Publié in Sébastien-Yves Laurent. Conflits, crimes et régulations dans le cyberespace, ISTE, 2021

LA CYBERDÉFENSE, DIMENSION NUMERIQUE DE LA SECURITE NATIONALE

Bertrand WARUSFEL,

Professeur à l'Université Paris 8, avocat au barreau de Paris

La notion de cyberdéfense ne cesse de s'étoffer au fur et à mesure que les déclarations et les documents officiels en affirment la nécessité stratégique. En 2019 en particulier, le ministère des Armées a confirmé que sa stratégie de cyberdéfense comporte à la fois une dimension défensive (dénommée « lutte informatique défensive ») et une dimension offensive (« lutte informatique offensive »).

Cette montée en puissance de la cyberdéfense comme concept opérationnel n'est pas surprenante. Elle s'inscrit dans un mouvement plus large qui a vu évoluer le périmètre de la sécurité des systèmes d'information (SSI) vers ce que l'on dénomme aujourd'hui la « cyber-sécurité » avec notamment un décloisonnement des préoccupations de sécurité des systèmes d'information publics et privés.

Mais c'est aussi l'affirmation politique et juridique actuelle des pratiques de sécurité nationale (qu'il s'agisse du cadre juridique du renseignement ou celui des opérations extérieures) qui rend plus nécessaire la définition d'un régime juridique de la cyberdéfense afin qu'il puisse s'inscrire tout entier dans le droit français de la sécurité nationale qui se construit progressivement.

Après avoir resitué la place spécifique de la cyberdéfense dans le continuum de la sécurité numérique, nous nous efforcerons de mettre en avant quelques aspects de son régime juridique et de la place qu'elle tient désormais dans le dispositif juridique et opérationnel de sécurité nationale.

I/ La cyberdéfense dans le cadre politico-juridique de la sécurité numérique

L'article 1er de la récente loi du 26 février 2018[1] nous donne une définition de ce qu'elle dénomme la « sécurité des réseaux et systèmes d'information » (et que nous dénommons plus généralement la cyber-sécurité). Cela consiste dans la capacité de ces réseaux et systèmes à *« résister, à un niveau de confiance donné, à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles »*.

1.1. Une définition de la cyberdéfense

Mais alors que la cyber-sécurité, ainsi définie, vise la résilience de tous les systèmes numériques, la cyberdéfense – telle que le vocabulaire officiel la présente – ne concerne que les systèmes considérés comme *« d'importance vitale »* et *« qui contribuent à assurer la cybersécurité »* et que l'État défend[2].

1 Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité (transposant notamment la directive NIS).

2 Elle est en effet définie comme un « ensemble des moyens mis en place par un État pour défendre dans le cyberespace les systèmes d'information jugés d'importance vitale, qui contribuent à assurer la cybersécurité » (Vocabulaire de la défense : cyberdéfense, *JORF*, 19 septembre 2017).

La notion de systèmes d'information *« essentiels »* et *« jugés d'importance vitale »* nous renvoie directement au code de la défense, dont l'article L1332-6-1 nous indique qu'il s'agit des systèmes des opérateurs d'importance vitale, lesquels sont les opérateurs *« publics ou privés »* dont *« l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation »* (selon l'article L. 1332-1 Cdèf).

On en déduit donc une double différentiation entre les concepts de cybersécurité et de cyberdéfense :

- d'une part, la cybersécurité a un champ d'application universel, puisqu'il s'agit d'assurer la résilience de tous les systèmes numériques, alors que la cyberdéfense ne s'attache qu'à assurer la sécurité des systèmes vitaux dont la défaillance pourrait nuire à la nation,

- d'autre part, si la cybersécurité est l'affaire de tous les responsables de systèmes et de réseaux, la cyberdéfense est une activité totalement régalienne qui est menée par différents de l'État, ou tout au moins sous sa responsabilité directe et en vertu des pouvoirs particuliers que la loi lui donne.

On peut d'ailleurs revoir quelque peu la définition initiale pour en clarifier la logique sous-jacente : la cyberdéfense est l'ensemble des moyens mis en place sous la responsabilité de l'État pour défendre dans le cyberespace les systèmes d'information dont l'atteinte affecterait le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation, c'est-à-dire la sécurité nationale.

Ce faisant, on s'éloigne d'une approche prioritairement organique au profit d'une logique basée sur la nature des menaces à traiter. Et cela permet de mieux resituer la cyberdéfense dans la gradualité des concepts sécuritaires français.

