



6ème séminaire annuel  
de l'Association française de droit de la sécurité et de la défense (AFDSD)  
organisé avec le concours de l'Institut des Hautes Études Internationales (IHEI) de Paris II

**jeudi 28 mars 2019**

## **L'EUROPE DE LA SÉCURITÉ ET DE LA DÉFENSE**



Sous la direction de Pascale MARTIN-BIDOU et de Anne-Sophie TRAVERSAC  
Maîtres de conférences à l'Université Paris II - Panthéon-Assas

LES ACCORDS DANS LE CADRE DE LA POLITIQUE DE SÉCURITÉ ET DE DÉFENSE COMMUNE ENTRE  
L'UNION EUROPÉENNE ET LES ÉTATS TIERS

par Anne CAMMILLERI

*Professeure des Universités, Université Paris 13 Sorbonne Cité  
Co-directrice de l'Institut de Droit public, sciences Politiques et Sociales- IDPS  
Co-directrice du Master Sécurité Défense et Intelligence Stratégique-Sciences Po Rennes*

La PSDC a beau être une politique intergouvernementale, régie par une procédure de décision basée sur l'unanimité, elle repose aujourd'hui sur un socle juridique harmonisé entre les règles du droit international général et le droit spécifique de l'Union européenne. Ainsi, depuis plus de dix ans, elle a défini un socle décisionnel lui permettant de mener à bien ses opérations extérieures (OPEX) sur un fond de classicisme juridique assumé du respect du principe de non ingérence (I). Mais, par ailleurs, elle souffre d'un manque de modernité qui mériterait une meilleure anticipation de la guerre du futur (II).

## **I- LA PERMANENCE DES ACCORDS ENTRE L'UNION EUROPÉENNE ET LES ETATS HÔTES ET PARTICIPANTS AU NOM DU RESPECT DU PRINCIPE INTERNATIONAL DE NON INGÉRENCE (ART. 43 UE)**

### **A L'assouplissement du formalisme des accords externes**

Le Mali fait partie des priorités européennes puisque la mission PSDC "Sahel Mali" a été prorogée jusqu'au 14 janvier 2021 sous le commandement du chef de mission Philippe Rio jusqu'au 30 septembre 2020<sup>1</sup>. Cette mission constitue une illustration intéressante de cet assouplissement du formalisme européen, grâce à la reconnaissance de la personnalité juridique de l'UE (a) et permet un nouvel élan des accords externes... en forme simplifiée ! (b).

#### **a. Un formalisme allégé grâce à la reconnaissance de la personnalité juridique de l'UE.**

Sur la demande du Mali, la Haute Représentante de l'UE pour les affaires étrangères et la politique de sécurité a signé un accord avec cet Etat, en forme simplifiée, correspondant à un simple échange de lettres dans le cadre de la mission EUCAP Sahel Mali (art. 1 de la décision du 15 avril 2014<sup>2</sup>). Le dialogue ainsi instauré entre l'UE et le Mali a permis la mise sur pied de la mission globale EUCAP Sahel Mali le 8 octobre 2014<sup>3</sup>.

---

<sup>1</sup> Décision (PESC) 2019/345 du COPS du 22 février 2019 prorogeant le mandat du chef de la mission PSDC de l'Union européenne au Mali (EUCAP Sahel Mali) (EUCAP Sahel Mali/1/2019), JOUE L 62/10 du 1.3.2019

<sup>2</sup> Décision (PESC) 2014/219/ du Conseil du 15 avril 2014 relative à la mission PSDC de l'Union européenne au Mali (EUCAP Sahel Mali) (JO L 113 du 16.4.2014, p. 21).

<sup>3</sup> Décision 2014/853/PESC DU Conseil du 8 octobre 2014 relative à la signature et à la conclusion au nom de l'Union de l'accord sous forme d'échange de lettres entre l'Union européenne et la République du Mali relatif au statut de la mission PSDC de l'Union européenne au Mali (EUCAP Sahel Mali) JOUE L 344/1 du 29.11.2014.

Au nom du principe de non ingérence, l'Union qui souhaite être visible sur la scène internationale signe des accords internationaux, en son nom, depuis qu'elle est dotée de la personnalité juridique. C'est d'ailleurs pour cela que l'Union européenne peut recourir à une simplification des accords internationaux ne nécessitant plus la signature des Etats membres participants. Cette " substitution" de personnalité juridique est déjà en soi une première simplification des relations politico-militaires en Afrique. Elle n'a, en revanche bien sûr, aucune signification de suprématie de l'UE à l'encontre des Etats membres. Mais elle contribue fortement à la simplification du formalisme international sans porter atteinte à la sécurité juridique du dispositif.

### **b. Le nouveau souffle des accords UE et Etats hôtes externes... en forme simplifiée !**

Pour illustration la mission déployée au Mali, se fit par une lettre signée au nom de l'UE le 20 octobre 2014, par la Haute Représentante qui retrace clairement l'évolution d'une mission historiquement militaire en 2013, visant à contribuer à la formation des forces armées maliennes (EUTM Mali). L'année suivante une mission civile en soutien aux forces de sécurité malienne venait terminer les contours d'une mission civile EUCAP SAHEL MALI au service d'une approche intégrée de l'intervention européenne.

L'arrivée visible de l'Union européenne sur la scène opérationnelle s'est traduite par le renforcement du processus de standardisation entamé dans les années 2003-2004 lors de l'élaboration des accords internes SOFA qui permirent de déterminer les règles de déroulement des OPEX<sup>4</sup>.

Le schéma juridique d'une opération ou mission était standardisé avec la mention systématique de plusieurs facteurs bien identifiés. Il s'agissait de définir systématiquement le type d'opération et son cadre, le statut du personnel (identification des personnels et des biens, immunité juridictionnelle, l'inviolabilité des biens et des installations). L'organisation de la gestion civile imposait la définition préalable du personnel détaché, celle du régime de liberté de circulation, de la chaîne de commandement, du traitement des informations classifiées, des aspects financiers, de la résiliation de l'accord et du règlement des différends avec le seuil de 40 000 euros.

*Pour une OPEX*, les spécificités de la chaîne de commandement militaire, le renvoi aux spécificités du mécanisme historique de financement Athéna pour l'identification des coûts communs et les dispositions relatives à la vie de l'accord sécurisaient la dimension juridique et financière de l'opération ou de la mission. Le contenu de cet accord était inscrit dans une décision du Conseil l'approuvant, publiée au JOUE, avec parfois une entrée en vigueur rétroactive pour couvrir les dommages potentiels subis par les acteurs déjà sur le terrain. Le succès de cette procédure a permis une certaine forme de standardisation. Cette standardisation, qui est source de légitimité, a permis d'aller vers la signature d'accords en forme simplifiée.

Ainsi, s'il l'on prend pour illustration la mission EUCAP SAHEL Mali, on mesure à la fois l'internationalisation du droit de l'UE et sa simplification.

