# L'intelligence artificielle dans le domaine de la sécurité et de la défense européenne

par Anne Cammilleri
*Professeur à l'Université Paris-Nord (Paris XIII – Sorbonne-Paris-Cité)*
*Co-directrice du Master Sécurité, Défense*
*et Intelligence Stratégique de Sciences-Po Rennes*

L'Intelligence artificielle (IA) devient le nouvel ADN du cinquième domaine opérationnel ! Nous retiendrons la définition suivante de l'IA formulée par la Commission européenne dans sa communication sur « *L'intelligence artificielle pour l'Europe* » du 25 avril 2018 *: « les systèmes qui font preuve d'un comportement intelligent en analysant leur environnement et en prenant des mesures – avec un certain degré d'autonomie – pour atteindre des objectifs spécifiques »*[1]. Elle y inclut *« Les systèmes dotés d'IA peuvent être purement logiciels, agissant dans le monde virtuel (assistants vocaux, logiciels d'analyse d'images, moteurs de recherche ou systèmes de reconnaissance vocale et faciale, par exemple) mais l'IA peut aussi être intégrée dans des dispositifs matériels (robots évolués, voitures autonomes, drones ou applications de l'internet des objets, par exemple) »*[2]*. Qu'est-ce qui différencie l'intelligence artificielle de l'intelligence humaine ? Est-ce l'existence* d'une conscience, qualité exclusive de l'humain et non de l'IA *?* Les réflexions les plus abouties pour définir les contours d'une éthique et d'un droit de l'IA proviennent de la recherche médicale.

On soulignera notamment les travaux de Cynthia Fleury au sein de la Chaire de philosophie à l'hôpital, de l'Université Paris-Descartes[3] : elle démontre que c'est l'existence d'une conscience qui différencie l'homme de l'intelligence humaine en s'appuyant sur *les Méditations* de Descartes et sur les travaux de Montaigne sur les stéréotypes. Elle cite les travaux du professeur neurologue Lionel Naccache

1. Communication de la Commission, L*'intelligence artificielle pour l'Europe*, 25/4/2018, COM(2018) 237 final.
2. *Op. cit*. p. 2.
3. C. Fleury https://bit.ly/2GcSwF0.

énonçant que la conscience humaine, c'est *« être conscient qu'il existe un monde en dehors de soi »*. Cynthia Fleury reprend la déclaration de Cambridge des chercheurs en neurosciences computationnelles sur la conscience soulignant que *« la conscience n'est pas une exception humaine, mais partagée avec des animaux »* (…) « *comme le perroquet gris du Gabon, les pies et les dauphins* ». L'IA, au contraire de l'intelligence humaine, n'a pas de conscience ! Elle est définie comme un *« ensemble de techniques pour permettre à une machine de simuler l'intelligence en faisant des tâches très compartimentées. Aucune IA n'est capable d'agencer des niveaux de IA »* (…) *« alors que l'intelligence humaine est une conscience, une entité, qui a une capacité de synthèse d'adaptation à un environnement »*.

Dans ce contexte, il était grand temps que l'Union européenne (UE) s'intéressât à cet investissement d'avenir, sachant que les États-Unis ont déjà investi depuis 2016 plus de 970 millions d'euros dans la recherche et la Chine avec plus de 1,7 milliards ambitionne de *« devenir le leader mondial d'ici à 2030 »*[4]. D'autres États, comme le Canada, l'Espagne, le Royaume-Uni restent attentifs aux progrès de la recherche.

## I. L'appropriation de l'IA dans le monde civil, une nécessité de survie !

L'IA et le numérique font partie de la même famille. Dès lors, on comprend la place qu'occupe aujourd'hui l'IA dans les politiques de l'Union européenne et le droit du numérique, avant même la Politique de Sécurité et de Défense Commune (PESC). L'Union développe une stratégie volontariste par le renforcement du marché numérique (**A**) et devra définir une éthique adéquate pour l'usage de l'intelligence artificielle (**B**).

### A. Une stratégie volontariste par le renforcement du marché unique numérique

Le programme pour 2021-2027 est ambitieux (1) et repose sur un investissement fort en faveur de la recherche civile, clé de l'avenir (2).

