sein de la politique de sécurité et de défense commune, d'autant plus avec la perception croissante par certains pays d'une menace grandissante sur le flanc Est. Le document d'évaluation de la mise en œuvre de la Stratégie générale de l'UE au titre de l'année 2017 pointe d'ailleurs la nécessité d'une remise à niveau de la vision stratégique de l'UE en termes de cyberdéfense[18]. Il s'agit là d'un chantier qui doit s'ouvrir en 2018 pour renforcer la cohérence, laquelle est centrale dans la performance de l'UE comme acteur de sécurité et de défense[19].

Au cœur de cette orientation, le renforcement de la coopération UE-OTAN est mis en avant par de nombreux analystes et acteurs européens suite à la déclaration commune de juillet 2016. Le centre d'Helsinki représente un premier pas important dans ce sens, d'autant plus que l'UE ne dispose pas en propre pour le moment d'une doctrine de cyberdéfense régionale[20]. La plupart des États européens membres de l'OTAN ont adopté la première version du Manuel de Tallinn, édité par le centre d'expertise OTAN sur le cyber (CCD-COE). Le Manuel qui est en version 2.0 depuis 2017[21], n'est toutefois pas un document contraignant juridiquement puisqu'issu d'un centre d'excellence et s'apparente plus à un guide commun de pratiques qu'à une véritable doctrine[22]. 2018 s'annonce, dans ce domaine également comme une année importante, car le renforcement des liens dans le cyberespace entre l'UE et l'OTAN passe avant tout par des exercices communs et un partage d'expériences[23] que les évolutions de l'UE sur le sujet peuvent rendre possible cette année.

Cette question du cyber au niveau communautaire est d'autant plus complexe qu'elle revient à mutualiser les faiblesses plutôt que les forces[24]. De la part des pays les plus avancés dans le domaine de la cyberdéfense, cette situation est d'autant plus délicate qu'elle est un frein à une intégration plus poussée des réseaux européens dans le domaine de la défense. Prenant cet aspect en compte, l'Agence européenne de défense met en œuvre non seulement une coordination dans le domaine technologique vis-à-vis des technologies de l'information et de la communication, mais elle est également active sur la formation et la montée en compétences (*capacity building*) des forces armées européennes. Il s'agit ainsi de disposer dans chaque État-membre d'une masse critique d'experts, aptes à mettre en œuvre des protocoles dans le domaine de la cyberdéfense, en regard des exigences de la Stratégie générale de l'UE définie en 2016. L'écart entre les pays est ici également très important, avec des évolutions technologiques prévisibles qui vont encore accroître les compétences demandées et les menaces potentielles.

## L'Europe face aux nouveaux enjeux

### Bitcoin et *blockchain*, intérêt ou piège ?

Les cryptomonnaies virtuelles dont l'engouement ne se dément pas, tendent à prendre une place de plus en plus importante au sein des sociétés très connectées comme celles des pays européens. Les déclarations politiques au sujet des cryptomonnaies se sont multipliées ces derniers mois, de la part de responsables nationaux ou communautaires. Il est important de rappeler à ce titre que ces cryptomonnaies ne sont pas, en termes juridiques, des monnaies et ne peuvent le devenir[25]. L'absence d'harmonisation dans l'approche des différents pays-membres – l'Allemagne reconnaissant le bitcoin comme une

18. https://europa.eu/globalstrategy/sites/globalstrategy/files/full_brochure_fr.pdf

19. H. Carrapico, A. Barrinha (2017), « The EU as a Coherent (Cyber)Security Actor? », *Journal of Common Market Studies*, Vol. 55, n° 6 , pp. 1254–1272.

20. L'OTAN peine également sur cette question, les différents sommets (Newport, Varsovie) apportant des avancées mineures.

21. M. Schmitt (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge, Cambridge University Press.

22. Il est également important de noter que la quasi-totalité des experts ayant rédigé ce manuel sont issus du monde anglo-saxon.

23. B. Lete, P. Pernik (2017), *EU–NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions*, GMF Policy brief 2017/38, Washington, German Marshall Fund.

24. O. Kempf (2014), *Alliances et mésalliances dans le cyberespace*, Paris, Economica.

25. M. Roussille (2015), « Le *bitcoin* : objet juridique non identifié », *Banque & Droit* n° 159, janvier-février 2015, pp. 27-31.