Par une lettre en forme simplifiée, la Haute représentante vise clairement à "recueillir l'agrément du chef d'Etat du Mali" pour la transformation de la mission militaire en mission civile. Elle précise toutefois qu'une réponse positive de sa part *"constituera un accord international juridiquement contraignant relatif au EUCAP Sahel Mali dont l'entrée en vigueur est définie à la date de réception de la lettre de réponse du Président du Mali."* Le

---

<sup>4</sup> Anne Cammilleri, *la Politique Européenne de sécurité et de défense*, Ed. Lavoisier, 2009.

formalisme ne disparaît pas puisque s'en suit une modification de la terminologie de l'accord visant à signifier la caractérisation civile de la mission. C'est bien en s'appuyant sur le constat de la transformation d'une mission militaire vers une mission civile que la Haute représentante, dans sa lettre du 20 octobre 2014, fait évoluer le cadre juridique de la mission, en recourant à la forme simplifiée de l'accord. Il s'agit, certes, d'un accord en forme simplifiée, mais l'opération de qualification juridique demeure forte, puisque le langage évolue avec un vocabulaire à connotation moins militaire passant du "commandant de l'opération" à celui de "chef de mission", des "quartiers généraux militaires" aux (simples) "quartiers généraux", des "personnels militaires" à la référence exclusive "des personnels", des "forces armées" aux "formateurs civils". Cette simplification ne se fait donc pas au détriment de la sécurité juridique requise.

C'est donc sans surprise qu'en réponse, le 31 octobre 2014, le Président du Mali, à son tour, donnait son accord pour faire évoluer le statut militaire de l'OPEX vers celui de la mission sur le territoire de son État. La continuité de la présence européenne sur le sol Malien se traduit par la continuité juridique des obligations existantes entre la première opex et la mission EUCAP Sahel Mali : *" toute mention de l'EUTM Mali est considérée comme se référant à l'EUCAP Sahel Mali"*

Il faut souligner que cette transformation de la mission militaire en mission civile permet- *globalement-* d'appliquer les règles précédemment posées dans l'accord du 4 avril 2013 pour la mission. Il en résulte que le Chef d'Etat Malien donne son agrément simplement : *"J'ai l'honneur de porter à votre connaissance que les termes de votre lettre recueillent mon agrément. Je vous prie d'agréer, Madame, l'assurance de ma très haute considération. Pour la République du Mali"*<sup>5</sup>.

L'intervention européenne au Mali permet ainsi de combiner de nombreuses qualités : le respect du formalisme international pour promouvoir le principe de non ingérence, la transformation de l'opération militaire en mission civile dans la continuité de la Politique de Sécurité et de Défense Commune, sur la base d'échanges formels mais simplifiés. La confiance est donc au rendez-vous et elle vise le retour à la paix ! Cette simplification formelle couplée à la maturité et au professionnalisme acquis par l'expérience de la signature des accords externes lors de la première décennie des années 2000 est mise aujourd'hui au service d'une stratégie intégrée (B).

## **B. Le défi de la PSDC : sa capacité à développer une approche intégrée.**

Les interventions extérieures de l'Union européenne reposent sur une approche à la fois globale et intégrée (a) mais avant tout dépendent de la signature d'accords avec des Etats tiers participants (b).

### **a. Entre intégration et globalisation de la politique extérieure de l'UE**

Lors de la réunion du Conseil du 25 juin 2018, sur la Région Sahel /Mali, les représentants des Etats membres ont mis l'accent sur la mise en place d'une approche intégrée qui dépasse largement l'approche initiale et spécifique de la PSDC. Il est pris acte de la contribution importante de l'UE, " mise sur l'adhésion au niveau local et la mise en place d'une approche intégrée pilotée au niveau politique et traitant de manière égale de la sécurité, la gouvernance et le développement.../... en particulier dans les zones les plus vulnérables"<sup>6</sup>. Il

---

<sup>5</sup> Brahim Boubacar Keïta.

<sup>6</sup> Conclusions du Conseil sur la Région du Sahel/Mali - lors de sa 3628<sup>e</sup> session, tenue le 25 juin 2018.

s'agit de renforcer la coopération avec les gouvernements des pays du G5 Sahel " pour assurer l'intégration effective du personnel formé dans le cadre des missions PSDC à leurs forces de sécurité nationales respectives". Le but est de renforcer, le cas échéant, le soutien civil et militaire à la coopération transfrontalière".

En revanche, sont inusitées jusqu'à alors les mentions selon lesquelles "il est essentiel de prendre en compte le lien entre " le changement climatique et la sécurité dans le dialogue politique, la prévention des conflits, le développement, et les stratégies en matière de risques de catastrophes, ainsi que d'en assurer pleinement l'articulation avec l'action humanitaire, dans une région qui pâtit gravement du changement climatique" (§7). La même approche intégrée permet de réaffirmer "le rôle essentiel des femmes et des filles pour ce qui est d'assurer la paix, le développement et la prospérité, et appelle les partenaires du Sahel à protéger et faire progresser l'émancipation des femmes et des filles et leur exercice des droits fondamentaux".

Cette approche intégrée sera indirectement soutenue financièrement par la révision du mécanisme d'ATHENA. Sa mutation en faveur de la *Facilité Européenne pour la Paix* qui devrait lui succéder permet de prévoir un budget pour la période 2021 -2027 de 10, 5 milliards d'euros auxquels s'ajouteront 13 milliards à destination des entreprises. Cela devrait permettre de financer les coûts communs militaires relatifs aux formations, l'équipement et les infrastructures, l'objectif étant "de maximiser l'impact et l'efficacité et la durabilité de l'ensemble des actions extérieures". Six opex sont concernées en Bosnie et en Afrique (Corne d'Afrique, la Somalie, le Mali, la RCA et la Méditerranée.

Une fois l'accord signé avec l'Etat hôte, les États membres participants à la mission/OPEX identifiés, l'Union européenne peut élargir la coopération en signant une seconde catégorie d'accords avec des Etats tiers qui souhaitent apporter leur soutien à un autre Etat tiers en s'associant à l'action de l'UE (b).

## **b. Les accords UE avec des Etats tiers participants**

L'UE étant une organisation européenne ouverte, elle accepte bien volontiers la participation d'Etats non européens pour la préparation et la réalisation d'une OPEX. Les accords ainsi passés, entre l'UE et les Etats tiers, sont également standardisés et l'Union essaie de maintenir une certaine uniformité. Toutefois, elle accepte également des dérogations aux règles générales qu'elle applique aux Etats membres. La Suisse est à cet égard un bon cas d'école. Mais cet affichage ne saurait signifier le renoncement cet Etat à faire valoir sa neutralité, même si elle participe effectivement à la mission Eucap Sahel, "*uniquement dans l'esprit et l'intérêt de la mission Eucap Sahel Mali*".