#### *1. L'approche volontariste européenne par le programme sur l'Europe numérique 2021-2027*[5]

La Commission a adopté ce programme dans les domaines informatiques de haute technicité, en faisant le constat initial d'un déficit dans le Calcul de

4. Stratégie précitée p. 5.
5. COM 2018, 434 final.

Haute performance (CHP). Elle souligne ainsi l'écart financier européen de l'investissement de deux milliards d'euros, là où les États-Unis prévoient dix fois plus. Aussi retient-elle, notamment, comme objets de recherche le CHP, l'intelligence artificielle, la cybersécurité. Concernant le CHP, l'enjeu mathématique est extraordinaire, puisqu'il s'agit de créer une infrastructure de super calcul de deux niveaux : de niveau *Peta-flopiques* ($10^{15}$ opérations par seconde) et de *pre*-exaflopique, c'est-à-dire $10^{18}$ opérations par seconde. Il s'agit du prolongement du programme PRACE de 2010, associant 25 états membres, qui permit de renforcer l'accès aux réseaux des États membres en fournissant sept systèmes de pointe par cinq États hébergeurs (la France, l'Allemagne, l'Italie, l'Espagne et la Suisse[6]).

Pour ce faire, une entreprise commune EURO-HPC sera créée. *L'entreprise commune* établie à Luxembourg réunira l'UE et douze États membres[7] (et un associé suisse), deux associations La *plateforme technologique européenne de calcul ETP4 HPC* et *la Big Data Association BDVA* belge. Il est possible à tout État d'adhérer ultérieurement. Elle prendra le relais du programme H 2020. Notons que la vigilance requise au regard de la protection du patrimoine scientifique et intellectuel est partielle, puisqu'il est prévu que toute entité qui soutient la recherche et l'innovation dans un État membre ou pays associé au H 2020 et qui est établie dans l'UE peut demander à devenir membre de l'entreprise commune. Toutefois, la qualité de membre de l'entreprise ne peut être transférée à un tiers sans l'accord préalable du Comité directeur.

Le second objectif consiste à renforcer les capacités fondamentales de l'IA en Europe, en intégrant les bases de données et des référentiels d'algorithmes, afin de les rendre accessibles à toutes les entreprises et les administrations publiques. Dans ce domaine, le programme vise à renforcer et à mettre en réseau les installations d'essai et d'expérimentation existants. Quatre types d'actions seront donc mises en œuvre au niveau européen :

– création *d'espaces européens communs et ouverts de données.* L'interopérabilité sémantique y sera recherchée ;

– le développement de bibliothèques d'algorithmes européennes communes, accessibles à tous ;

– un cofinancement des États membres dans des sites de classe mondiale pour favoriser des expérimentations et essais dans des conditions réelles dans de secteurs dits essentiels dont la sécurité, mais aussi la santé, la surveillance de la terre, l'environnement, la mobilité et d'autres domaines publics ;

– ces sites seront équipés de grandes installations, de calcul reposant sur les dernières technologies IA y compris les domaines émergents que sont l'informa-

6. Adoption du CHP par le CESE lors de son assemblée plénière du 4 mai 2018.
7. France, Belgique, Bulgarie, Croatie, Allemagne, Grèce, Italie, Luxembourg, les Pays-Bas, la Slovénie, Portugal, Slovénie, Espagne et même la Suisse.

tique neuromorphiques, l'apprentissage profond (*Deep learning*) et la robotique. Le CHP sera en synergie avec les autres programmes H 2020, Horizon Europe, Europe numérique et Erasmus.

*Le troisième* objectif est de renforcer la confiance dans la cybersécurité par la création d'un centre européen de compétences industrielles, technologiques et de recherche : il s'agit de consolider des capacités essentielles pour garantir l'économie numérique dans une société démocratique. Les investissements dans des équipements avancés sont évidemment complémentaires à ceux envisagés en IA pour protéger les infrastructures critiques et notamment la mise en réseau des centres de compétences (ANSSI) pour définir des produits de cybersécurité de confiance. Cette synergie entre l'IA et la cybersécurité renforcera l'effectivité du *principe de Security by design*. Cet ensemble produira un cercle vertueux, favorable à la modernité. Tel est le sens de la proposition de règlement du Parlement européen et du Conseil, du 12 septembre 2018, établissant le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination[8], sur l'initiative de la Commission européenne lors de la réunion des dirigeants en 2018 à Salzbourg. Ce nouveau dispositif viendrait renforcer l'entrée en vigueur de la directive NIS[9] qui permet de mieux protéger le marché de la cybersécurité représentant plus de 600 milliards d'euros.

