L'armée française et la cyberguerre

par Jean-Christophe VIDELIN

Maître de conférences de droit public (HDR)
à l'Université de Grenoble-Alpes, GRDPE

Dans un environnement particulièrement instable et porteur de menaces protéiformes, le format des armées, notamment celle de la France, est source de réflexion. Deux menaces sont, à ce titre, porteuses de transformations potentielles : le terrorisme et la cyberattaque. Ces deux menaces présentent des points communs. C'est une menace qu'un faible[1] peut exercer sur le fort, transnationale, peu onéreuse et difficilement maîtrisable mais qui nécessite pour les États d'importants moyens humains et techniques pour y faire face. La France a pris la mesure du risque depuis plusieurs années[2] au point d'être considérée par les Nations Unies, en juillet 2017, comme l'un des dix pays les plus impliquées dans la cybersécurité[3].

Au préalable, la définition de la cyberattaque d'ordre militaire doit être arrêtée. De manière générale, c'est l'usage volontairement malveillant du cyberespace, le réseau maillé des infrastructures des technologies de l'information (dont Internet), des réseaux de télécommunication, des systèmes informatiques, des processeurs et des mécanismes de contrôle intégrés ainsi que de leurs opérateurs. Ce fut le cas avec l'attaque numérique contre le réseau administratif et bancaire de l'Estonie en 2007 ou le rançonnage numérique en 2017 contre des entreprises et des hôpitaux. Ces derniers ne pouvaient reprendre contrôle de leur service numérique que contre le versement d'une somme d'argent. La cyberattaque va concerner des attaques qui ont un impact dans l'activité militaire (opération, infrastructure, recherche) : cyberattaques contre le réseau informatique gérant les centrifugeuses du programme iranien nucléaire ou contre le réseau informatique géorgien avant l'intervention russe. La frontière n'est cependant

1. Les États peuvent également l'utiliser en raison de son faible coût et de la quasi-impossibilité à en identifier l'instigateur.
2. Jean-Marie Bockel, « La cyberdéfense », *RDN*, n° 751, juin 2012, p. 27.
3. *Half of all countries aware but lacking national plan on cybersecurity*, UN News Centre (site internet), 5 juil. 2017.

pas toujours claire. Ainsi, la stratégie de la Russie[4] de véhiculer via des réseaux sociaux de fausses informations dans l'élection présidentielle américaine[5] ou dans le référendum sur le retrait du Royaume-Uni des traités sur l'Union européenne[6] peut apparaître comme une cyberattaque quasi-militaire puisqu'elle porte atteinte au fonctionnement normal des institutions des États[7]. Elle constitue « une atteinte à sa souveraineté et à son indépendance », comme l'avait précisé à l'Assemblée nationale Jean-Marc Ayrault, le ministre des affaires étrangères[8].

En réponse, la cybersécurité militaire et civile constitue un ensemble des moyens techniques ou non afin d'intervenir dans le cyberespace pour garantir le fonctionnement des services jugés essentiels (défense, sécurité intérieur, transport, santé, finance). En France, une stratégie nationale en matière de cybersécurité a été arrêtée en 2015[9] sous l'autorité du Premier ministre. En matière de cybersécurité civile, la France a agi rapidement en créant au sein du Secrétariat général de la défense et de la sécurité nationale (SGDSN), l'Agence nationale de sécurité des systèmes d'informations (ANSSI). Ces compétences se sont étendues et renforcées progressivement (C. déf., L. 2312-1 et s.). En matière de cybersécurité militaire, l'effort a été plus progressif. L'armée s'est elle-même saisie de cet enjeu, puis celui-ci a été formalisé dans le Livre blanc de la défense et de la sécurité nationale de 2013[10] et consolidé avec la loi de programmation militaire 2014-2019[11]. Les avancées sont rapides d'un point de vue doctrinale et institutionnelle.

Pour autant la dimension immatérielle et transnationale des cyberattaques impose, tout comme l'ensemble de l'action militaire française, de respecter le droit international public. En 2013, le groupe des experts gouvernementaux constitué au sein de l'organisation des Nations unies a considéré que le droit international public est applicable au cyberespace. Les difficultés sont néanmoins nombreuses[12]. De manière générale, culturellement et