« monnaie privée » au contraire de la France par exemple – ne pose ainsi pas de problème insurmontable. La Banque centrale européenne affirme cependant depuis 2012 que le statut juridique du bitcoin est particulièrement flou. Pire encore, l'anonymat des transactions et le système lui-même du bitcoin (ou des autres cryptomonnaies) en fait un instrument particulièrement utilisé dans le contexte de la criminalité organisée ou du financement du terrorisme. A ce titre les autorités européennes se positionnent sur un créneau qui tient à la fois de la sécurité publique et de la protection économique du citoyen pour se positionner en faveur d'une règlementation contraignante. En 2014 l'Autorité bancaire européenne a ainsi rendu un avis demandant à la Commission d'adopter des règles particulières et, dans le même temps, dissuadant les pays-membres et leurs banques d'accepter les cryptomonnaies. Fin 2017, l'UE a annoncé – après un accord entre les États-membres et le Parlement - un plan de lutte contre le blanchiment d'argent lié au terrorisme, ciblant spécifiquement l'anonymat des transactions en cryptomonnaies[26]. Sa mise en œuvre au cours de l'année 2018 s'avère également un objet d'attention, notamment eu égard, ici encore à la nature transnationale du marché concerné et à la possibilité pour les acteurs malintentionnés de recourir à des prête-noms.

Au-delà des cryptomonnaies, la technologie de la *blockchain* intéresse également de nombreux acteurs européens comme des banques ou des compagnies d'assurances, mais l'absence pour le moment d'une véritable orientation de l'UE sur ces domaines pourrait en retarder le développement. La nécessité d'une analyse approfondie de la résilience de cette technologie en matière de cybersécurité – avec une vision commune – se heurte pour le moment à la limite des compétences de l'ENISA, en attendant sa transformation en agence de cybersécurité.

### L'IA, un objet cyber encore indéfini

L'Intelligence artificielle (IA), dont les technologies émergent rapidement de manière civile voire militaire, représente pour l'Union européenne un objet encore indéfini. Une proposition de résolution du Parlement de janvier 2017, se fondant sur un rapport de la commission des affaires juridiques[27], demande à la Commission de proposer une définition communautairement acceptée de l'IA et de la robotique autonome. La confusion entre IA et robotique qui demeure relativement courante, est néanmoins préoccupante eu égard aux différences entre ces deux technologies qui peuvent potentiellement se combiner selon les utilisations. La problématique de la définition juridique de l'intelligence artificielle – et les questions de droit et de responsabilité qui en découlent – se pose en ce moment à l'ensemble des pays européens. Les États-membres étant loin d'avoir adopté chacun une règlementation sur ce sujet, l'UE dispose ici d'une opportunité de poser un cadre en amont, réaffirmée dans la déclaration commune sur les priorités législatives de 2018-2019[28]. Toutefois, la transversalité des sujets couverts par l'IA impose une concertation qui s'annonce longue et doit se faire en lien avec les règlementations entrant en vigueur cette année (SRI, RGPD).

Ainsi l'intelligence artificielle repose sur la famille technologique de l'apprentissage dit *machine learning*. Ces technologies nécessitent ainsi que la machine puisse être entraînée, avec ou sans supervision, grâce à des ensembles de données. Or l'entrée en vigueur du RGPD ainsi que les obligations qui l'accompagnent ont un effet certain sur la possibilité d'utiliser des données aux fins d'entraînement d'IA. La réutilisation de données personnelles, au-delà de leur première finalité, pour du *machine learning* dans ce cas, est ainsi proscrite par l'article 5 du RGPD.

Le droit de refuser toute décision fondée sur un traitement automatique, constitue également une protection pour les citoyens, mais limite identiquement l'usage potentiel des IA dans plusieurs domaines, notamment de l'action publique, sauf dans ces cas définis (sécurité publique, défense nationale principalement). La problématique du cadre idoine – restrictif mais suffisamment incitatif – nécessaire au développement des technologies d'IA en Europe est pleinement ouverte. Les recherches menées dans de nombreux laboratoires publics et privés sur des blocs technologiques (reconnaissance des images, transcription du langage naturel, apprentissage autonome, etc.), sont pour l'Europe

26. https://www.latribune.fr/economie/union-europeenne/bitcoin-l-ue-veut-plus-de-transparence-pour-lutter-contre-le-blanchiment-761976.html

27. M. Delvaux (2017), *Rapport contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique (2015/2103(INL))*, Bruxelles, Parlement européen.

28. https://ec.europa.eu/luxembourg/news/une-union-plus-unie-plus-forte-et-plus-d%C3%A9mocratique-d%C3%A9claration-commune-sur-les-priorit%C3%A9s_fr

une opportunité de rattraper un retard certain dans le domaine des technologies de l'information et de la communication (TIC). Les organes de régulation de l'UE doivent ainsi se saisir rapidement de ce dossier pour être en mesure d'accompagner la recherche et le développement.

## Une question demeure : quelle base industrielle ?

Au-delà des aspects juridiques et organisationnels qui se mettent en place au début de cette année, une problématique importante demeure inexplorée, celle de la base industrielle et technologique cyber (BITC) européenne. A l'instar de la BITD (base industrielle et technologique de défense), la BITC est à la fois, au niveau de l'UE, un domaine souverain pour les États comme un enjeu communautaire, eu égard au montant des investissements nécessaires. Au-delà des règlementations sur l'IA ou la robotique, de nombreux domaines sont concernés dès à présent, en lien avec les obligations juridiques récentes.