On retiendra la double base juridique des articles 187 TFUE et 173 § 3 TFUE pour le soutien de la base industrielle. Ce centre devrait être *« le principal instrument de l'Union pour mettre en commun les investissements dans la recherche, le développement technologique et industriel en matière de cybersécurité »* On soulignera, tout particulièrement (art. 4 § 7), le lien avec la défense clairement établi : il revient au centre de compétences de *« renforcer la coopération entre les sphères civile et militaire en ce qui concerne les technologies et les applications à double usage dans le domaine de la cybersécurité »*. Il s'agit ensuite de gérer un maillage territorial par la création de centres nationaux de coordination qui seront accrédités par la Commission qui en publiera la liste (art. 6 règlement) et qui fonctionneront, en réseau, sous la coordination du Centre de compétences.

Sera ainsi reconnue une *communauté de compétences* qui *« se compose de l'industrie, d'organismes universitaires et d'organisations de recherche sans but lucratif, ainsi que d'associations, d'entités publiques et d'autres entités traitant de questions opérationnelles et techniques »* (art. 8 § 2). L'établissement permettra,

8. Proposition de règlement du Parlement européen et du Conseil du 12/9/2018 établissant le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination COM(2018) 630 final.
9. Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, JOUE L 194, 19/7/2016, p. 1-30.

dans l'Union européenne, l'obtention d'une accréditation des compétences en recherche et développement industriel, en formation et éducation (art. 8 § 3c.). Ce Centre de compétences travaillera, notamment, avec « *EC3* » au sein d'Europol et l'Agence européenne de défense. (art. 10). À l'inverse, le rôle de l'ENISA y est circonscrit en qualité *« d'observateur permanent au sein du conseil de direction »* (art. 12 § 7).

La mission principale du comité est l'adoption d'un plan stratégique pluriannuel des priorités en matière de cybersécurité et on soulignera notamment qu'il décide de la méthode de calcul de la contribution financière des États membres (art. 13 s.). L'Union détiendra 50 % des droits de vote indivisible et chaque État aura une voix. L'adoption des décisions est assez redoutable à obtenir en termes de légitimité avec l'obligation d'obtenir au sein du Conseil *« des décisions à la majorité d'au moins 75 % de l'ensemble des voix, y compris celles des membres absents, représentant au moins 75 % du total des contributions financières au Centre de compétences »* (art. 15 § 3).

Le directeur exécutif et le conseil de direction peuvent s'appuyer sur un comité consultatif industriel et scientifique et *« des représentants de la Commission et de l'ENISA qui peuvent participer aux travaux du comité consultatif industriel et scientifique et les appuyer »* (art. 18 § 5). La contribution financière de l'Union ancrée sur le programme *« Horizon Europe »*, serait de 1 981 668 000 euros ! (art. 21). Enfin, la Cour de justice sera compétente pour les litiges relatifs aux clauses compromissoires et aux agents. Il est intéressant de noter que la protection des données à caractère personnel est bien un principe retenu ; mais, elle est renvoyée à un règlement *ad hoc* attendu en 2018, et non pas à une application pure et simple du règlement général sur la protection des données (art. 43 § 1).

Ce centre aura nécessairement un rôle d'orientation et d'application du système européen de certification des produits de cybersécurité. 2018 est l'année qui a lié l'évolution européenne de la cybersécurité, de la cyberdéfense et de l'intelligence artificielle. Pour preuve de cette évolution majeure, le Parlement européen a adopté, le 13 juin 2018, une résolution sur la cyberdéfense en ce sens[10]. Mais c'est bien un investissement fort sur la recherche civile qui est la clé de l'avenir.

### *2. Un investissement fort sur la recherche civile, clé de l'avenir*

Au titre des stratégies de coopération, l'Union européenne incite les États membres à se doter de *stratégies nationales ad hoc* afin de renforcer *« la capacité technologique et industrielle de l'UE et le recours à l'IA dans l'ensemble de l'économie »*. Tel est déjà le cas de la France depuis le 29 mars 2018 avec le rapport

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

Villani, *« Donner un sens à l'intelligence artificielle »*[11], mais aussi de la Finlande et l'Allemagne. Dans l'esprit de la construction européenne, l'IA figure dans les programmes-cadres de recherche sur la robotique. Le 10 avril 2018, 25 États membres (dont le Royaume-Uni) ont signé une déclaration de coopération relative au développement d'une IA visant à prendre en compte les questions éthiques, sociales, économiques et juridiques. Ils ont été rejoints, en 2018, par la Roumanie, la Grèce, la Croatie. L'Europe des 28 existe donc encore autour de l'enjeu stratégique de développement de l'IA : c'est la preuve de la prise de conscience de la transformation du marché unique imposée par l'IA. Il connait déjà des applications industrielles avec le projet de recherche *Aeroarms*[12] utilisant des drones.