4. V. Les guerres informationnelles du Kremlin, *Le Monde*, 13 au 18 mars 2017.
5. Martin Untersinger, « Entre les États-Unis et la Russie, des relents de guerre froide dans le cyberespace », *Le Monde*, 14 octobre 2016.
6. Philippe Bernard, « Moscou accusé d'avoir interféré dans le référendum sur le Brexit », *Le Monde*, 16 novembre 2017, p. 2.
7. Martin Untersinger, « La France menace de "mesures de rétorsion" tout État qui interférerait dans l'élection », *Le Monde*, 2 mars 2017.
8. Nathalie Guibert, « La démocratie, nouvelle cible de la cyberguerre », *Le Monde*, 20 février 2017.
9. La *Stratégie nationale pour la sécurité du numérique* a été présentée le 16 octobre 2015 par le Premier ministre Manuel Valls. La France se donnera notamment les moyens de défendre ses intérêts fondamentaux dans le cyberespace. Elle consolidera la sécurité numérique de ses infrastructures critiques et œuvrera pour celle de ses opérateurs essentiels à l'économie.
10. *Livre blanc sur la défense et la sécurité nationale*, Paris, Doc. fr., 2013, 162 p., spéc., p. 105 s.
11. Loi n° 2013-1168 du 18 décembre 2013 *relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale* (*JORF*, 19 décembre 2013, p. 20570).
12. V. Karine Bannelier, Théodore Christakis, « Cyberattaques - Préventions-réactions : rôle des États et des acteurs privés », *Les cahiers de la Revue défense nationale*, 2017, 90 p.

juridiquement, le cyberespace est un espace de liberté, exploité et développé par des groupes (américains) très puissants. Plus spécifiquement, la cyberattaque est le plus souvent non localisable. Il suffit d'ordinateurs relais, pour brouiller davantage l'origine de l'attaque. Le cyberespace, de l'aveu de l'ambassadeur français en charge de la cyberdiplomatie, « *ressemble au Far West : le droit est applicable, mais il est peu appliqué, tout le monde agit ou peut agir de manière offensive, et il n'y a pas grand-chose pour brider les intentions malveillantes* » [13].

La question est donc de savoir si l'armée française est pleinement libre dans ses moyens d'action agressive et défensive en matière de cyberdéfense. La doctrine s'entend déjà pour considérer que des interprétations extensives du droit international public peuvent amener à conclure que les cyberattaques notamment d'ordre militaire constituent une atteinte au droit de la sécurité internationale[14]. En effet, l'article 2, paragraphe 4, de la Charte des Nations Unies dispose que « *[l]es membres de l'Organisation s'abstiennent, dans leurs relations internationales, de recourir à la menace ou à l'emploi de la force, soit contre l'intégrité territoriale ou l'indépendance politique de tout État, soit de toute autre manière incompatible avec les buts des Nations Unies* ». Ce point est central car il ouvre la voie à un droit à la légitime défense prévue à l'article 51 de la charte de l'organisation des Nations unies.

Le ministère américain de la Justice en 1999 avait initialement exprimé des doutes[15]. La question porte évidemment sur le sens à donner au terme « *force* ». La Cour internationale de Justice (CIJ) n'a jamais eu l'occasion de statuer sur cette question mais sa jurisprudence permet de penser que la cyberattaque constitue une agression armée puisque dans son avis consultatif du 8 juillet 1996 portant sur la licéité de la menace ou de l'emploi des armes nucléaires, la CIJ a rappelé que la « *force* » n'est pas définie dans la charte des Nations Unies et que son interdiction ne se limite pas à des armes particulières. L'informatique est une arme dès lors qu'elle a pour objet de porter atteinte au fonctionnement de services, ce qui peut avoir des conséquences notamment sur les réseaux informatiques utilisées par les armées[16]. C'est également l'emploi massif du cyberespace par l'État islamique qui a confirmé la France dans sa politique d'accélérations des efforts budgétaires et diplomatiques à conduire pour y faire face, annoncées dès l'actualisation de la loi de programmation militaire en juillet 2015[17].

---

13. V. Loïc Simonet, « L'usage de la force dans le cyberespace et le droit international », *RDN*, n° 751, juin 2012, p. 51.
14. *Ibid*.
15. *Ibid*.
16. V. pour une analyse plus étendue, Loïc Simonet, *ibid*.
17. « Cette posture sera complétée par le dispositif de cyberdéfense militaire renforcé, qui fera l'objet d'un effort marqué sur la période de programmation, en relation étroite avec le domaine du renseignement. La France développera une organisation de cyberdéfense étroitement intégrée aux forces, disposant de capacités défensives et offensives pour préparer ou accompagner les opérations militaires. L'organisation opérationnelle des armées intégrera ainsi une chaîne opérationnelle de cyberdéfense, cohérente avec l'organisation et la structure opérationnelles de nos armées et adaptée aux caractéristiques propres à cet espace de

Ce faisant, la cyberattaque emportait le besoin de repenser l'armée (**I**) et exigeait également une internationalisation de la cyberdéfense (**II**).

I. Cyberdéfense, une armée repensée

L'armée a été repensée de deux manières : l'une concernant les modalités opérationnelles des actions militaires (**A**), l'autre à propos de l'organisation institutionnelle (**B**).

A. Une approche opérationnelle enrichie

Le ministre de la défense, alors Jean-Yves Le Drian, affirmait en 2015 que « *le premier enjeu, pour nos forces armées, est désormais d'intégrer le combat numérique y compris de manière offensive ce qui constitue leur principale faiblesse, [c]e nouveau milieu est devenu un domaine militaire à part entière, dans lequel il faut positionner ses forces, défendre sa puissance et y exploiter toutes les occasions pour vaincre l'adversaire* » [18]. L'action est triple mais une limite apparaît.