### **1. la Suisse pleinement sous drapeau européen !**

"Eucap sahel Mali a reçu l'appui du Canada et de la Norvège qui ont mis à la disposition de la mission SAHEL Mali, deux experts en ressources humaines : "EUCAP Sahel Mali est composée à ce jour de 110 internationaux, issus de 15 Etats membres de l'Union européenne et de ces 3 Etats-tiers, et de 50 personnels maliens sur contrat local"<sup>7</sup>

A partir du 23 mars 2016, sur la base d'un accord signé entre l'UE et la Suisse, cette dernière sera donc... sous pavillon européen, pendant toute la période de sa participation à la mission Eucap Sahel ! Si la Suisse participe aux opérations européennes au Mali depuis

---

<sup>7</sup> Source Europa.

2013, force est de constater que sa neutralité constitutionnelle ne lui interdit donc pas de participer à la mission EUTM Mali pour contribuer à la formation des forces armées maliennes depuis le 15 avril 2014<sup>8</sup>, participation prorogée par un nouvel accord le 23 mars 2016, fondé sur la double base juridique des articles 37 TUE et 218 TFUE<sup>9</sup>.

La démarche de participer aux OPEX sous drapeau européen étant libre de toute contrainte, cette dernière a accepté dans un premier temps d'appliquer sans condition certaines des règles de l'Union européenne dans une dizaine de situations, de l'article 5 de l'accord UE/Suisse de 2016 :

1. Ainsi le §5 de l'accord permet à la Suisse d'imposer à son personnel auprès de la mission d'exercer sa mission et d'agir "*en ayant uniquement à l'esprit l'intérêt d'EUCAP Mali*" (§5 de l'accord) ;
2. comme beaucoup d'Etats membres la Suisse a souhaité que son personnel participant à la mission " relève de sa juridiction" (art. 2) ;
3. il lui appartient de répondre à toute plainte liée à la mission qui émanerait d'un membre de son personnel ou qui la concerne ;
4. elle doit tenter toute action notamment juridique ou disciplinaire à l'encontre de son personnel s'il y a lieu ;
5. elle renonce à présenter des demandes d'indemnités, autres que des demandes contractuelles, "en cas de dommage, de perte ou de destruction de biens appartenant à l'une ou l'autre partie ou utilisés par elles, résultant de l'accomplissement de leurs tâches en liaison avec les activités menées au titre du présent accord"..., sauf en cas de négligence grave ou de faute intentionnelle !
6. elle doit déclarer renoncer aux demandes d'indemnités à l'encontre de tout Etat participant lors de la signature de l'accord sur la base de la réciprocité des Etats membres ;
7. elle applique les règles et procédure de sécurité pour l'échange d'informations classifiées ;
8. Les autorités nationales transfèrent le contrôle opérationnel de leur personnel au commandant d'opérations civiles de l'Union européenne. (Art. 4 §2)
9. elle reconnaît que le commandant d'opérations civiles de l'Union européenne est responsable de l'EUCAP Sahel Mali et en exerce le commandement et le contrôle au niveau stratégique. (art. 4 §3) et que "le chef de mission est responsable de l'EUCAP Sahel Mali et en exerce le commandement et le contrôle" (art. 4§4) ;
11. Le chef de mission dirige l'EUCAP Sahel Mali et en assure la gestion quotidienne. (art. 4§5) ;
10. La Confédération Suisse a les mêmes droits et obligations en matière de gestion quotidienne de la mission que les États membres de l'Union qui y participent, conformément aux instruments juridiques visés à l'article 1 (art. 4 §6) ;
11. La Confédération Suisse désigne un point de contact des contingents nationaux (PCN) pour représenter son contingent national au sein de l'EUCAP Sahel Mali.

---

<sup>8</sup> - Décision 2014/293/PESC du Conseil du 15 avril 2014 relative à la signature et à la conclusion de l'accord entre l'Union européenne et la Confédération Suisse relatif à la participation de la Confédération Suisse à la mission militaire de l'Union européenne visant à contribuer à la formation des forces armées maliennes (EUTM Mali), JOUE L 151/16 du 21.5.2014.

<sup>9</sup> Décision (PESC) 2016/612 du Conseil du 23 mars 2016 relative à la signature et à la conclusion de l'accord de participation entre l'Union européenne et la Confédération suisse relatif à la participation de la Confédération suisse à la mission PSDC de l'Union européenne au Mali (EUCAP Sahel Mali), JOUE L 105/1 du 21.4.2016 ; Décision (PESC) 2015/610 du Comité politique et de sécurité du 15 avril 2015 prorogeant le mandat du chef de la mission PSDC de l'Union européenne au Mali (EUCAP Sahel Mali/2/2015) JOUE L 101, 18.4.2015, p. 60.

**2. Mais la Suisse ne serait plus la Suisse si on n'assistait pas à l'expression de la cristallisation de sa neutralité** : Aussi a-t-elle su négocier une mise en œuvre de l'accord qui tienne compte de sa neutralité. Dans le cadre d'un accord UE-Etats tiers participants, force est de constater que les règles classiques appliquées depuis la création de la PSDC ne sont pas appliquées intégralement à la Suisse, qui a construit un modèle de participation protégeant au maximum sa souveraineté et surtout sa neutralité. Ainsi, nombreuses sont les situations où le droit commun de la PSDC ne lui est pas applicable. Dans ce cas, les dérogations font primer le droit constitutionnel suisse sur le droit de l'Union européenne : tel est le cas dans l'accord du 23 mars 2016 en vertu duquel elle n'applique pas le droit de la PSDC classique : si les hypothèses sont moins nombreuses que les précédentes elles sont toutes aussi importantes, tant sur le plan symbolique que politique.

2.1. A la différence des Etats membres, le personnel suisse participant à EUCAP Sahel Mali reste entièrement sous le commandement de ses autorités nationales (art. 4 §1) ; ce principe dérogatoire demeure néanmoins assez classique dans le cadre des accords UE et Etats tiers. A titre d'exemple on peut citer l'accord avec le Monténégro du 16 mars 2010 pour sa participation en Somalie à l'opération militaire ATALANTA. Dans la définition de la chaîne de commandement la règle était également inscrite selon laquelle les membres des forces restaient sous le commandement de leurs autorités nationales (art. 5 de la décision du 16 mars 2010)<sup>10</sup>. Ce n'est donc pas à proprement parler une exception à l'application "du droit commun d'une participation des Etats tiers" à une OPEX.

2.2. Sans remettre en cause le principe de la responsabilité du contrôle disciplinaire dans le champ de compétence du chef de mission, la Suisse a exigé que les mesures disciplinaires éventuelles demeurent du ressort de la compétence nationale suisse (Art. 4 §7) ; là encore c'est une règle assez généralisée auprès des Etats tiers qui veulent garder la maîtrise des sanctions comme élément d'expression de leur souveraineté.

2.3. Elle doit être consultée préalablement si l'Union européenne prend la décision de mettre fin à l'EUCAP Sahel Mali, si et seulement si, la Suisse apporte encore une contribution à l'EUCAP Sahel Mali à la date à laquelle l'EUCAP Sahel Mali prend fin. La même consultation est requise par le Commandant de la mission qui peut, à tout moment demander le retrait de sa contribution.