En matière de recherche civile, la Commission a lancé des initiatives d'envergure pour l'IA, notamment relatives à la mise au point de *composants et systèmes électroniques* plus efficaces tels que les puces neuromorphiques, sur le modèle de structures biologiques telles que le cerveau. Ce projet s'inscrit dans le cadre de l'entreprise commune ITC ECSEL *Composants et systèmes électroniques pour un leadership européen* pour lequel 4, 8 milliards d'euros d'investissements publics-privés sont prévus jusqu'en 2020. Il prend le relais de la recherche des entreprises communes ENIAC et ARTEMIS sur la nanoélectronique et les systèmes embarqués. D'autres thématiques convergentes concernent des projets phares relatifs à l'émergence de technologies quantiques. Selon une stratégie bien rodée, la Commission s'appuie sur un réseau de pôles d'innovation numériques *ad hoc*.

Au titre des essais et expérimentations, la Commission assume également *une politique de soutien aux essais et à l'expérimentation*, en matière de recherche fondamentale comme industrielle. Ce sont les soins de santé, les transports et le contrôle et l'entretien des infrastructures, l'agroalimentaire et la production intégrée par ordinateur, qui feront l'objet d'un appui conséquent, mais ces thématiques ne sauraient être exhaustives. L'Institut Européen d'Innovation et de Technologie intégrera l'IA dans l'ensemble des programmes qu'il soutient en faveur du développement d'un véritable vivier de talents dans le domaine de l'IA. Il reste à espérer que ce rayonnement touchera la sécurité et la défense sur la base des recherches duales.

### B. Définir une éthique adéquate pour l'usage de l'IA

Les règles éthiques doivent être définies dès la conception de la technologie (1) et reposer sur une méthode bien circonscrite (2).

11. C. Villani, « *Donner un sens à l'intelligence artificielle* », *rap. 28 mars 2018* https://www.aiforhumanity.fr/
12. (*AErial RObotics System integrating multiple ARMS and advanced manipulation capabilities for inspection and maintenance*).

### *1. Quelle éthique recherchée au moment de la conception de la technologie ?*

Comme toute révolution industrielle, l'arrivée de l'IA impose un débat sociétal éthique. La position de la Commission est très claire : *« ensemble, nous pouvons placer la puissance de l'IA au service du progrès humain »*[13]. Il n'est plus question de donner une quelconque personnalité juridique aux robots et la personne humaine est bien au centre de la construction européenne[14]. *Exit* les transhumanistes ! Il est absolument nécessaire d'accompagner l'encadrement juridique de l'IA par un débat substantiel sur l'éthique. Mais, il apparait très vite que l'éthique et le droit sont ici unis, l'éthique ayant le devant de la scène, puis l'expérimentation permettra de faire émerger un nouveau *corpus* juridique, afin d'encadrer tous les usages. La Commission appuie sa démarche sur les valeurs de l'UE, le respect des droits fondamentaux ainsi que sur le RGPD[15] et travaille avec le Groupe européen d'éthique des sciences et des nouvelles technologies.

Il s'agit donc d'une démarche juridique et éthique. Comme, dans de nombreux programmes de recherche existants, cette éthique doit notamment signifier l'intégration, *lors de la conception de la technologie,* des éléments permettant d'assurer à la fois la protection de la vie privée (*privacy by design*) et la sécurité de l'utilisation produit (*security by design*) tout au long du cycle de vie de la technologie. Ainsi ces deux principes pourraient bien devenir l'essence même de la conception d'une technologie IA éthique. Mais il serait bien trop réducteur de penser que cette éthique puisse se résumer au respect de ces deux principes. D'ailleurs, la Commission entend établir *des lignes directrices, en* y ajoutant notamment la recherche de la transparence algorithmique dès sa conception.