Le cyber est un domaine technologique dual par essence et les investissements faits aux niveaux civil et militaire tendent à se recouper et à se compléter. Le modèle d'interaction public-privé américain, à l'origine du développement d'Internet à partir de l'Arpanet militaire initial, est loin d'être généralisé en Europe. De fait, l'UE en tant qu'organisation achoppe sur les modèles et les instruments de financement d'une éventuelle BITC. La création, annoncée en juin 2017, d'un Fonds européen de la défense s'intègre dans une volonté de développer de nouveaux outils permettant de renforcer la coopération industrielle de défense au niveau de l'Union. Celui-ci entend donner des capacités financières renforcées – surtout à partir de 2020 où il est censé atteindre € 5,5 milliards annuels – pour des projets sur l'ensemble du spectre des technologies de défense. La cyberdéfense étant l'une des 4 priorités de l'Agence européenne de défense, nul doute que le cyber est appelé à occuper une place majeure dans les financements.

L'évolution inattendue de la Coopération structurée permanente (CSP) en matière de défense, avec un nombre de pays bien supérieur (23) aux estimations originelles, peut se révéler un atout dans le cyber. Parmi les 17 projets collaboratifs identifiés fin 2017 pour la CSP, deux concernent directement le cyber (« Cyber Threats and Incident Response Information Sharing Platform » et « Cyber Rapid Response Teams and Mutual Assistance in Cyber Security ») et plusieurs autres incluent nécessairement un volet cyber (sur les systèmes semi-autonomes, le *command and control*, etc.)[29]. Toutefois, les décisions au sein de la CSP se prenant à l'unanimité, la mise en application de ces programmes risque d'être délicate à conduire. 2018 qui est la première année de mise en œuvre de la CSP s'avère, dans ce domaine également, une charnière importante, y compris sur les modalités de mise en œuvre.

Malgré ces deux nouveaux éléments – complétés par la Revue annuelle des capacités de défense – les budgets alloués demeurent très faibles au niveau européen. A titre de comparaison le budget de la R&D de défense aux États-Unis pour l'année fiscale 2018 est de près de 84 milliards USD, dont 3,2 milliards pour la seule DARPA. De fait le différentiel de puissance économique entre les principaux industriels en matière de cybersécurité et de cyberdéfense des deux côtés de l'Atlantique, demeure colossal. En comparant deux classements, d'une part le Cybersecurity 500 de Cybersecurity Ventures et, d'autre part, le BVP Cyber index de Bessemer Ventures Partners, il est aisé de se rendre compte de l'écart existant entre les firmes américaines et européennes. Sur les 25 premières entreprises du Cybersecurity 500[30], seules 3 sont européennes[31] ; concernant le BVP Cyber index[32], seul Gemalto – bientôt absorbé par Thales – représente le Vieux continent au sein des entreprises capitalisées à plus d'un milliard USD. L'émergence de leaders européens en matière de cybersécurité est en cours[33], mais ces derniers demeurent faibles par rapport à leurs homologues hors-UE, américains principalement. La volonté des autorités nationales et communautaires risque ainsi de se heurter à la réalité d'un marché dominé par des firmes extra-européennes ou leurs filiales implantées sur le continent[34].

29. http://www.consilium.europa.eu/media/32082/pesco-overview-of-first-collaborative-of-projects-for-press.pdf

30. https://cybersecurityventures.com/cybersecurity-500-list/#home/?view_1_per_page=500&view_1_page=1

31. EY ne pouvant être considérée comme une entreprise européenne malgré son siège londonien.

32. https://www.bvp.com/strategy/cyber-security/index

33. PWC (2017), *Cyber security: European emerging market leaders*, Londres, PWC UK.

34. Une analyse analogue peut être faite dans d'autres domaines comme l'Internet des Objets par exemple

## Conclusion

2018 s'annonce ainsi comme une année charnière dans le cyberespace pour l'Union européenne ; ce sera probablement celle qui amplifiera ou amoindrira les contradictions internes de l'Europe sur ces questions. La réforme du statut de l'ENISA qui se cristallise autour de la problématique de la certification des produits en matière de cybersécurité, laisse apparaître des enjeux identiques à ceux rencontrés dans d'autres secteurs. L'Europe, au travers du RGPD et de la directive SRI, a fortement avancé sur l'harmonisation juridique des règlementations et elle se trouve maintenant confrontée à la nécessité de compléter celles-ci par des transferts de compétence. Or le différentiel de volonté, de maturité et de finances entre les pays-membres menace de faire éclater une cohésion reposant sur un dénominateur commun évident, mais relativement petit. Le problème rencontré est ainsi comparable à celui sur la défense – le cyber étant de toute façon par essence un domaine dual – avec un point de bascule clairement identifié à partir duquel s'ouvrent deux voies difficilement conciliables. D'une part, un transfert des compétences vers le niveau communautaire au risque de noyer ou d'amoindrir les exigences à cause d'un différentiel de compétences et de volontés. D'autre part une Europe qui demeurerait à plusieurs vitesses avec des initiatives minilatérales menées par certains pays, à l'image de la coopération franco-allemande pour la certification des *clouds* (European Secure Cloud)[35]. Les premiers mois de 2018 seront sans doute décisifs sur ce point.◊