En premier lieu, la priorité reste, pour chacun des pays, la défense de ses installations souveraines. La protection des réseaux de communication militaires et celle des systèmes d'armes de plus en plus connectés embarqués sur les bateaux, avions et autres blindés est impératif. La rénovation du porte-avions Charles de Gaulle et notamment le changement complet du centre de commandement opérationnel du bâtiment est pensé dans ce sens[19].

En deuxième lieu, l'officier général en charge de la cyberdéfense expliquait plus récemment que du renseignement aux frappes, toutes les opérations menées contre l'EI sont doublées d'un volet « cyber ». Les ordinateurs de l'EI sont attaqués avant que les avions de chasse ne bombardent ses installations.

C'est pour cette raison que Le Centre de préparation et de conduite des opérations (CPCO) intègre un centre de conduite des opérations informatiques au côté des autres armes : Le général Didier Castres, alors sous-chef opérations à l'état-major des armées, a indiqué qu'« *Il faut intégrer ab initio la dimension numérique à tous nos travaux de planification militaire* »

---

confrontation: unifiée, pour tenir compte de l'affaiblissement de la notion de frontière dans cet espace; centralisée au sein du centre de planification et de conduite des opérations de l'état-major des armées, pour garantir une vision globale et une mobilisation rapide des moyens nécessaires; et spécialisée, car faisant appel à des compétences et des comportements spécialement adaptés ». Loi nº 2015-917 du 28 juillet 2015 *actualisant la programmation militaire pour les années 2015 à 2019 et portant diverses dispositions concernant la défense*, (*JORF*, 29 juil. 2015, texte n° 1).

18. Nathalie Guibert, « La France revendique sa place dans la cyberguerre offensive », *Le Monde*, 25 sept. 2015.

19. Dominique Gallois, « Porte-avions "Charles-de-Gaulle" : une rénovation à 1,3 milliard d'euros », *Le Monde éco.*, 12 juin 2017.

des opérations[20]. Par ailleurs, une compagnie de combat d'environ 700 hommes, déployables dans les opérations extérieures, sera prête en 2018. Les armées considèrent que l'arme informatique doit « *apporter un appui* » aux forces conventionnelles : « *C'est une nouvelle forme de frappe dans la profondeur, aux effets qui peuvent être considérables »*, a précisé Jean-Yves Le Drian, qui a ajouté que « *c'est aussi une forme d'appui tactique aux combattants, par exemple pour perturber les défenses antiaériennes en leurrant ou en neutralisant des systèmes radars. Certains l'ont déjà fait.* » Au final, l'objectif de neutraliser « *y compris de façon permanente* » contre « *des infrastructures matérielles ou immatérielles* » [21].

En troisième et dernier lieu, le spectre de la cyberdéfense est étendu à l'action psychologique, qui a pris une forme complétement nouvelle en raison des réseaux sociaux. Ainsi, le commandement cyber compte des officiers spécialisés dans la contre-propagande afin de protéger les troupes sur le terrain et de contrer la propagande de Daech. Le général Didier Castres a indiqué que dans la seule sphère francophone, étaient recensés, en 2015, 2 370 sites Internet pro-Daech, 41 000 tweets quotidiens et 3 millions de followers.

Une limite existe, qui rappelle les enjeux d'un rapprochement éventuel sur les missions des forces spéciales et les actions clandestines, y compris numériques[22] : la distinction entre le rôle des armées et de la DGSE. La France n'a pas les moyens des États-Unis et la séparation des activités de cyberdéfense entre des services du ministère de la défense peut interroger. Certaines activités sont en effet communes. Certes, le volet offensif au sens large – interceptions et pénétrations de réseaux informatiques étrangers, collecte de masse, surveillance – demeure le domaine de la DGSE, qui dispose de l'outil technique. La lutte offensive venant en appui des opérations militaires menées par la France sur le terrain, en Irak ou au Sahel, relève, elle, de l'état-major des armées. Du ciblage à la contre-propagande, la lutte informatique est désormais intégrée à toutes les opérations militaires, au premier chef celles menées contre l'organisation État islamique. La réunion des moyens techniques pourrait présenter une utilité certaine. Les hésitations sont néanmoins manifestes, tout comme cela s'est traduit en termes de réorganisation institutionnelle.