### *2. Quelle méthode éthique pour l'utilisation de la technologie intégrant de l'IA ?*

La Commission soutient les règles relatives à la non-discrimination, la dignité et ouvre un débat plus large sur les travaux du groupe européen d'éthique des sciences et des nouvelles technologies (GEE), de la société civile et notamment de nombreux chercheurs proposent de se référer aux principes AZILOMAR[16] qui couvrent toute la recherche éthique relative à l'IA. Antérieurement, le GEE

13. Rapport Commission, p. 16 et 22.
14. A. Cammilleri, « *Chronique annuelle sur les nouvelles technologies*, », *RDUE* 2017 n° 4 pp. 99-143.
15. Art. 13, § 2, point f), art. 14, § 2, point g), et art. 15, § 1, point h), du règlement (UE) 2016/679 du RGPD.
16. Service de la Commission, doc. de travail : *La responsabilité pour les nouvelles technologies numériques L'intelligence artificielle pour l'Europe* {COM (2018) 237 final ; les principes AZILOMAR.

a publié, le 9 mars 2018, une déclaration pertinente sur *« l'IA, la robotique et les systèmes autonomes »*[17]. Il a retenu une approche globale, en travaillant sur la recherche de la meilleure éthique de la conception à la production et l'utilisation de l'IA, en s'appuyant sur la Charte des droits fondamentaux de l'UE : il souligne l'importance de la mécatronique qui est l'association de l'IA et de l'apprentissage profond (*deep learning*) à l'origine des systèmes d'armes robotisés et des véhicules autonomes. Il invite à travailler sur des réflexions morales et sur les règles de responsabilité morale et juridique envisagées : le groupe reprend la notion d'autonomie de la personne qui demeure « *un aspect important de la dignité humaine qui ne devrait pas être relativisé* » et rejette l'octroi d'une personnalité juridique des robots[18]. Il souligne ainsi que pour les systèmes d'armes létales autonomes (SALA) et des véhicules autonomes, il semble que la nécessité d'un contrôle important de la part de l'être humain pour assurer la responsabilité morale ait fait consensus. Il implique que *« les êtres humains (et non les ordinateurs et leurs algorithmes) doivent fondamentalement rester aux commandes et, de ce fait, demeurer moralement responsables »*[19].

La Commission a souhaité élargir ses sources d'expertise. C'est la raison pour laquelle l'Alliance européenne pour l'IA a été inauguré le 14 juin 2018 réunissant 52 experts, le *High Level Group on Artificial Intelligence (AI HLG)* incluant neuf français. Ses travaux portent sur les thèmes de *« l'équité, la sécurité et la transparence de l'IA »*. L'Alliance a pour mission de proposer des bonnes pratiques. L'objectif de l'Union est ainsi de garantir l'existence d'un cadre éthique et juridique approprié, *« fondé sur les valeurs de l'Union et conforme à la Charte des droits fondamentaux de l'UE, comprenant notamment de futures orientations sur les règles existantes en matière de responsabilité du fait des produits, une analyse détaillée des nouveaux défis et une coopération avec les parties prenantes, …/… en vue de l'élaboration de directives sur l'éthique de l'IA »*[20]. La Commission s'appuiera sur l'évaluation faite par l'Agence des droits fondamentaux sur l'utilisation de ces nouvelles technologies pour faire évoluer, si nécessaire ce cadre éthique. En France, la question du *« militaire augmenté »* a été notamment étudiée par l'IRSEM[21]. De telles interrogations éthiques ne sont pas toujours présentes dans le discours outre atlantique dominant et la frontière entre médecine thérapeutique et médecine de performance n'est pas toujours aisée à identifier[22].

---

17. *Déclaration sur l'intelligence artificielle, la robotique et les systèmes « autonomes ».* Au-delà d'un cadre éthique étroit. p. 12.
18. Le PE ne veut pas attribuer de droits humains aux robots, M. Delvaux, 13/04/2018.
19. p. 12 du rapport précité.
20. Communication de la Commission précitée sur l'IA du 25 avril 2018, p. 51.
21. A. Colin : L'homme augmenté, réflexions sociologiques pour le militaire, IRSEM, 2016 n° 42, p. 11.
22. H. Hude, Réflexions d'éthique sur le soldat augmenté, *Cahiers de la revue de défense nationale* 2017.

Mais, l'enjeu n'est pas seulement européen, il est aussi nécessairement international ! Rechercher les contours de l'éthique de l'IA est un sujet passionnant qui attire les consultations citoyennes : la Commission souligne l'importance de la déclaration de Montréal du 3 novembre 2017[23] qui énonce les valeurs et les domaines positifs d'action de l'IA en visant le bien être des personnes, l'autonomie, la justice, la vie privée, la connaissance, la démocratie la responsabilité qui rejoignent assez bien les 10 grands principes d'UNI Global Union pour une IA éthique[24]. Il suffit de reprendre la liste des principes éthiques de l'IA, pour que le juriste constate que ces règles éthiques sont d'ores et déjà des normes relevant souvent des droits fondamentaux. On assiste à une construction d'un cadre juridique dont l'affichage éthique se veut rassurant face à l'imaginaire collectif de ce que sera l'IA, demain.