2.4. Sur le plan financier, elle n'est pas soumise au processus du partage des coûts communs d'ATHÉNA : elle assume tous les coûts liés à sa participation à l'EUCAP Sahel Mali, sans préjudice. L'Union européenne a d'ailleurs exempté la Confédération suisse de toute participation financière au budget opérationnel de l'EUCAP Sahel Mali.

2.5. En cas de décès, de blessure, de perte ou de dommage causés à des personnes physiques ou morales du ou des États dans lesquels la mission est menée, la Confédération suisse verse des indemnités, lorsque sa responsabilité a été établie, selon les conditions prévues dans l'accord relatif au statut de la mission.

---

<sup>10</sup> Décision du Conseil du 16 mars 2010 relative à la signature et à la conclusion de l'accord entre l'Union européenne et le Monténégro sur la participation du Monténégro à l'opération militaire de l'Union européenne en vue d'une contribution à la dissuasion, à la prévention et à la répression des actes de piraterie et de vols à main armée au large des côtes de la Somalie (opération Atalanta).

2.6. L'accord mentionne "*un principe de non-conformité*" (art 7) qui s'apparente plus à l'obligation de respecter ses obligations conventionnelles. A défaut, l'autre partie a le droit de résilier l'accord moyennant un préavis d'un mois. Ce délai est assez classique dans ce type d'accord (cf. les accords entre l'UE et les Etats tiers participants ex : accord avec le Monténégro art.8. en 2010).

2.7. Le règlement des différends se fait traditionnellement par voie diplomatique (art. 8), mais bien évidemment il n'y a pas ici comme dans les règles de l'Union européenne l'intervention possible en dernier lieu du président de la CJUE. Cette règle se retrouve également dans l'accord avec le Monténégro, art.9.

2.8. Les règles d'entrée en vigueur et de fin sont sensiblement les mêmes à l'exception près selon laquelle l'accord avec la Suisse "*reste en vigueur pendant la durée de la contribution de la Confédération suisse à la mission*" (art. 9§4 de l'accord). Sinon, le respect de la notification mutuelle et la possibilité d'appliquer l'accord à titre provisoire, à compter de sa signature, sont des règles qui ne dérogent pas fondamentalement au droit commun de la PSDC et elles contribuent à renforcer la souplesse du droit.

### **c. L'externalisation de la protection européenne des droits fondamentaux en Somalie**

Deux accords UE avec le Monténégro<sup>11</sup> et la Croatie<sup>12</sup> (avant qu'elle n'adhère à l'UE le 1<sup>er</sup> juillet 2013) sont intéressants en ce qu'ils intègrent une dimension d'externalisation de la Charte des droits fondamentaux en dehors du territoire de l'UE dès 2009. Depuis les premières OPEX, la règle était posée, mais il s'agissait alors d'appliquer la protection effective du procès équitable sur les territoires des Etats africains concernés. On assiste également, avec la situation en Somalie, à un transfert des personnes pour jugement, en dehors des territoires où ont eu lieu leurs arrestations, pour un jugement possible au Monténégro.

Ainsi en Somalie, dès 2010, les forces navales du Monténégro organisent le transfert des personnes soupçonnées d'avoir commis des actes de piraterie ou de vols à main armée dans les eaux territoriales d'un Etat côtier se trouvant dans la zone d'opération d' EUNAVFOR et contrôlent leurs biens saisis, leur traitement et leur transfert en vue de leur jugement. Mais, il ne s'agit pas d'une obligation, puisque le Monténégro peut accepter sur demande de l'EUNAVFOR le transfert des personnes à des fins d'enquêtes et de poursuites.

Lorsqu'elle agit dans le cadre du présent accord, l'EUNAVFOR ne transfère les personnes concernées qu'aux autorités répressives compétentes du Monténégro<sup>13</sup>. La protection effective des droits fondamentaux est détaillée dans l'accord. Il s'agit de vérifier l'exigence de l'interdiction des traitements inhumains et dégradants ; des traitements arbitraires, de la torture de la peine de mort. Sont également mentionnées des obligations

---

<sup>11</sup> Décision du Conseil du 16 mars 2010 relative à la signature et à la conclusion de l'accord entre l'Union européenne et le Monténégro sur la participation du Monténégro à l'opération militaire de l'Union européenne en vue d'une contribution à la dissuasion, à la prévention et à la répression des actes de piraterie et de vols à main armée au large des côtes de la Somalie (opération Atalanta).

<sup>12</sup> Décision 2009/597/PESC du Conseil du 27 juillet 2009 relative à la signature et à l'application provisoire de l'accord entre l'Union européenne et la République de Croatie sur la participation de la République de Croatie à l'opération militaire de l'Union européenne en vue d'une contribution à la dissuasion, à la prévention et à la répression des actes de piraterie et de vols à main armée au large des côtes de la Somalie (opération Atalanta) JO L 202, 4.8.2009, p. 83–83; art. 6 de l'Accord entre l'Union européenne et la République de Croatie du 27 juillet 2009 sur la participation de la République de Croatie à l'opération militaire de l'Union européenne en vue d'une contribution à la dissuasion, à la prévention et à la répression des actes de piraterie et de vols à main armée au large des côtes de la Somalie (opération Atalanta) JO L 202 du 4.8.2009, p. 83–89.

<sup>13</sup> Annexe de l'accord §2.b.



*positives* telles que le droit pour la personne d'être détenue dans des locaux adéquats, d'accéder aux soins, d'observer sa religion, d'accès au juge sans délai sur les questions de légalité de la détention, le jugement dans un délai raisonnable, le respect de la présomption d'innocence et le droit au procès équitable.

Aujourd'hui, le rôle du représentant spécial de l'UE pour les droits de l'Homme est central pour protéger les valeurs de l'UE. M. Eamon GILMORE, nommé représentant spécial de l'Union européenne (RSUE) pour les droits de l'homme jusqu'au 28 février 2021<sup>14</sup>, dispose d'un budget non négligeable pour la période allant du 1<sup>er</sup> mars 2019 au 28 février 2021 de 2 100 270,50 EUR. (art. 5 de la décision). Il doit notamment veiller à la cohérence en vue d'atteindre les objectifs généraux de l'UE et - à ce titre - il doit se coordonner avec les actions des membres de la Commission et avec les autres RSUE (art.11). Il doit surtout pour le sujet qui nous intéresse maintenir des liens étroits avec les chefs ou commandants de missions dans le cadre de la PSDC (art. 6 §2 de la décision du 28 février 2019).

Au final, les accords externes en PSDC allient les avantages de la souplesse et de l'harmonisation des procédures afin de favoriser au mieux la finalité de la mission engagée. Ce panorama que l'on pourrait presque trouver idyllique souffre tout de même d'un sérieux manque de modernité, dans la prise en compte de la place croissante des enjeux de la cyberguerre. Il serait probablement utile de procéder à l'insertion de règles juridiques et éthiques en faveur des nouvelles formes de guerre du futur (II).