35. https://www.ssi.gouv.fr/actualite/escloud-un-label-franco-allemand-pour-les-services-informatique-en-nuage-de-confiance/

*Les opinions exprimées ici n'engagent que la responsabilité de leur auteur.*

## Dernières publications

- Benjamin Hautecouverture, « Why must the sanctions against Pyongyang be strengthened ? », note n° 22/2017, 19 December 2017
- Mohamed Ben Lamma, « Face au chaos libyen, l'Europe se cherche encore », note n° 21/2017, 14 décembre 2017
- Benjamin Hautecouverture, « Pourquoi il faut renforcer les sanctions contre Pyongyang », note n° 20/2017, 6 décembre 2017
- Benjamin Hautecouverture, « Crise nucléaire nord-coréenne : que peut faire l'UE ? », note n° 19/2017, 15 novembre 2017
- Emmanuelle Maître, « Le couple franco-allemand et les questions nucléaires : vers un rapprochement ? », note n° 18/2017, 7 novembre 2017
- Monika Chansoria, « Indo-Japanese Strategic Partnership : Scope and Future Avenues », note n° 17/2017, 19 September 2017
- Antoine Vagneur-Jones, Can Kasapoglu, « Bridging the Gulf: Turkey's forward base in Qatar », note n° 16/2014, 11 August 2017
- Patrick Hébrard, « Pérennité du groupe aéronaval : enjeux stratégiques et industriels », note n° 15/2017, 10 août 2017
- Régis Genté, « Le jeu russe en Libye, élément du dialogue avec Washington », note n° 14/2017, 26 juillet 2017
- Antoine Vagneur-Jones, « Global Britain in the Gulf: Brexit and relations with the GCC », note n° 13/2017, 18 July 2017
- Stéphane Delory, Can Kasapoglu, « Thinking Twice about Iran's Missile Trends : the Threat is Real but Different than Predicted », note n° 12/2017, 29 June 2017
- Anne-Claire Courtois, « Le Burundi en crise : Pirates contre 'Vrais' Combattants », note n° 11/2017, 20 juin 2017
- Antoine Bondaz, « North Korea's capabilities and South Korea's dilemma » note n° 10/2017, 2 juin 2017
- Antoine Bondaz, « La réaction chinoise au déploiement du THAAD, illustration du dilemme sud-coréen », note n° 09/2017, 10 avril 2017
- Emmanuelle Maître, « A treaty banning nuclear weapons: diversion or breakthrough?, note n° 08/2017, 16 March 2017
- Antoine Vagneur-Jones, « War and opportunity: the Turkistan Islamic Party and the Syrian conflit », note n° 07/2017, 2 March 2017
- Bruno Tertrais, « La pérennisation de la composante océanique : enjeux et perspectives », note n° 06/2017, 28 février 2017
- Antoine Bondaz et Marc Julienne, « Moderniser et discipliner, la réforme de l'armée chinoise sous Xi Jinping », note n° 05/2017, 24 février 2017
- Gérard Gerold et Thomas Sullivan, « République démocratique du Congo : une alternance pacifique est-elle encore possible ? », note n° 04/2017, 16 février 2017
- Valérie Niquet, « Le saut dans l'inconnu : quelles relations entre Pékin et Washington avec Donald Trump ? », note n° 03/2017, 6 février 2017
- Jean-Paul Maréchal, « Après Paris et Marrakech, quelles perspectives pour le régime climatique mondial ? », note n° 02/2017, 18 janvier 2017
- Valérie Niquet, « Sécurité maritime en Asie : l'impossible indifférence de l'Europe », note n° 01/2017, 4 janvier 2017

La Fondation pour la Recherche Stratégique est une fondation reconnue d'utilité publique. Centre de recherche indépendant, elle réalise des études pour les ministères et agences français, les institutions européennes, les organisations internationales et les entreprises. Elle contribue au débat stratégique en France et à l'étranger.

WWW.FRSTRATEGIE.ORG

4 BIS RUE DES PÂTURES 75016 PARIS TÉL : 01 43 13 77 77 FAX 01 43 13 77 78

ISSN : 2273-4643