Toutefois, l'épineuse question de la soumission des technologies de l'IA aux règles de la responsabilité du fait des produits demeure. La Commission mène une étude pour évaluer les difficultés relatives à l'application du principe de la responsabilité du fait des produits pour proposer en 2019 une révision de la directive sur la responsabilité du fait des produits, afin de garantir la clarté juridique pour les consommateurs et les producteurs en cas de produits défectueux. Nombreux sont les juristes qui émettent des avis réservés sur l'application du droit de la responsabilité classique[25].

## II. Les enjeux de l'IA dans la politique de sécurité et de défense commune

L'avenir nous dira si la coopération structurée permanente (CSP) va favoriser la convergence des IA opérationnelles (**A**) alors même que déjà sont visibles certains signaux faibles de la participation française à la CSP (**B**).

### A. La Coopération structurée permanente (CSP) comme moyen de convergence entre IA opérationnelles ?

La vedette de l'année : la CSP est-elle bien un moyen de convergence entre IA opérationnelles ou n'est-elle pas le miroir aux alouettes américain ? Il faut tenir compte de la dimension politique de la CSP, test majeur de l'effectivité de la solidarité (1) et se demander si l'on vient ressusciter l'Organisme Conjoint de Coopération en matière d'armement (OCCAR) (2).

23. https://www.montrealdeclaration-responsibleai.com.
24. Les dix principes pour une IA intelligente présentés par Uni Global Union : https://bit.ly/2IwoVds.
25. Le droit à l'épreuve de la robotique LGDJ 2018 ; A. Touati et C. Chasseriau, *Chatbots, quel(s) responsable(s)* ?, *Wolters Kluwer France – Actualités du droit,* 6 juin 2018.

### *1. La dimension politique de la CSP : le test majeur de l'effectivité de la solidarité*

Une perception optimiste de la chose permet de souligner que le recours à la CSP, notifié par les États membres de l'UE au Conseil et à la Haute Représentante doit permettre de prendre en compte la spécificité de la chose militaire ! Sur la base de la coordination de plans nationaux, il s'agira d'optimiser la recherche et l'acquisition de technologies – *idéalement européennes !* – afin de préparer la guerre du futur ! Nul ne doute que la compétition technologique sera, entre les États membres, une source de progrès pour mener les opérations de combat de demain. L'objectif affirmé par le chef des armées français serait *« la refondation d'une Europe souveraine et unie »*[26] !

La notification par les États membres de l'UE de leur volonté de s'allier[27] est, à n'en pas douter, un événement majeur dans la manière d'anticiper les futures OPEX. Le Parlement européen incite au développement des cyber-technologies qui intègre l'IA, l'internet des objets et la robotique[28]. Le lien naturel entre la cybersécurité et l'IA est enfin posé, témoignant d'une immense évolution des mentalités qui permettra d'avancer dans le bon sens, en concevant l'usage de l'IA à tous les niveaux[29] ! Loin devant, sont les États-Unis qui ont, d'ores et déjà, recours à l'IA dans le cadre de leurs opérations militaires : comme l'admet le service de recherche du Congrès américain[30], l'usage de l'IA vise, surtout, la collecte d'informations, la logistique, les opérations dans le cyberespace, le commandement et le contrôle de véhicules autonomes. En Europe, la restructuration institutionnelle autour de l'IA semble s'organiser dans le cadre de l'Organisme conjoint de coopération en matière d'armement.

### *2. Ressusciter l'Organisme Conjoint de Coopération en matière d'armement (OCCAR) ?*

Une perception toujours politique de la CSP, mais moins optimiste, est de signaler le risque que cela fasse *« pschitt »* ! En effet une lecture attentive des