---

20. Cité *in* Nathalie Guibert, *loc. cit*.
21. « *En temps de guerre, l'arme cyber pourra être la réponse, ou une partie de la réponse, à une agression armée, qu'elle soit de nature cyber ou non, a expliqué le ministre, en détaillant la doctrine française. Nos capacités cyber-offensives doivent donc nous permettre de nous introduire dans les systèmes ou les réseaux de nos ennemis, afin d'y causer des dommages, des interruptions de service ou des neutralisations temporaires ou définitives, justifiées par l'ouverture d'hostilité à notre encontre. En utilisant pour cela des moyens sophistiqués, dont nous sommes parfois les concepteurs, et qui doivent résister à tout risque de détournement*. », cité *in* Nathalie Guibert, « La France revendique sa place dans la cyberguerre offensive », *Le Monde*, 25 sept. 2015.
22. Daniel Reiner, Jacques Gautier, Gérard Larcher, *Le renforcement des forces spéciales françaises, avenir de la guerre ou conséquence de la crise ?,* Sénat, Rapport d'information n° 525, 13 mai 2014, 82 p.

B. Une réorganisation institutionnelle limitée

Les cyberattaques deviennent un enjeu de souveraineté étatique dont un des aspects relève du champ militaire. Sa nature même – l'immatérialité – interdit une catégorisation organique telle qu'elle peut exister entre les armées de terre, de l'air et de la marine nationale. Elle impose ainsi une transversalité organique qui se traduit, au sein des armées, par une organisation interarmées. Cette transversalité s'est manifestée dans le secteur civil dès 2009 avec la création de l'Agence nationale de sécurité des systèmes d'information (ANSSI), qui relève du secrétariat général de la défense et de la sécurité nationale (SGDSN). Le périmètre de l'agence est indiscutablement interministériel. Elle assure en effet une double mission : une d'autorité de sécurité, qui se décompose en opérations de sensibilisations aux menaces et en opérations de prévention ; une autre d'autorité de défense qui implique de répondre aux attaques et de contribuer à la reprise de l'activité normale des systèmes d'information.

Dans le domaine militaire, la prise de conscience a lieu au même moment et ne se traduit pas immédiatement par des conséquences organiques significatives.

Dans un premier temps, en 2011, le ministère de la défense arrête une doctrine en matière de cyberdéfense et se dote dès l'année suivante d'une structure interarmées, placée sous l'autorité du chef d'état-major des armées, portée essentiellement sur une dimension opérationnelle et de gestion de crise. 80 personnes y sont affectées. En sus, une chaire de cyberdéfense à vocation interarmées a été inaugurée au mois de juillet 2012 au sein des écoles de Saint-Cyr Coëtquidan[23]. Puis début 2014, le ministère avait indiqué qu'une enveloppe de 1 milliard d'euros serait consacrée à la nouvelle arme « *cyber* » dans les cinq ans, dont 500 millions d'investissements industriels et technologiques, soit un triplement de l'effort pour ce domaine qualifié de « *priorité nationale* ». Confortée par les orientations de l'actualisation de la loi de programmation militaire en juillet 2015, la France avait pour la première fois revendiqué sa place dans la lutte informatique offensive, lors d'une réunion de cyber-commandeurs alliés à l'École militaire.

Toutefois, ces évolutions et l'importance croissance de la cyberdéfense incitent le ministère de la défense et l'État-major des armées à faire évoluer de manière plus significative l'organisation institutionnelle. Il est vrai que la structure à vocation strictement opérationnelle n'est plus le bon périmètre ; elle doit s'étendre à l'ensemble du spectre militaire : planification, ressources humaines, expertise, recherche, relations internationales en sus donc de l'opérationnel.

Ainsi, dans un second temps, en mai 2017, l'armée française consolide son commandement cyber par la création d'un véritable commandement

23. Arnaud Coustillière, « La cyberdéfense : un enjeu global et une priorité stratégique pour le ministère de la défense », *Sécurité globale*, 2013/1 (n° 23), p. 27-32.

interarmées, le « *Comcyber* ». Au préalable, le chef d'état-major des armées voit ses attributions étendues à la conduite de la défense des systèmes d'information du ministère de la défense (C. déf., art. R. 3121-2 8°). Il coordonne son action avec l'autorité nationale de défense des systèmes d'information, en d'autres termes le directeur de l'ANSSI. Ensuite, le gouvernement a fait le choix de créer un commandement interarmées de cyberdéfense[24]. Il répond aux trois critères fixés à l'article R. 3211-1 du code de la défense : La mission principale s'exerce au profit de plusieurs armées, directions ou services de soutien ou de la gendarmerie nationale ; il relève organiquement du chef d'état-major des armées ; le personnel est issu d'au moins deux armées, directions ou services de soutien ou de la gendarmerie nationale.

A l'image du « *Cybercom* » américain, le nouvel état-major coiffe toutes les unités opérationnelles informatiques des armées et des services de la défense, soit 2 600 personnes au total. L'avancée institutionnelle n'est pas uniquement symbolique. Il existe en effet un seul autre commandement interarmées, celui de l'espace[25]. Mais le *Comcyber* est hiérarchiquement plus élevé. Le commandant Espace n'a pas bénéficié d'une reconnaissance par son intégration dans le code de la défense car il est hiérarchiquement placé sous l'autorité d'un sous-chef d'état-major, lui-même placé sous celle du major général de l'état-major des armées alors que l'officier général commandant le *Comcyber* est, comme l'officier général « relations internationales militaires » directement placé sous celle de ce dernier[26].