Rappelons en effet, que depuis 2009 et la nouvelle rédaction de l'article .1111-1 Cdéf une hiérarchie conceptuelle totalement renouvelée a été introduite en droit français qui repose sur la notion cardinale de « sécurité nationale ». Cette sécurité nationale se distingue des autres aspects de la sécurité intérieure par le fait qu'elle se concentre exclusivement sur l'anticipation et le traitement des *« menaces et des risques susceptibles d'affecter la vie de la Nation»*.

On peut dès lors considérer que la cyberdéfense, qui ne vise qu'à assurer la sécurité des systèmes numériques d'importance vitale pour la Nation est un concept de sécurité nationale, ou plus exactement qu'elle constitue la dimension cyber de la sécurité nationale[3].

1.2. Le rattachement de la cyberdéfense à la stratégie de sécurité nationale

Cette proposition d'interprétation de la notion de cyberdéfense se confirme si l'on regarde ce qu'induit la cyberdéfense en termes de moyens juridiques et opérationnels à déployer par l'État et les opérateurs d'importance vitale. On a pu écrire en effet que *« la sécurité nationale correspond à une dimension très spécifique de l'intérêt général qui a pour attribut de pouvoir justifier la mise en œuvre par le pouvoir exécutif de prérogatives spéciales entrainant des limitations à l'exercice des libertés publiques »*[4].

3 Cette affirmation a déjà été formulée dès 2013 par le Gal Watin-Augouard qui voit dans la cyberdéfense « uhn des piliers de la sécurité nationale » (Marc Watin-Augouard, « Cybermenaces et sécurité nationale », in Christian Vallar & Xavier Latour, Le droit de la sécurité et de la défense en 2013, PUAM, 2014, p. 298.

4 Bertrand Warusfel, "Le contentieux de la sécurité nationale", in Bertrand Warusfel & Florent Baude (dir.), *Annuaire 2018 du droit de la sécurité et de la défense*, Ed. Mare & Martin, 2018, pp. 203-218.

Or ce qui distingue clairement la cyberdéfense du reste de la cybersécurité, c'est bien qu'elle justifie la mise en œuvre par l'État de plusieurs prérogatives particulières, dont, comme nous allons le voir, les plus contraignantes – et les plus dérogatoires aux libertés, dont celle du commerce et de l'industrie – se retrouvent dans le code de la défense.

Par ailleurs, la définition officielle de la cyberdéfense de 2017 que nous avons pris pour référence mentionne également que *« la cyberdéfense met notamment en œuvre la lutte informatique défensive et la lutte informatique offensive »*. Or, ces deux dimensions de la « lutte » cybernétique relève l'une et l'autre des moyens spéciaux de l'État.

La lutte informative défensive (LID dans la signalétique du ministère des Armées) relève plus particulièrement des actions de renseignement puisqu'elle *« couvre principalement les missions : anticiper, détecter et réagir et complète les missions : prévenir, protéger et attribuer »*[5]. Elle est d'ailleurs planifiée et conduite par le ComCyber, en coordination avec l'ANSSI et les services de renseignement[6].

Quant à la lutte informatique offensive (LIO), elle se définit comme un « e*nsemble coordonné d'actions menées dans le cyberespace par un État contre des systèmes d'information ou de données pour les perturber, les modifier, les dégrader ou les détruire »[7].* Elle relève donc directement de la défense militaire, puisque *« l'objectif premier de la LIO est de contribuer dans le cyberespace à la supériorité militaire »[8].*

Or, là encore la conformité avec la logique de la sécurité nationale est patente. Les services spécialisés de renseignement ont notamment mission de recueillir les renseignements relatifs aux *« menaces et aux risques susceptibles d'affecter la vie de la Nation »*[9] tandis que, plus explicitement encore « la politique publique de renseignement concourt à la stratégie de sécurité nationale »[10]. Tandis que, de son côté, *« la politique de défense a pour objet d'assurer l'intégrité du territoire et la protection de la population contre les agressions armées » et « contribue à la lutte contre les autres menaces susceptibles de mettre en cause la sécurité nationale »*[11]. Or tout comme la sécurité nationale ainsi définie, la doctrine de cyberdéfense française comporte donc bien un sous-ensemble particulier défiée à la mise en œuvre des moyens militaires lorsque la nature de l'attaque l'impose.

Si donc la cyberdéfense est partie intégrante du dispositif français de sécurité nationale, il convient encore d'en préciser le cadre juridique d'emploi.