26. A. Cammilleri, *« Recherche commun désespérément ! », Blog de droit européen* d'Olivia Tambou : https://blogdroiteuropeen.com/, avril 2018.
27. Une CSP où ne participent ni le Danemark ni le Royaume-Uni ni Malte, soit pour des raisons historiques de volonté de différenciation, soit pour l'absence de niveau de capacités suffisantes.
28. Résolution 2018/2004 (INI) du PE du 13 juillet 2018 sur la cyberdéfense. (2018)0258.
29. *Rapport d'information n° 1 141* de la Commission de la défense nationale et des forces armées de l'Assemblée nationale du 4 juillet 2018, présenté par Bastien Lachaud et Valetta Ardisson au terme d'une mission d'information sur la cyberdéfense.
30. Daniel S. Hoadley & Nathan J. Lucas, *Artificial Intelligence and National Security*, April 26, 2018, Congressional Research Service 7-5700. https://fas.org/sgp/crs/natsec/R45178.pdf.

textes[31] permet de souligner les faiblesses européennes *: si l'AED demeure le Forum européen de développement des capacités,* l'apparition de signaux faibles de plus en plus prégnants témoigne de son recul. L'AED n'interviendra qu'en *« soutien »* de la coopération pour l'évaluation des contributions des États participants *« en vue de faciliter la coopération »*. Parallèlement, on assiste au retour en force de l'OCCAR comme *« organisme privilégié »* pour la gestion des programmes communs ! Il est malheureusement possible de douter de l'effectivité de la solidarité européenne en faveur du recours systématique à des technologies *européennes* puisque les États membres ont réaffirmé leur attachement à ce que *« l'exigence de normes communes techniques et opérationnelles garantisse l'opérabilité avec l'OTAN »*. Cette dépendance scientifique et technique à la standardisation de l'OTAN, cumulée au contexte politico-économique entretenu par le Président des États-Unis, rend l'indépendance militaire de l'Union européenne vis-à-vis des États-Unis bien délicate ! Aussi, la France pourrait-elle s'octroyer un rôle diplomatique et militaire important dans le cadre de la CSP…Mais les premiers signaux sont, là encore, plutôt des signaux faibles (B) !

## B. Les signaux faibles de la participation française à la CSP

L'enjeu, ici, est d'apprécier l'effectivité de la solidarité européenne. Sur les dix-sept projets identifiés, huit sont sans aucune participation française et, à l'inverse, si on célèbre l'évènement politique, on saluera la participation française à neuf d'entre eux qui seront mis au service des missions de Petersberg, notamment dans le cadre de la lutte contre le terrorisme. On peut alors prendre le verre à moitié plein (1) ou à moitié vide (2).

### *1. Prenons le verre à moitié vide*

Actuellement en France, il est vrai, en matière de recherche, que *« l'IA est encore peu utilisée dans les armées, à part pour quelques fonctions de base comme le traitement d'image »*[32]. Ainsi, le 16 mars 2018, Florence Parly, ministre des Armées, annonçait un plan pour le développement de l'IA pour renforcer les capacités militaires françaises. Il s'agit de doter la défense d'un budget annuel de 100 millions d'euros consacrés à l'IA, et des experts devraient être recru-

31. Décision (PESC) 2017/2315 du Conseil du 11 décembre 2017 établissant une coopération structurée permanente (CSP) et fixant la liste des États membres participants. Décision (PESC) 2018/340 du Conseil du 6 mars 2018 établissant la liste des projets, JOUE L 65/24 du 8/3/2018. Recommandation du Conseil 2018/C 88/01 du 6/3/2018 concernant une feuille de route pour la mise en œuvre de la CSP, JOUE C 88/1 du 8/3/2018.

32. Entretien avec Eva Cruck, DGA, ancienne coresponsable du programme sécurité globale de l'ANR.

tés d'ici 2022 au sein de la Direction générale de l'armement (DGA). Elle a aussi annoncé la création d'une *« Agence de l'innovation de défense »* au sein du ministère, qui inclura des *start-up* et cherchera à nouer des partenariats au niveau européen[33]. La moitié du budget annuel alloué à l'IA militaire devrait financer des programmes de recherche, et quelque 10 millions d'euros le seront pour l'évaluation et l'intégration au système de défense. À titre d'exemple, le système de combat aérien futur (avion ou drones), le projet *Man Machine Teaming (MMT[34])* est *« une initiative lancée et financée par la Direction générale de l'armement. Elle est animée par Dassault Aviation et Thales »*. Il s'agira de développer un système aérien cognitif comprenant un *« Assistant Virtuel et Smart Cockpit »*. Dans le cadre de la définition du système de combat aérien futur (SCAF), ce projet *« explore la possibilité de développer un système aérien cognitif »*.