Au titre des articles D. 3121-24-2 et R. 3121-2 du code de la défense, l'officier général « *commandant de la cyberdéfense* » assiste et conseille le ministre de la défense dans son domaine de compétences[27]. Ses attributions sont amples mais connaissent une double limite[28]. L'officier général *« commandant de la cyberdéfense »* a en effet la charge de la protection des systèmes d'information placés sous la responsabilité du chef d'état-major des armées et de la conduite de la défense des systèmes d'information du ministère de la défense et de la conception, de la planification et de la conduite

---

24. V. Arrêté du 4 mai 2017 *modifiant l'organisation de l'état-major des armées* (*JORF*, 5 mai 2017, texte n° 87). V. égal. N. Guibert, « L'armée française consolide son commandement cyber », *Le Monde*, 13 déc. 2016.

25. Arrêté mod. du 7 juillet 2010 *portant création du commandement interarmées de l'espace et modifiant l'arrêté du 16 février 2010 portant organisation de l'état-major des armées et fixant la liste des autorités et organismes directement subordonnés au chef d'état-major des armées* (*JORF*, 17 juillet 2010, texte n° 32) et Instr. n°294/DEF/EMA/CIE *relative à l'organisation et aux principes de fonctionnement du commandement interarmées de l'espace* du 15 septembre 2015, BOA, n° 52, 26 nov. 2015. Il a existé entre 2009 et 2013 un commandement interarmées des hélicoptères.

26. Arrêté mod. du 20 mars 2015 *portant organisation de l'état-major des armées et fixant la liste des commandements, services et organismes relevant du chef d'état-major des armées ou de l'état-major des armées* (*JORF*, 4 avril 2015, texte n° 32).

27. Décret n° 2017-743 du 4 mai 2017 *relatif aux attributions du chef d'état-major des armées* (*JORF*, 5 mai 2017, texte n° 78) ; Arrêté du 4 mai 2017 *modifiant l'organisation de l'état-major des armées* (*JORF*, 5 mai 2017, texte n° 87).

28. Arrêté du 4 mai 2017 *modifiant l'organisation de l'état-major des armées*, art. 19 (*JORF*, 5 mai 2017, texte n° 87).

des opérations militaires de cyberdéfense, sous l'autorité du sous-chef d'état-major « *opérations* ». Il contribue à l'élaboration de la politique des ressources humaines de cyberdéfense et coordonne la contribution des armées et organismes interarmées à la politique nationale et internationale de cyberdéfense, notamment pour l'élaboration et la mise en œuvre des plans de coopération. Il contribue à la définition des besoins techniques spécifiques de cyberdéfense. Il assure la cohérence du modèle de cyberdéfense du ministère et sa coordination générale développe et anime la réserve de la cyberdéfense. Pour l'exercice de ses attributions, l'officier général « *commandant de la cyberdéfense* » s'appuie sur des unités spécialisées en cyberdéfense appartenant aux armées et aux organismes interarmées, sur lesquelles il exerce une autorité fonctionnelle.

Cette configuration concourt au renforcement de l'interarmérisation. Les 600 spécialistes, ingénieurs et techniciens de la Direction générale pour l'armement (DGA) s'y ajouteront. Le *Comcyber* français couvrira quatre pôles : la protection des réseaux informatiques des armées, la défense, avec le Centre d'analyse de lutte informatique défensive, les opérations offensives et de renseignement et la réserve. D'ici à 2019, les forces cyber doivent disposer en plus du renfort de 4 400 réservistes.

Cette évolution importante ne va pas au-delà : la constitution d'une quatrième armée est rejetée. Ce rejet est justifié par le chef d'état-major des armées, alors Pierre de Villiers, en faisant référence aux forces spéciales qui, un temps, avaient été envisagées comme une quatrième armée : « *Pourquoi ne faut-il pas de quatrième armée de cyberdéfense ? La raison est simple : une armée, c'est une culture dans un milieu. Les unités des forces spéciales – les commandos marine, les commandos parachutistes de l'air, la brigade des forces spéciales de l'armée de terre – sont rattachées organiquement à leur armée respective. Pour ce qui est des opérations, elles relèvent toutes du commandement des opérations spéciales. L'idée est donc de préserver la cohérence organique des armées. Cela fonctionne bien et selon notre culture, et de constituer un commandement de cyberdéfense, à l'image des forces spéciales, qui regroupe ceux que nous appelons les "combattants numériques". […] Le dialogue avec les armées est également satisfaisant, le commandement cyber relevant du chef d'état-major des armées tel qu'il a été désigné voici quelques mois. En clair, le système fonctionne bien, permet de conduire des opérations de qualité et garantit notre compétitivité. J'ajoute que la cyberdéfense comporte deux dimensions. La dimension défensive, d'une part. Elle relève du cadre interministériel et de l'agence nationale de la sécurité des systèmes d'information (ANSSI), qui dépend du SGDSN. La dimension opérationnelle, d'autre part, qui recouvre la contre-influence et la "guerre cyber". Elle est pilotée par le ministère des armées. Cette organisation fonctionne bien et une quatrième armée n'est donc pas nécessaire. Il faut toutefois poursuivre nos efforts, car nous serions dépassés à la moindre baisse de régime. Dans ce domaine comme dans le secteur numérique, les mutations sont très rapides et nous devons être en mouvement*