## **II. DÉPOUSSIÉRER LES ACCORDS EXTERNES**

Force est de constater que les guerres modernes se font aussi dans le 5<sup>ème</sup> élément opérationnel qu'est le cyberspace. Si le domaine civil a pour une fois une approche normative globale plus avancée que dans le secteur de la défense, cela ne signifie pas un repli de la cyberdéfense (A). Les acteurs de la défense s'interrogent par ailleurs sur l'évolution des tactiques de guerre dans le cyberspace, pour tenir compte de l'arrivée de l'intelligence artificielle. Dans les deux cas les Etats tout comme l'Union européenne ne sont que trop contemplatifs et pas assez offensifs et doivent contribuer davantage à la prise en compte des enjeux juridiques et éthiques des nouvelles formes de conflictualités (B).

### **A. Le retour de l'approche globale dans le domaine civil... une piste pour la défense ?**

L'approche globale développée par l'Union européenne dans le domaine civil est un tournant dans la politique globale de sécurité (a), mais elle demeure encore volontairement absente dans la définition du cadre juridique européen pour la cyberguerre de demain (b).

#### **a. Le précédent de l'approche globale des derniers accords UE avec le Japon et le Canada**

**1. Le précédent des accords UE/ Canada et UE/ Japon : une approche globale de la sécurité.** Du fait de la nécessité aujourd'hui d'encadrer des OPEX ou des missions civiles par l'outil informatique, il est inévitable de protéger nos communications. Alors, au-delà des

---

<sup>14</sup> Décision (PESC) 2019/346 du Conseil du 28 février 2019 portant nomination du représentant spécial de l'Union européenne pour les droits de l'homme, *JOUE* L 62/12 DU 1.3.2019.

règles européennes<sup>15</sup> qui ont harmonisé nos classifications d'échanges, il convient de souligner l'évolution des accords signés par l'UE en matière de sécurité et de défense.

A titre illustratif, prenons l'accord UE / Australie du 22 avril 2015 comme sujet d'étude établissant un cadre pour la participation de l'Australie aux opérations de gestion de crises menées par l'UE. Il reprenait la présentation formelle pour les Etats participants (c'est-à-dire les règles de participation aux coûts communs, l'arrangement *ad hoc* pour les forces australiennes, la prise en charge des plaintes liées aux dommages, le contrôle des informations classifiées, la chaîne de décisions politiques et opérationnelles, les règles de la chaîne de commandement militaire et la participation de l'Australie au mécanisme d'Athéna. Aucune mention spécifique n'est faite au regard de la cybersécurité dans le cadre de l'OPEX. Le sujet demeure régalien et ne semble pas pouvoir être soumis à un quelconque cadre juridique européen. Chaque Etat garde sa propre conception de la cybersécurité/ cyber souveraineté en OPEX.

Deux ans après, l'UE signa un nouvel accord avec l'Australie... pour une durée indéterminée par la décision du 29 décembre 2016. Le titre 2 de cet accord est relatif au dialogue politique et la coopération sur les questions de politique étrangère et de sécurité. Ce titre permet à l'Australie d'affirmer l'existence d'une politique de gestion de crise (art. 5) qui vise à promouvoir la paix et la stabilité internationales et, surtout au regard du sujet qui nous intéresse, à acter la participation de l'Australie à la gestion de crise menée par l'UE (art. 5 §3 de l'accord cadre). Dans un premier temps, en phase avec les développements onusien, l'Australie promeut la lutte contre la prolifération des armes de destructions massives, des armes légères et de petits calibres et autres armes conventionnelles (art. 7). Elle promeut la coopération dans le cadre de la lutte contre le terrorisme, dans le cadre ONU sien, ainsi que la compétence de la Cour Pénale internationale. Mais au regard du sujet qui nous intéresse on retiendra surtout trois articles qui vont faire évoluer le cadre normatif des accords UE / Etat tiers :

\* *l'article 11 : sécurité internationale et cyberspace* tend à développer une culture commune basée sur l'importance accordée à la coopération et les échanges de vues dans le domaine de la sécurité internationale et du cyberspace notamment sur les règles de conduite et l'application du droit international dans le cyberspace. Ainsi, cet accord cadre reconnaît l'importance de l'élaboration de mesures visant à assurer la confiance et le renforcement des capacités ;

\* *l'article 36§2 sur la lutte contre la cybercriminalité* : dans les domaines de la haute technologie du cyberspace, de l'électronique et de la lutte contre les contenus illégaux notamment à caractère terroriste ;

\* *Article. 36§3* permet la reconnaissance de l'importance de la promotion de la convention de Budapest sur la cybercriminalité "*en tant que norme mondiale en matière de lutte contre la cybercriminalité*" ;

\* *l'article 60 qui renforce, a contrario, la protection du secret national* : l'esprit de l'accord étant d'interdire de divulguer des informations qui porteraient atteinte à la sécurité publique, le renseignement, à la défense et aux affaires militaires.

---

<sup>15</sup> Décision du Conseil (2013/488/UE) du 23 septembre 2013 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'Union, JOUE L 274/1 du 15.10.2013.

Il résulte de ces quatre articles une volonté de l'Australie de prendre toutes les mesures requises pour tenir compte des risques de crises cyber dans le domaine civil comme dans celui de la défense. Mais il s'agit surtout d'une posture défensive. Il n'y a pas de positionnement offensif, affiché publiquement au niveau de l'Union européenne, à l'instar de celui déclaré par Mme Florence Parly, lors du Forum international de la cybersécurité, à Paris le 22 janvier 2019.

## **2. L'approche globale de la cybersécurité est également une démarche adoptée par le Japon dans ses relations avec l'UE<sup>16</sup> :**

Dans l'accord de partenariat stratégique entre l'UE et le Japon publié au JO le 24 août 2018 et dont l'entrée en vigueur est effective depuis le 1er janvier 2019, il convient de souligner la prise en compte, par le biais de l'article 36 de l'accord, d'une coopération sur les questions liées au cyberspace. Le Japon a une position politique très ouverte en faveur de l'approfondissement de la coopération d'échanges au sein des enceintes internationales et régionales ; mais il promet aussi la coopération en vue de consolider la capacité des Etats tiers à renforcer leur cybersécurité et à lutter contre la cybercriminalité. Il vise également la lutte contre le terrorisme (art.8), la gestion et l'amélioration de la coordination des réponses en cas de catastrophes et l'action humanitaire (art.12), ou encore la gestion des activités de sécurité au regard de la nécessité de protéger l'espace extra-atmosphérique (art.16). Cette approche globale fondée sur le dialogue international est beaucoup plus délicate à mettre en œuvre dans le domaine de la défense. Aujourd'hui il existe une absence assumée de cadre juridique européen pour la cyberguerre de demain (b).