Alors réjouissons-nous qu'au niveau de l'Union européenne la participation française future puisse porter sur neuf projets de la CSP pour lesquels on peut aisément imaginer que les progrès offerts par l'IA, pourront être un outil au service de la finalité de la mission : ainsi le projet relatif au *Commandement médical* permettra une amélioration de la prise en charge des blessés par l'utilisation de l'IA dans certaines opérations de santé. On peut considérer que les technologies fondées sur l'IA et la cybersécurité permettront une participation de la France *en radio-logicielle sécurisée européenne,* dans les *centres de formations des missions,* par la prise en charge de la *fonction opérationnelle en matière d'énergie* ou encore la participation à des équipes *d'intervention rapide face à un incident de sécurité.* Il en est de même pour l*es projets relatifs à l*a *mise en réseau de plateformes logistiques et d'appui d'opération, la mobilité militaire avec l'appui des drones et en dernier lieu dans le cadre du noyau dur opérationnel d'EUFOR.*

La France devra être capable de valoriser son savoir-faire, en s'appuyant sur les pôles d'excellence *ad hoc* et surtout sur son riche réseau d'industriels de la sécurité et de la défense réunis au sein du COFIS. L'avenir est donc à l'optimisme pour la recherche appliquée et la vente sur étagères des technologies françaises et européennes comme en témoigne le marché des drones.

### *2. Prenons le verre à moitié vide*

*La France ne s'est pas associée à huit projets de la coopération structurée permanente.* Si l'on comprend bien que notre pays n'a plus les moyens d'être omniprésent, il n'en demeure pas moins que notre absence est délicate stratégiquement à concevoir dans des projets relatifs au centre européen de certification des formations pour les armées européennes, dans l'organisation des dispositifs de déploiements des secours en cas de catastrophes, ou pire dans les projets de surveillance de

33. La France est-elle armée dans la course à l'intelligence artificielle ?Charles Thibout, IRIS, 19 mars 2018 : https://bit.ly/2Zd3IKz.
34. https://man-machine-teaming.com/

protection portuaire et maritime. Voire surprenante, notre absence pour la réalisation de la plateforme de partage d'informations en matière de menaces et d'incidents informatiques alors même que nous avons été un État particulièrement actif dans la mise en œuvre de la directive NIS[35]. Nous ne participons pas au système de commandement et de contrôle stratégique pour la PSDC, alors que nous sommes un État particulièrement investi dans les OPEX. Nous ne nous sommes pas associés au projet sur les véhicules blindés de combat et ceux relatifs à l'appui feu indirect.

Une explication pourrait être qu'étant particulièrement investis sur ces thématiques nous souhaiterions garder une avance certaine, afin de favoriser la filière de sécurité nationale, dans des contrats publics de gré à gré. On resterait alors sur ces sujets dans une posture régalienne affirmée ! Or, dans tous ces projets l'IA sera amenée à modifier les usages et l'absence de la France sur ces thématiques est un signal faible. *Dans le* débat sur l'interdiction des armes autonomes, on s'achemine vers la consécration d'une obligation selon laquelle décider d'engager une cible soit toujours *« une décision prise par un être humain »*[36], et le Groupe Européen d'Éthique des Sciences et des Nouvelles Technologies a adopté la même prudence en imposant *« un contrôle important de la part de l'être humain sur ces systèmes et sur la façon d'instituer des formes de contrôle moralement souhaitables »*[37].

**En conclusion**, on reprendra le propos de Jean Claude Junker, président de la Commission européenne, dans son *discours sur l'état de l'Union, en 2018,* intitulé « *l'heure de la souveraineté européenne » : « Je voudrais que l'Europe quitte les gradins du stade mondial. L'Europe ne doit pas être un spectateur, un commentateur des événements internationaux. Elle doit être un acteur constructif, un façonneur, un architecte du monde de demain »*[38].

35. Directive 2016/1148 du 6 juillet 2016 NIS transposée par la loi n° 2018-133 du 26 février 2018.
36. R. Chatila et C. Tessier, « *Armes létales autonomes : de quoi parle-t-on ? », CNRS Le journal* 15.03.2018 ; *adde,* chronique d'A. Cammilleri, *RDUE* 2017 précitée sur le rejet de la singularité technologique et le refus de la personnalité juridique des robots.
37. Groupe Européen d'Éthique des Sciences et des Nouvelles Technologies, « Déclaration sur l'intelligence artificielle, la robotique et les systèmes "autonomes" », 9/3/2018, p. 14.
38. J.-C. Junker, « État de l'Union en 2018, heure de la souveraineté européenne », 12.9.2018.