permanent. Les effectifs doivent poursuivre leur montée en puissance. Nous devons former en permanence et fidéliser ces personnes très spécialisées. C'est tout un modèle de gestion des ressources humaines au niveau de l'État qu'il faut ériger… » [29]. Les évolutions seront d'ordre budgétaire et humain mais plus organisationnel. En termes stratégique, une action internationale apparaît par ailleurs essentielle.

II. La Cyberdéfense, une internationalisation nécessaire

Le caractère international des cyberattaques y compris d'ordre militaire par l'utilisation d'infrastructures dans différentes États impose une coopération internationale[30]. Elle s'est concrétisée dans le champ opérationnel (**A**) mais elle est plus incertaine dans celui juridique (**B**).

A. La mise en place de réponses opérationnelle

L'amiral Arnaud Coustillière, alors officier général cyberdéfense, expliquait en 2015 qu'« *il y a deux sujets sur lesquels nous [les États] pouvons agir ensemble : l'État islamique et les mafias russes* » [31]. L'amiral Coustillière avait défendu la création d'un « *club des cybercommandeurs* » élargi, en dépit des réticences exprimées par son homologue américain : « *Travailler en coalition dans ce domaine est un chantier énorme* », a-t-il admis[32]. La coopération interalliée sera impossible en matière défensive, jugent les militaires, chacun répugnant à dévoiler ses vulnérabilités. Mais « *le volet offensif est beaucoup plus simple* », assurait l'amiral, « *nous pouvons au moins coordonner nos attaques* »[33].

D'une part, les coopérations sont interétatiques comme a pu l'illustrer le rassemblement de vingt officiers généraux étrangers « *cybercommandeurs* », dont plusieurs États du Maghreb et du Golfe, alliés de la France. Le ministre britannique de la défense, Michael Fallon, a ainsi révélé que son pays et la France avaient créé un « *cybergroupe deux étoiles* », autrement dit une réunion permanente militaire de haut niveau pour la guerre informatique. C'est particulièrement le cas contre l'État islamique (EI).

---

29. Audition du général Pierre de Villiers, chef d'état-major des armées, *JOAN*, Commission de la défense nationale et des forces armées, Compte rendu n° 3, 2 juillet 2017.
30. Même si chaque État développe sa propre stratégie, v. not. L'Allemagne lance une « cyber-armée », *Le Monde.fr*, 31 mars 2017. Selon le ministère de la défense allemand, la Bundeswehr a subi pendant les neuf premières semaines de cette année 284 000 cyberattaques, sans toutefois subir de dommages. Basée à Bonn, le KdoCIR entrera en action samedi avec 260 personnes et comptera à terme 13 500 personnels, militaires et civils, ce qui « *correspond à peu près aux effectifs de la Marine* », a précisé le général Leinhos.
31. Nathalie Guibert, « La France revendique sa place dans la cyberguerre offensive », *Le Monde*, 25 sept. 2015.
32. *Ibid*.
33. *Ibid.*

D'autre part, la coopération s'appuie sur les organisations internationales. En tant que membre de l'OTAN, la France est pleinement actrice de la stratégie cyber de l'OTAN. Depuis 2010, avec le sommet de Lisbonne, le concept stratégique de l'OTAN intègre ainsi la cyberdéfense. Cette intégration résulte d'une réflexion lancée, pour la première fois, au sommet de Prague, en 2002[34]. Elle a abouti à l'élaboration d'un document qui fait référence : le manuel de cyberdéfense de Tallin[35]. A sa suite, en 2014, une autre avancée significative s'est manifestée avec la directive donnée à l'OTAN par les ministres de la défense des pays de l'Alliance d'élaborer une nouvelle politique de cyberdéfense renforcée intégrant la défense collective, l'assistance aux Alliés et la gouvernance rationalisée.