### **b. L'absence assumée de cadre juridique européen pour la cyberguerre de demain**

Au sein de l'Union européenne depuis près de 3 ans un dialogue institutionnel politique intense s'est développé entre le Parlement européen et le Conseil afin de faire émerger un cadre juridique en faveur de la cybersécurité. Cet accord entre les Etats membres a été trouvé le 20 décembre 2018, il a été enfin approuvé par le Parlement européen le 12 mars 2019 et si la publication de l'Acte de Cybersécurité n'est pas encore faite au jour de notre colloque, c'est une simple question de temps requis pour la traduction dans les 24 langues de l'UE.

Dans ma chronique sur la cybersécurité et l'intelligence artificielle de 2017<sup>17</sup>, j'avais fortement critiqué la version initiale de cette proposition de règlement qui ne sanctuarisait pas le droit de la sécurité et de la défense nationale et proposait, notamment, un cadre de certification des produits de défense qui risquait fort de nous tirer vers le bas, au regard des règles de libre concurrence au sein du marché intérieur applicables aux produits de sécurité et de défense. Le master 2 SEDEFIS étant membre du pôle rennais du pôle d'excellence cyber,

---

<sup>16</sup> Décision UE (2018) 1197 du Conseil du 26 juin 2018 relative à la signature entre l'UE et ses Etats membres d'une part et le Japon d'autre part, *JOUE* L 216/1 du 24.8.2018.

<sup>17</sup> Chronique Anne Camilleri 2017 droit de la cybersécurité et intelligence artificielle, le rejet de la " singularité technologique", *RDUE* 2017 n° 04 PP. 99-143.

j'avais alors écrit aux deux commissions parlementaires pour les alerter sur les risques inhérents d'une définition aux contours larges du droit de la cybersécurité en matière de défense. En juillet 2018, avec le Général Boone nous avons eu l'honneur d'être auditionnés par la commission parlementaire en charge de ce sujet. Nous avons alors confirmé cette urgence d'exclure le secteur régalien de la défense de cette réglementation essentiellement économique que constitue l'acte européen de cybersécurité. Grâce notamment à l'action de l'ANSSI, c'est chose faite avec la mise sous close des secteurs régaliens de la sécurité et de la défense grâce à l'invocabilité des règles relatives à la compétence partagée dans le domaine du cyberspace entre les Etats membres et l'Union européenne<sup>18</sup>. C'est chose faite dans la version finale de l'acte législatif européen sur la cybersécurité, dans la nouvelle définition de l'article 1§1 du texte final qui reconnaît la compétence exclusive des Etats membres en matière de cybersécurité "*dans les domaines de la défense, la sécurité nationale et les activités de l'Etat dans les domaines du droit pénal*". Dans le même esprit, la version finale du règlement ne contient plus de référence à l'obligation, prévue initialement à l'encontre des entreprises, de notifier des informations relatives à des incidents concernant la sécurité publique d'un Etat. Conforme à l'esprit de sa création l'ENISA n'aura aucune compétence dans ces domaines. Si la cybersécurité est depuis longtemps un enjeu tactique important dans la réalisation et le succès de nos OPEX européennes, c'est aussi parce que les États gardent la maîtrise nationale défensive et offensive des techniques des cyberattaques dans le champ des missions globales dans lesquelles l'Union européenne est engagée. Même si la coopération entre les Etats membres est ouverte et forte, l'avantage tactique ne saurait être sous-estimé, comme en témoigne par exemple la déclaration de la ministre de la défense française sur le positionnement officiel d'une cyberdéfense qui se veut désormais offensive<sup>19</sup> !

A titre d'illustration française, dans le même esprit le projet ROS0<sup>20</sup> portant sur le renseignement d'origine ouverte piloté au sein du programme intelligence Campus par la Direction du Renseignement Militaire vise expressément à renforcer les capacités de ce service "dans de nouveaux espaces cyber et spatial afin de tenir compte des nouvelles menaces". La Générale Gervais a souligné que "le support d'Intelligence Campus doit permettre le croisement aussi bien des sciences sociales que des sciences dures pour permettre de répondre aux attentes des opérateurs et utilisateurs finaux" en se tournant vers le monde civil afin de diffuser l'innovation à l'ensemble de la communauté du renseignement". Il s'agit de faire face à ce que la Générale qualifie de la "*massification des données*" en lien avec ARTEMIS projet de la DGA pour la création d'une infrastructure souveraine de stockage.

## **2. La montée en puissance de l'OTAN dans le cyberspace**

En matière de cybersécurité, cette montée en puissance se traduit par une réforme de sa doctrine, par le renforcement de ses partenariats avec des Etats tiers et avec l'Union européenne

### **2.1 La réforme de sa doctrine incluant la cyberdéfense**

---

<sup>18</sup> Anne Cammilleri, chronique annuelle : en 2018, le calcul exaflopique nous fait tourner la tête ! *RDUE* n °2 2019 à paraître dans le numéro de la revue du mois de mai 2019.

<sup>19</sup> Voir en France, discours de Mme Florence Parly, ministre des armées, sur la cyberdéfense, au Forum international de la cybersécurité, à Paris le 22 janvier 2019.

<sup>20</sup> Alban Léger, Nicolas Fiocre, *L'intelligence campus, nouveau vecteur du renseignement militaire*, portail de l'IE, 26 février 2019, <https://portail-ie.fr/short/2083/lintelligence-campus>.

Mais ce focus sur le renforcement des solutions nationales ne saurait signifier une absence de prise en compte de la cybersécurité dans le cadre de nos OPEX. Le positionnement public de l'OTAN est clair : dès le sommet de Lisbonne en 2010, l'OTAN constatait la montée en puissance des cyberattaques et considérait que la lutte constituait une "tache essentielle" de l'Organisation. Mais c'est surtout lors du sommet au Pays de Galles le 5 septembre 2014 que l'OTAN "entérine une politique de cyberdéfense renforcée fondée sur l'indivisibilité de la sécurité des alliés" ; l'organisation consacre les principes de prévention, de détection et de résilience de l'organisation en matière de défense" ainsi que "le principe de solidarité des parties alliées pour protéger les réseaux nationaux et de conclure que "la cyberdéfense relève de la tâche fondamentale de l'OTAN qu'est la défense collective. *Il reviendrait au Conseil de l'Atlantique Nord de décider, au cas par cas, des circonstances d'une invocabilité de l'article 5 à la suite d'une cyberattaque*".

Lors de la déclaration du Sommet de Bruxelles des 11 et 12 juillet 2018 les chefs d'Etat et de Gouvernements ont renforcé leur position en créant, à Varsovie, un poste de secrétaire adjoint au renseignement qui a pour mission le partage d'informations sur les menaces hybrides et le cyberspace. Il s'agit de soutenir une posture globale de dissuasion et de défense du cyberspace. Toutefois, l'organisation souligne que cette mission défensive permettra *"l'utilisation de toutes les gammes de capacités, y compris cyber, pour assurer la dissuasion et la défense et lutter contre l'éventail complet des cybermenaces. Cette cyberésilience est complétée par la possibilité, pour tout Etat membre qui en fait la demande de se voir mettre à disposition les équipes requises pour répondre à des attaques hybrides "* (§20 de la déclaration).