II/ L'émergence d'un régime juridique cohérent de la cyberdéfense

Différents textes français mais aussi européens[12] ont contribué depuis une dizaine d'années à densifier le dispositif juridique permettant aux plus hautes autorités de l'État (et en premier

5 Ministère des armées, Politique ministérielle de lutte informatique défensive (LID), 2019.
6 Idem.
7 Vocabulaire 2017 précité.
8 Ministère des armées, Politique ministérielle de lutte informatique offensive (LID), 2019.
9 Article L.811-2 du code de la sécurité intérieure (issu de la loi relative au renseignement du 24 juillet 2015)..
10 Art. L.811-1 CSI.
11 Art. L.1111-1 Cdéf précité, 3ème alinéa.
12 S'il pourrait paraître étonnant que le droit européen intervienne dans un domaine relevant de la sécurité nationale des Etats-membres (qui en concernent la compétence exclusive d'après l'article 4.2 TUE), il faut admettre cependant que, de manière indirecte, le droit de l'Union européenne incorpore de plus en plus de problématiques de sécurité qui se combinent plus ou moins efficacement avec les mesures proprement nationales (v. notre analyse : B. Warusfel, "L'entrée de l'Union européenne dans les champs de la défense et de la sécurité", *Cahiers de la sécurité et de la justice,* 1er semestre 2014, n° 27-28, pp. 189-198).

lieu au Premier ministre) de mettre en œuvre les actions de cyberdéfense que peut imposer la protection de la sécurité nationale.

Nous trouvant dans le champ de la sécurité nationale, il convient notamment de distinguer les prérogatives spéciales ayant vocation à s'appliquer en permanence dès lors qu'un objectif de sécurité nationale est en jeu de celles qui sont des moyens exceptionnels ne pouvant être utilisées temporairement pour répondre à une crise ou un conflit.

2.1. Les moyens juridiques de la posture permanente de cyberdéfense

Les moyens juridiques permanents de cyberdéfense sont toutes les dispositions permettant à l'État, par l'intermédiaire de son autorité nationale de sécurité des systèmes d'information (ANSSI), d'imposer à différents acteurs majeurs de la société numérique des mesures préventives de cybersécurité.

Il s'agit tout d'abord des obligations que le code de la défense impose aux opérateurs d'importance vitale (dont on a évoqué le rôle central dans la cyberdéfense) qui doivent respecter les « règles de sécurité » fixées par l'ANSSI et qui « peuvent notamment prescrire que les opérateurs mettent en œuvre des systèmes qualifiés de détection des événements susceptibles d'affecter la sécurité de leurs systèmes d'information » et faire appel à des prestataires de service qualifiés par la même ANSSI [13]. En 2018, plus de 1000 systèmes informatiques qualifiés d'importance vitale répartis entre plus de 350 opérateurs étaient recensés.

Mais la transposition de la directive NIS (Network and Information Security du 6 juillet 2016) par la loi du 26 février 2018 et le décret du 23 mai 2018 a élargi la possibilité pour l'autorité de sécurité d'imposer également des obligations : aux « opérateurs de services essentiels » et aux « fournisseurs de service numérique ». La loi de programmation militaire de 2018 **a** complèté le tout en pouvant imposer aux opérateurs de communication électronique d'installer sur leur réseau des sondes de détection de cyberattaques qui sont sous le contrôle direct de l'ANSSI[14].

A ces règles de prévention des vulnérabilités et d'anticipation des menaces, qui constituent un droit dérogatoire permanent justifié par l'impératif national de cybersécurité s'ajoutent logiquement des dispositions destinées à n'entrer en vigueur qu'en période de crise.

2.2. Les instruments exceptionnels de riposte à la crise

Comme l'indique un récent rapport parlementaire sur la cyberdéfense, *« le modèle français repose sur quatre acteurs principaux qui forment en quelque sorte le premier cercle de la cyberdéfense »*[15]. A chacun de ces quatre niveaux, correspond une branche de la riposte nationale contre les cyberattaques.

Le premier niveau de riposte consiste simplement pour l'État à déclencher si nécessaire les enquêtes judiciaires et les sanctions associées qui sont prévues dans le code pénal et qui répriment les infractions cybercriminelles[16]. Depuis leur introduction en droit français en 1988 avec la fameuse *« loi Godfrain »* (du nom du parlementaire qui porta la proposition de

13 Art. L1332-6-1 Cdéf..

14 Art. L. 2321-2-1 Cdéf. créé par la loi de programmation militaire du 13 juillet 2018.

15 Assemblée nationale, Rapport d'information sur la cyberdéfense, 4 juillet 2018, document n° 1141

16 Sur la liaison à établir entre la répression pénale de la cybercriminalité et la cyberdéfense, v. M. Watin-Augouard, précité, p. 303.

loi), les articles 323-1 à 323-7 du code pénal ont vu leur quantum de peines s'alourdir mais aussi leur champ d'application s'élargir.