L'Union européenne se veut également active. La compétence européenne se dégage de l'article 15 du Traité de Lisbonne, attribuant compétence partagée entre l'Union européenne et les États pour les réseaux transeuropéens. Cette compétence porte initialement sur la cybersécurité civile[36]. Mais, depuis 2013[37], l'Union européenne a défini sa politique de sécurité informatique en intégrant pleinement les enjeux militaires. L'objectif est de développer une politique et des moyens de cyberdéfense dans le cadre de la PSDC (Politique de sécurité et de défense commune), considérant le danger que représentent les attaques informatiques en termes de sécurité nationale y compris dans le domaine militaire. L'Union européenne voit des réponses à ce danger par la coopération accrue des États membres avec l'Agence européenne de défense (AED), par la réunion et la prise en compte de l'expérience et des bonnes pratiques des agences et des organes existants ainsi que des États membres, par l'intégration de la gestion des crises informatiques dans la planification de la gestion des crises et la mise en place

34. Les dirigeants des pays de l'Alliance réunis au sommet de Riga, en 2006, ont réaffirmé la nécessité de protéger davantage ces systèmes. Suite aux cyberattaques qui ont touché des institutions publiques et privées de l'Estonie en avril et en mai 2007, les ministres de la Défense des pays de l'Alliance sont convenus, en juin 2007, qu'il était urgent de mener des travaux dans ce domaine. Résultat, l'OTAN a adopté sa première politique de cyberdéfense en janvier 2008. À l'été 2008, le conflit entre la Russie et la Géorgie a montré que les cyberattaques pouvaient devenir un élément essentiel de la guerre conventionnelle. En juin 2011, l'OTAN a approuvé la deuxième version de la politique de cyberdéfense. En avril 2012, la cyberdéfense a commencé à être intégrée dans le processus OTAN de planification de défense. Les besoins pertinents en matière de cyberdéfense sont recensés et priorisés dans le cadre de ce processus. L'objectif est notamment de renforcer les moyens. En juillet 2012, dans le cadre de la réforme des agences de l'OTAN, la NCIA (*NATO Communications and Information Agency*) a été créée. Au sommet du pays de Galles, en septembre 2014, les Alliés ont entériné la nouvelle politique de cyberdéfense et approuvé un nouveau plan d'action.

35. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare*, University Cambridge, 2nd éd., 2016.

36. Dès 2004, l'ENISA (*European Network and Information Security Agency*) est créée.

37. Communication de la Haute représentante de l'Union européenne pour les affaires étrangères et la politique de sécurité, « Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé », février 2013 [JOIN(2013) 1] ; Cadre d'action de l'UE en matière de cyberdéfense, 18 nov. 2014 [Consilium 15585/14] ; Communication conjointe au Parlement européen et au Conseil Cadre commun en matière de lutte contre les menaces hybrides : une réponse de l'Union européenne, JOIN(2016) 18 final, 6 avr. 2016 ; Résolution du Parlement européen du 12 septembre 2013 sur la stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé (2013/2606(RSP)).

une force européenne de cyberdéfense. L'Union européenne souligne la bonne coopération opérationnelle avec l'OTAN dans le domaine de la cybersécurité et la nécessité de renforcer cette coopération, afin d'éviter les doubles emplois et de compléter les activités[38].

Concrètement, le 10 février 2016, l'OTAN et l'Union européenne ont conclu un arrangement technique sur la cyberdéfense visant à aider les deux organisations à mieux prévenir les cyberattaques et à y répondre plus efficacement. Cet arrangement technique entre la NCIRC (NATO *Computer Incident Response Capability*) et le centre d'alerte et de réaction aux attaques informatiques de l'Union européenne (CERT/UE) fixe un cadre pour l'échange d'informations et le partage de pratiques de référence entre les équipes d'intervention d'urgence[39].

De plus, en proposant la création d'un Fonds européen pour la défense en juin 2017, la Commission européenne[40] peut contribuer au financement de recherches pour lutter contre les cyberattaques même si la somme globale est modeste : 500 millions d'euros annuel pour la recherche à partir de 2020 alors que les budgets militaires cumulés des Vingt-Huit approchent les 200 milliards d'euros. Pour autant, les capacités cyber et réponses aux menaces de guerre hybride sont parmi les dossiers. Surtout, c'est une avancée politique symboliquement très forte qui fait pleinement entrer l'Union européenne dans les enjeux militaires.

B. Les incertitudes d'un cadre juridique international

L'action militaire y compris cyber ne peut s'affranchir des règles juridiques non seulement pour déterminer ce qui est entendu comme une agression, *jus ad bellum*, mais également ce qui peut être autorisé comme actions militaires, *jus in bello*. La France et notamment via le ministère de la défense contribue à la réflexion pour l'élaboration d'un droit international de la cyberguerre. La France est sur ce point un acteur important car elle sait que son investissement militaire dans le cyberespace ne peut pleinement être efficace que s'il est accompagné d'une réglementation internationale. On peut ici trouver le même raisonnement qu'en matière d'espace extra-atmosphérique et d'arme nucléaire. La France mène une action diplomatique afin de peser dans les négociations internationales. Ainsi un ambassadeur pour la cyberdiplomatie et l'économie numérique a été nommé. Sous sa conduite, une conférence a été organisée en avril 2017 à Paris sur la