## **2.2. L'élargissement de ses partenariats**

Ce positionnement va au-delà de l'UE puisque l'OTAN mentionne l'initiative de renforcement des capacités de défense et sécurité dans les domaines prioritaires de cyberdéfense avec la Jordanie (§56 de la déclaration 2018).

## **2.3. Le renforcement des liens OTAN -UE**

Au-delà de l'approfondissement des relations de l'OTAN avec des Etats, l'organisation renforce le partenariat avec l'Union européenne en le qualifiant de partenariat *"unique et essentiel"* (§69)... *"pour assurer leur autonomie et intégrité décisionnelle et institutionnelle notamment sur les questions maritimes de cybersécurité et de cyberdéfense, y compris pour la protection des infrastructures critiques, notamment la sécurité énergétique"* (§78 de la déclaration). Par l'ensemble de ces engagements qui témoigne d'une grande ouverture, on voit bien qu'en 2019, la Dame Otanienne du haut de ses 70 ans a bon pied bon œil !

En dernier lieu, il convient d'envisager les conséquences juridiques de l'IA dans la gestion des crises par l'Union européenne et comment les enjeux éthiques peuvent-ils être intégrés dans les accords externes de l'UE (B).

## **B. Les enjeux juridiques et éthiques des nouvelles formes de conflictualités**

Le sujet de la consécration juridique d'un principe international d'interdiction du recours aux armes autonomes est un sujet politiquement sensible tout à fait dans l'actualité. Si le droit positif peine à faire émerger un principe d'interdiction du recours aux armes autonomes dans un conflit armé (a), les premières solutions relèvent plus de l'éthique que du droit (b).

**a. Consacrer l'interdiction du recours aux armes autonomes, un premier pas qu'il reste à codifier.**

Les enjeux juridiques autour de l'arrivée de l'IA dans le domaine civil<sup>21</sup> comme dans celui de la défense sont essentiels pour définir les nouveaux contours de l'art de faire la guerre. L'interdiction du recours aux armes autonomes n'est pas encore une règle juridique du droit international des conflits armés. Les instances onusiennes n'ont pas encore inscrit cette interdiction dans le marbre. Tout au plus, deux résolutions peuvent être citées : d'une part le 15 mars 2018, l'Assemblée parlementaire Euronest réunissant plusieurs parlements - dont le Parlement européen - recommandait "*d'agir en faveur d'une politique plus transparente et responsable en ce qui concerne l'utilisation de robots tueurs dans les zones extraterritoriales*"<sup>22</sup>. D'autre part, le Parlement européen, le 12 mars 2018, condamnait le recours aux systèmes d'armes autonomes<sup>23</sup>. JR Ganascia a souligné l'importance de rejeter la singularité technologique pour laisser l'Humain au centre du dispositif de décision<sup>24</sup>. Son approche appliquée au monde civil peut tout à fait s'exporter dans le monde de la défense et en faveur du droit des conflits armés. "*L'autonomie correspond à une séquence de causalités qui ne fait pas intervenir d'agent humain*". Il considère "*que l'état de développement des technologies en IA n'autorise pas à comprendre comment de tels systèmes d'armes seraient construits et cela ne permet pas non plus d'appréhender la nature de ces systèmes. Bref, la crainte de voir une nouvelle génération de Sala révolutionner la guerre paraît bien peu fondée*"<sup>25</sup>. Sans rentrer ici dans le débat sur l'émergence de nouvelles armes intelligentes autonomes sur la scène internationale, on retiendra que le point vers lequel le monde civil et militaire semblent converger est bien la décision de laisser l'Homme au centre du pouvoir de décision. Certains auteurs proposent même de qualifier de crime de guerre toute action inverse en cas d'utilisation d'un système robotique armé ou encore plaide pour l'interdiction du recours aux essaims de drones<sup>26</sup>. La législation nationale<sup>27</sup> comme européenne<sup>28</sup> en matière de

---

<sup>21</sup> *Intelligence artificielle - État de l'art et perspectives pour la France, étude économique*, Le Pôle interministériel de Prospective et d'Anticipation des Mutations économiques (Pipamea, Février 2019).

<sup>22</sup> Déclaration d'Euronest du 15.3.2018, JOUE C 99/3 5 15.3.2018. cf. extrait du Federal Register / Vol. 83, No. 223 / Monday, November 19, 2018 / Proposed Rules : 2) Artificial intelligence (AI) and machine learning technology, such as: (i) Neural networks and deep learning (e.g., brain modelling, time series ; prediction, classification); (ii) Evolution and genetic computation (e.g., genetic algorithms, genetic programming); (iii) Reinforcement learning; (iv) Computer vision (e.g., object recognition, image understanding).

<sup>23</sup> Parlement Européen, *Résolution sur les systèmes d'armes autonomes (2018/2752(RSP))*, 12 septembre 2018 ([www.europarl.europa.eu/](http://www.europarl.europa.eu/)). "Autonomie des Létalité en robotique militaire", *Les cahiers de la Revue Défense Nationale* 2018 ; Eric Germain, "Trouvez le Sala ! La campagne internationale contre les « robots tueurs » : une décennie et déjà trois histoires", *RDN* 2018, n° 809, P. 256.

<sup>24</sup> Jean-Gabriel GANASCIA, *Le mythe de la singularité technologique, Faut-il craindre l'intelligence artificielle ?* Ed. Le Seuil 2017

<sup>25</sup> Jean-Gabriel GANASCIA, *La révolution de l'Intelligence artificielle (IA) en autonomie*, *RDN* 2018, p. 41.

<sup>26</sup> J.M MOSCHETTA, "Les futurs systèmes de drones, Drone de neutralisation chirurgicale à réponse graduée", *RDN* 2018, n° 809, P. 117.

<sup>27</sup> Loi n° 2016-1428 du 24 octobre 2016 relative au renforcement de la sécurité de l'usage des drones civils *JORF* n°0249 du 25 octobre 2016

<sup>28</sup> Règlement (UE) 2018/1139 du Parlement européen et du Conseil du 4 juillet 2018 concernant des règles communes dans le domaine de l'aviation civile et instituant une Agence de l'Union européenne pour la sécurité aérienne, et modifiant les règlements (CE) n° 2111/2005, (CE) n° 1008/2008, (UE) n° 996/2010, (UE) n° 376/2014 et les directives 2014/30/UE et 2014/53/UE du Parlement européen et du Conseil, et abrogeant les règlements (CE) n° 552/2004 et (CE) n° 216/2008 du Parlement européen et du Conseil ainsi que le règlement (CEE) n° 3922/91 du Conseil *JOUE* L 212, 22.8.2018, p. 1.

drones souligne la prise de conscience de la nécessité de mieux encadrer ces nouveaux instruments qui sont d'ores et déjà mis au service de la protection de la défense nationale. Comme le soulignait Julien Ancelin (lors du dernier colloque de l'AFSD à Bordeaux), "la position française face à l'autonomie des moyens de combat oscille entre détermination et ambiguïté"<sup>29</sup>.