D'une part, l'article 323-3 Cpen poursuit aussi depuis fin 2014[17] le fait « d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données », ce qui permet une meilleure protection contre les actes de cyberespionnage. Mais d'autre part la même réforme de 2014 a prévu que l'attaque de tout *« système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat »* constitue une circonstance aggravante de toutes ces infractions qui augmente les peines encoures aux articles 323-1 à 323-3 Cpen et qui permet lorsqu'elles sont commises en bande organisée d'atteindre une peine maximale de dix années de prison et 150.000 € d'amende[18]. Même si l'on peut s'interroger sur la raison qui a poussé le législateur à ne viser ici que les traitements de données personnelles, et non tous les systèmes d'informations de l'État (dont la sensibilité peut être extrême – notamment dans des domaines techniques – sans traiter des données à caractère personnel), ce renforcement constitue clairement un signal politique et un dispositif juridique visant la riposte à des attaques majeures visant les structures-clés de l'administration dématérialisée.

Cette riposte juridique pourrait être d'ailleurs transnationale puisque les dispositions pénales françaises s'intègrent dans le cadre de la Convention Cybercrimalité de 2001, laquelle organise la coopération policière et judiciaire des Etats signataires pour mener des enquêtes et des incriminations transnationales face à des attaques tout aussi globalisées. On notera encore que cette protection pénale des systèmes numériques publics peut s'accompagner d'une riposte technique, puisque l'article L. 2321-2-1 du code de la défense permet à l'ANSSI de prendre des mesures de surveillance technique particulières lorsqu'elle *« a connaissance d'une menace susceptible de porter atteinte à la sécurité des systèmes d'information des autorités publiques »*.

Mais la cyberdéfense dispose depuis quelques années d'autres instruments d'exception qui sont spécifiquement conçus pour permettre une riposte technique et opérationnelle. Trois autres acteurs sont engagés au sein de l'État dans cette dimension « offensive » de la cyberdéfense.

Evoquons en quelques mots, le plus discret de ces acteurs, à savoir la communauté du renseignement. Si l'on sait que les services spécialisés ont notamment une mission de détection des menaces y compris cyber, on connaît moins – secret de défense oblige – leurs capacités intrusives (ou réactives à une attaque extérieure). Seule une disposition pénale sibylline nous indique à l'article 323-8 du code pénal que « le présent chapitre n'est pas applicable aux mesures mises en œuvre, par les agents habilités des services de l'Etat désignés par arrêté du Premier ministre parmi les services spécialisés de renseignement mentionnés à l'article L. 811-2 du code de la sécurité intérieure, pour assurer hors du territoire national la protection des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 du même code ». On en conclut logiquement de l'énoncé de cette immunité pénale particulière que certains services spécialisés (la DGSE en premier lieu) peuvent s'impliquer dans des opérations offensives contre des systèmes numériques étrangers à des fins hautement stratégiques de sécurité nationale (puisqu'est fait spécifiquement référence à la protection des intérêts nationaux).

Plus visible est – depuis les textes de cette dernière décennie – le rôle central du Premier ministre, avec son bras armé en la matière qui est l'ANSSI. Autorité nationale de cybersécurité,

17 Précisément depuis la loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme (qui a modifié l'article 323-3 Cpen).

18 Art. 323-4-1 Cpen.

l'ANSSI est le pivot autour duquel vont être mises en œuvre les prérogatives exceptionnelles que l'article L2321-2 du code de la défense confère au chef du gouvernement[19]. C'est en effet le Premier ministre au travers de l'ANSSI qui va intervenir pour *« répondre à une attaque informatique qui vise les systèmes d'information affectant le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation »*. Là encore, et malgré la disparité (regrettable) de la terminologie, il s'agit de réagir à une menace de sécurité nationale à laquelle la loi va permettre d'opposer une riposte pouvant aller jusqu'à la pénétration des systèmes adverses et leur *« neutralisation »* en utilisant toute sorte d'équipements ou de logiciels proches de ceux qu'utilisent de leur côté les cyberdélinquants (puisqu'ils sont décrits comme de nature à *« permettre la réalisation d'une ou plusieurs des infractions prévues aux articles 323-1 à 323-3 du code pénal »*). Les pouvoirs du Premier ministre (et donc de l'ANSSI) vont alors très loin puisqu'ils permettent même d'imposer aux entreprises et opérateurs privés visés par la cyberattaque les mesures qu'ils doivent mettre en œuvre[20].