38. Communication conjointe au Parlement européen et au Conseil, *Cadre commun en matière de lutte contre les menaces hybrides : une réponse de l'Union européenne*, JOIN(2016) 18 final, 6 avr. 2016 ; résolution du Parlement européen du 12 septembre 2013 *sur la stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé* (2013/2606(RSP)).
39. Fabrice Jaouën, Andreas Kornmaier, « Coopérations européennes en matière de cyberdéfense » *RDN*, n° 770, mai 2014, p. 47 s.
40. Nathalie Guibert, Jean-Pierre Stroobants, « Bruxelles propose la création d'un Fonds européen pour la défense », *Le Monde Éco*., 7 juin 2017.

« *construction de la paix et [de] la sécurité internationales de la société numérique* » afin d'« *approfondir la réflexion juridique sur les questions de paix et de stabilité dans le cyberespace est nécessaire* », estime M. Martinon[41].

Or, les difficultés sont nombreuses pour déterminer la responsabilité de l'État dans une cyberattaque, les conditions d'une légitime défense numérique ou bien encore les actions militaires numériques offensives et défensives déployées sur un champ de bataille conformes au droit international. Des travaux ont commencé au sein notamment de l'ONU ou de l'OTAN[42] mais les avancées sont réduites[43] à l'exception du Manuel de Tallinn rédigé en 2013 par des experts mandatés par l'OTAN[44]. La souveraineté de l'État est au cœur des négociations.

Pourtant, l'ONU conduit, depuis 2004, un groupe des experts gouvernementaux (GGE), afin d'établir des règles dans le cyberespace. En 2013, puis en 2015, deux rapports avalisés par l'Assemblée générale des Nations unies ont reconnu des principes généraux, par exemple, l'application du droit international dans le cyberespace ainsi que des normes de comportement. Une étape cruciale dans ce processus est intervenue à la fin du mois de juin 2017, avec le dernier « *round* » de négociations du CGE car il pouvait déboucher sur des règles plus précises. Or, les négociations ont échoué. La raison de l'échec est à trouver dans l'opposition russe notamment sur les sanctions qui pourraient être employées à l'encontre des auteurs…ou des États hébergeurs des infrastructures physiques. A l'issu de ces négociations, la France a de nouveau rappelé sa volonté que « *l'ensemble des États [reconnaissent] l'applicabilité du droit international existant à leurs actions dans le cyberespace* »[45].

L'objectif de la France et des négociations internationales était d'ouvrir la voie vers un « *mécanisme collectif de responsabilité* » au nom de l'obligation de diligence de l'État. En d'autres termes, tout État par lequel transite une attaque informatique assume la responsabilité de la faire cesser par une intervention sur ses infrastructures. Le droit international public a depuis longtemps pour principe la responsabilité internationale de l'État du fait de son action ou de son inaction y compris en raison du comportement de ses ressortissants[46]. Mais l'application de ce principe se heurte au fait que ce principe devrait s'appliquer à tous les États par laquelle transiterait la cyberattaque. Ce ne serait donc pas uniquement l'État d'origine. Cette position avait été retenue au niveau international lors des négociations du

41. Nathalie Guibert, « La France à la recherche d'un délicat "ordre public dans le cyberespace" », *Le Monde*, 6 avr. 2017.
42. C'est également le cas de l'OSCE, v. *Cyber Security for Critical infrastructure : Strengthening Confidence Building in the OSCE*, Vienne, 15 fév. 2017. Pour plus de détails, v. Karine Bannelier, Théodore Christakis, *op. cit*.
43. V. Karine Bannelier, Théodore Christakis, *op. cit*.
44. *Op. cit*.
45. Déclaration du ministre des affaires étrangères, 29 juin 2017.
46. C.I.J., 4 avr. 1949, aff. du Détroit de Corfou, Rec. 1949, p. 22.

groupe des experts gouvernementaux en 2015, sans en ignorer les très nombreuses difficultés techniques pour agir de la part de certains États.

L'enjeu est, plus globalement, de déterminer le rôle de l'État dans les cyberattaques. En effet, certains défendent la logique du hack back, qui serait finalement, pour ses défenseurs, une légitime défense numérique par une contre-attaque – pas une simple défense – contre l'agresseur numérique. Or, cette légitime défense serait ouverte aux victimes, et donc pas seulement à l'État mais également aux opérateurs privés ou mêmes des personnes physiques privées. Cela peut avoir un effet dissuasif mais un double risque – plus important – existe : une erreur dans l'identification de l'agresseur et une escalade dans les attaques et contre-attaques qui impliqueraient à terme inévitablement les États.

L'armée doit donc repenser les menaces y compris numériques car elles impliquent plus facilement de nouveaux acteurs non seulement comme attaquants – mais là il n'y a rien de nouveau – mais comme défenseurs.