Le chemin à parcourir est donc encore long pour consacrer juridiquement cette interdiction du recours aux armes autonomes. *A fortiori*, sans que cela soit impossible, imposer une clause juridique et éthique sur l'usage des technologies basées sur l'IA dans les accords UE avec des Etats tiers ne sera pas chose aisée. Toutefois, tous les Etats tiers n'en sont pas encore à ce stade de développement technologique. Les accords devront comprendre des règles de l'Union européenne pour autoriser -ou interdire- dans certaines circonstances l'usage des technologies usant des systèmes d'armes autonomes dans le cadre de leurs missions. Le principe d'interdiction devrait être la règle et l'émergence de règles éthiques s'avère urgente (b).

### **b. Quelle éthique faut-il recommander dans le cadre des nouvelles formes de combat.**

L'axiome selon lequel l'Humain doit à tout moment être au centre du pouvoir de décision dans les combats militaires doit être au cœur de toutes les décisions. Pour le reste, les sujets sont encore largement discutés. Ainsi, la revue de défense nationale qui a consacré un numéro spécial sur cette question à la fin de l'année 2018, a permis à des professionnels de la défense d'émettre des avis divers. On retiendra par exemple celui de deux chercheuses qui ont démontré "qu'il n'est pas possible, à l'heure actuelle, d'intégrer un raisonnement éthique et juridique au sein d'un système algorithmique semi-autonome semblable à celui que pourrait tenir un soldat, rendant alors acceptable son usage sur un champ de bataille modernisé. Le principal obstacle à la réalisation d'une machine éthique étant la formalisation de grands principes subjectifs et qualitatifs"<sup>30</sup>.

Je conclurais en vous invitant à deux sources d'informations sur les règles éthiques à retenir : la première est le colloque organisé par l'Université Laval, à Québec sur ces enjeux éthiques réunissant de nombreux chercheurs et professionnels de la défense<sup>31</sup>. Parmi les règles qui sont ressorties avec un certain consensus on en retiendra une essentielle : l'agilité ! Parce que l'agilité est en enjeu éthique et tactique dans le domaine militaire<sup>32</sup> (voir par exemple l'intégration des outils de cybersécurité dans la marine française pour prendre en compte la menace cyber dans son paysage stratégique présentée à Euronaval 2018). La seconde source est européenne avec l'édiction de neuf règles retenues par le Comité d'Experts sur l'IA auprès de la Commission européenne. A la lecture de leur énoncé, force est de constater que ces dernières sont pour l'essentiel d'entre elles surtout des juridiques ! Ainsi, on retiendra l'attachement de l'Union européenne à la protection à la démocratie et à l'état de droit<sup>33</sup>, à la

---

<sup>29</sup> Julien ANCELIN, "La position française face à l'autonomie des moyens de combat : entre détermination, et ambiguïté", Université de Bordeaux, Ministère des Armées. A paraître in revue de l'*Annuaire du droit de la Sécurité et de la Défense* n° 1, 2019, Mare et Martin.

<sup>30</sup> Adeline AUFFRET et Tatiana KOZLOVSKY, "Dilemmes éthiques militaires : du langage juridique et des principes éthiques au langage informatique", *ENS Rennes, RDN* 2018 .P. 193.

<sup>31</sup> Gagner la guerre du futur : considérations juridiques et éthiques sur l'intelligence artificielle. rev. Les cahiers de Propriété intellectuelle canadienne, n° spécial octobre 2018 intelligence artificielle, vol.30 n°3, PP.769-687, Ed. Yvon Blais, 2018.

<sup>32</sup> A. Cammilleri, "Considérations juridiques et éthiques sur la cybersécurité internationale", *Rev. des cahiers canadiens de propriété intellectuelle*, n°octobre 2018, pp.767-788 ; J. Masclure et MN Saint Pierre, "Le nouvel âge de l'intelligence artificielle : une synthèse des enjeux éthiques", *même revue* pp. 741-766.

<sup>33</sup> Voir en ce sens l'avis du CEPD, Giovanni BUTTARELLI, visant notamment la menace que constitue la manipulation en ligne au regard de la protection des données à caractère personnel en raison de l'augmentation

justice, à l'équité et à la solidarité, à la sécurité, la sûreté. L'Union européenne retient également l'intégrité physique et mentale, la dignité humaine, la protection des données et de la vie privée. Dans une logique de protection des enjeux environnementaux, sont également visés l'usage responsable des nouvelles technologies conforme au développement social et environnemental et à la durabilité et la protection de la planète afin d'assurer la prospérité continue de l'humanité et à la préservation d'un environnement convenable pour les générations futures.

Si la démarche est évidemment louable et utile, l'analyse des principes retenus montre, sans ambiguïté, que plusieurs principes énoncés, s'ils ont une finalité éthique clairement exprimée sont essentiellement des principes juridiques consacrés tant par des règlements européens du type du règlement général sur la protection des données que par le droit interne des Etats membres<sup>34</sup>. Certains évoquent la nécessité d'une retenue éthique. Comme je l'écrivais dans ma chronique sur la cybersécurité et sur l'intelligence artificielle<sup>35</sup>, comment ne pas citer ici l'académicien Pierre Delvolvé qui, au sujet des usages technologiques, fit l'éloge de deux grands principes " *l'un propre à la science : celui de l'intégrité scientifique, l'autre, qui dépasse la science mais s'y applique : celui de la dignité humaine*"<sup>36</sup>. L'intelligence artificielle n'échappera pas à cette règle. Aujourd'hui, c'est le combat de l'innovation et de la raison contre l'arbitraire et la déshumanisation, qui se joue, à l'échelle planétaire !

---

du nombre de personnes et d'objets connectés à l'internet et de l'importance croissante des systèmes d'intelligence artificielle. Résumé de l'avis du contrôleur européen de la protection des données sur la manipulation en ligne et les données à caractère personnel, *JOUE C 233/8* du 4.7.2018.

<sup>34</sup> ex français : de l'intelligence artificielle à l'intelligence juridique, mettre les progrès technologiques au service des métiers du droit, Lexis Nexis, 2018 et bien sur le rapport Villani, *Donner un sens à intelligence artificielle*, mars 2018, précité dans la chronique de 2017. Pour les initiatives proches en Allemagne et en Finlande, cf. Communication de la Commission p.21§3.1

<sup>35</sup> Anne Cammilleri, à paraître Chronique de cybersécurité et sur l'intelligence artificielle, *RDUE* n°2, mai 2019.

<sup>36</sup> Pierre Delvolvé, "L'encadrement normatif de la science", *RFDA* 2018. 487.