Mais la riposte opérationnelle peut être également dirigée par le COMCYBER au sein des armées *« lorsque l'attaque informatique vise exclusivement les capacités opérationnelles des armées ou les chaînes de commandement de la défense »*. L'autorité compétente est alors « le commandement opérationnel de la cyberdéfense de l'état-major des armées, en liaison avec l'ANSSI »[21].

Enfin, et pour terminer de gravir tous les échelons de la mise en œuvre des moyens de sécurité nationale, le ministère des armées inscrit son action cyber dans le cadre de la nouvelle « Stratégie nationale de la cyberdéfense » publiée en 2018[22] et qu'il a complété en rendant publics ses *« éléments publics de doctrine militaire de lutte informatique offensive »*[23] qui – bien que très généraux dans leur terminologie – affirme que la *« chaîne action militaire »* vient en complément des chaînes *« protection », « renseignement »* et *« investigation judiciaire »*, en pratiquant si nécessaire la lutte informatique offensive[24].

Bien que les Armées restent logiquement très avares d'indication précise sur les opérations offensives que la France pourrait décider de lancer pour punir ses agresseurs et protéger ses infrastructures numériques, le message est clair : l'usage des cyber-armes par les forces françaises n'a pas vocation à soutenir uniquement les opérations militaires classiques (en neutralisant des systèmes numériques adverses) mais xpourrait aussi permettre de répliquer à une attaque cyber de grande envergure. Le préambule du document est, à cet égard, très clair lorsqu'il évoque les différentes cyberattaques « contre l'Estonie en 2007, contre les réseaux électriques de l'Ukraine, contre TV5 Monde en 2015, le rançongiciel Wannacry au printemps 2017 ou encore l'attaque NotPetya en juin 2017, (qui) illustrent les champs d'actions possibles pour des attaquants dont les quatre objectifs majeurs sont l'espionnage, les trafics illicites, la déstabilisation et le sabotage »[25]. Plus loin, il est également évoqué que les cyber-opérations offensives peuvent être *« menées en appui de la lutte informatique défensive »*[26]. On notera enfin que la dernière loi de programmation militaire a étendu

19 Dont l'application fait l'objet d'une instruction classifiée du 7 mars 2016 (v. SGDSN, Revue stratégique de cyberdéfense, 2018, p. 47).

20 Article L1332-6-4 Cdéf.

21 Revue stratégique de cyberdéfense, précitée, p. 48.

22 Pour une synthèse de ce texte important, v. notamment François Delerue & Aude Géry, Le droit international dans la « Stratégie nationale de la cyberdéfense », note de recherche n° 58, IRSEM, 11 juillet 2018.

23 Eléments publics de doctrine militaire de lutte informatique offensive, Ministère des armées, 2019.

24 Idem, p. 4.

25 Idem, p. 4.

26 Idem, p. 10.

« l'excuse pénale » déjà reconnue aux combattants en opération, à ceux d'entre eux qui seraient impliqués dans des « actions numériques »[27]

En conclusion, il apparaît que le dispositif très empirique qui a progressivement émergé pour faire face aux menaces numériques nouvelles se décline selon une pyramide dont les différents niveaux sont cohérents avec la manière dont on peut appréhender la sécurité nationale.

SI la cyberdéfense se distingue largement de la cybersécurité du quotidien[28] (de la même manière que la sécurité nationale n'a pas la charge des missions classiques de sécurité publique), elle se concentre sur l'anticipation et la traitement des menaces majeures affectant la vie national. Cela confère alors à la puissance publique des prérogatives dérogatoires pouvant restreindre certaines libertés (comme lorsque l'ANSSI a le pouvoir d'imposer à des acteurs privés de mettre en œuvre tel ou tel aspect d'un référentiel de cybersécurité, ou d'installer des sondes sur leurs réseaux).

Au-delà - et dans les limites de ce que le droit des conflits armés et le droit humanitaire autorisent - la cyberdéfense peut comporter aussi un prolongement offensif extrême de nature militaire, manifestant ainsi dans le domaine du traitement des menaces numériques l'affirmation du Livre blanc sur la défense et la sécurité nationale de 2008 selon laquelle « (aux) objectifs (de sécurité nationale) concoure la politique de défense, en totalité ». La gradualité des moyens de la cyberdéfense et leur doctrine d'emploi s'inscrivent donc dans le cadre plus large de la protection de la sécurité nationale.

27 Article L.4123-12 Cdéf modifié.

28 Cette distinction était déjà nette dans la présentation des deux premiers objectifs de la « stratégie nationale pour la sécurité numérique » (Premier ministre, 2015 pp. 14-23) dont l'un vise la protection des intérêts de la Nation contre la crise informatique majeure, tandis que le second traite de « la confiance numérique » et de la protection de la vie privée contre la cybermalveillance.