ECOLE DE GUERRE

PROMOTION *VERDUN*
2015 -2016

L'Union européenne et la sécurité : Existe-t-il une cyberstratégie européenne ?

Lieutenant-Colonel Christophe Despré

Sous la direction de

Delphine Deschaux-Dutard

Professeur à l'université de Grenoble-Alpes

TABLE DES MATIERES

RESUMÉ

Nos sociétés sont aujourd'hui confrontées à une dépendance technologique qui s'est considérablement amplifiée durant les dernières décennies et qui a donné vie à un nouveau milieu, le cyberespace, qui a généré de nouvelles menaces dont les enjeux sont considérables et que certains experts en stratégie considèrent comme une 5ème espace de conflictualité.

L'universalité de cette menace est telle qu'une coopération entre les Etats et les organisations semble indispensable. L'Union européenne a ainsi élaboré en février 2013 une stratégie de cybersécurité, de portée très générale, qui repose avant tout sur un partage de responsabilités avec les Etats membres. Mais la plus-value réelle de cette stratégie de cybsersécurité parait toute relative avec une Europe, souvent limitée à un rôle de coordinateur, sans réels pouvoirs de contraintes. De plus, le niveau de sécurité entre les Etat membres est très disparate et le principe de souveraineté qui prédomine, limite fortement l'échange de renseignements et le partage de bonnes pratiques pourtant essentiels.

En parallèle, des coopérations bilatérales « à la carte » se sont développées entre Etats ainsi qu'une coopération avec l'OTAN. Ces coopérations, qui sont toutes caractérisées par une stratégie des petits pas, semblent davantage affirmées que suivies d'actions concrètes. Or, une complémentarité entre ces deux organisations semble tout de même possible avec l'OTAN qui pourrait se focaliser sur la cyberdéfense et l'UE qui dispose des moyens de développer l'approche globale de la cybersécurité. Enfin, la stratégie de cybersécurité européenne s'inscrit dans une stratégie beaucoup plus globale, davantage affirmée en terme de gouvernance et de protection des libertés fondamentales, comme la protection des données personnelles et l'accès universel à l'Internet.

SUMMARY

Our societies are now facing a technological dependence which is greatly amplified in recent decades and that has given life to a new environment, cyberspace, which has generated new threats that the stakes are quite high.

The universality of the threat is such that cooperation among states and organizations seems essential. Europe has developed in February 2013 a cybersecurity strategy, very general, which is primarily based on a sharing of responsibilities with Member States. But the effectiveness of this strategy seems quite relative with a Union, often limited to a coordinating role without real power of constraints. Moreover, the level of security between Member States is very uneven and the principle of sovereignty prevails, severely limits the exchange of information and sharing of good practices that are essential.

In parallel, bilateral cooperations have developed between States as well as cooperation with NATO. These cooperations, which are all characterized by a strategy of small steps, seem more asserted that followed by concrete actions. However, complementarity between the two organizations still seems possible that NATO could focus on cyberdefense and the EU which has the means to develop the comprehensive approach for cybersecurity. Finally, the European cybersecurity strategy is part of a much broader strategy, more developed in terms of governance and protection of fundamental freedoms, such as data protection and universal access to the Internet.

INTRODUCTION

Le cyberespace est devenu un enjeu majeur dans nos sociétés car il est porteur de la 4ème révolution industrielle, progrès qui s'est amorcé à la fin du siècle précédent, et qui impacte notre monde dans tous les domaines notamment diplomatique, technologique, économique, et social. Les relations internationales et les dernières crises ont parallèlement souligné l'émergence de nouvelles menaces associées à ce milieu qui constituent un défi pour la sécurité et la défense. Facteur aggravant pour l'Europe, elle constitue la zone où il y a le plus de personnes connectées à l'Internet et celle où les transactions par carte bancaire sont les plus nombreuses et les enjeux y sont donc particulièrement importants. Quelques Etats en Europe ont pris conscience de ces enjeux et se sont activement engagés dans ce nouveau milieu en développant une stratégie pour le numérique et en prenant en compte les aspects essentiels concernant sa sécurité. Mais les nombreuses vulnérabilités générées dépassent largement le périmètre de nos frontières nationales et une action plus coordonnée parait donc indispensable. L'UE pourrait jouer un rôle majeur et l'objet de cette étude consiste à s'interroger sur la stratégie mise en place par l'Union pour coordonner l'action des Etats membres ainsi que sur ses relations avec le reste du monde et en particulier avec l'OTAN dans le but de garantir sa sécurité.

L'étude initiale de la question fait apparaître que, bien que l'UE ait élaboré une stratégie de cybersécurité, publiée en février 2013 et reposant sur deux piliers la liberté et la sécurité, la prise en compte en compte des problématiques de défense et de sécurité semble en réalité un peu « embryonnaire », limitée à une rôle de coordination et finalement plutôt à la main des Etats membres qui restent en grande partie souverains sur le sujet. Ce premier constat souligne d'une certaine manière le retour au réalisme dans les relations internationales avec une prédominance des Etats-nations et de leur souveraineté en particulier dans les domaines de la politique étrangère, la sécurité et la défense. Il semblerait que l'Europe se soit en revanche fortement engagée sur les problématiques de gouvernance, de droit et d'accès au cyberespace et en particulier d'Internet avec des motivations d'ordre plutôt économique et sociale. Or, les études réalisées à ce jour sur le sujet ne mettent pas suffisamment en lumière cette orientation plus globale et ne développent que succinctement son éventuelle complémentarité. Cette étude a donc pour ambition d'analyser la pertinence et l'efficacité de cette stratégie avec celle des Etats membres et des organisations internationales et régionales, en particulier de l'OTAN.

Le corpus documentaire se décline en de nombreuses sources que constituent les publications de l'UE, de l'OTAN et de la France. Un certain nombre d'ouvrages et d'articles de spécialistes de la cybersécurité présentent différentes visions du cyberespace et de ses enjeux, analysent les « cyberstratégies » de l'Union Européenne et de l'OTAN et abordent les relations entre les différents acteurs, les Etats et les organisations. En revanche, il n'a pas été jugé utile d'analyser la stratégie de chaque Etat membre en terme de cybersécurité. L'étude prend donc comme hypothèse que les Etats membres se répartissent en trois groupes distincts : ceux conscients de l'ampleur des défis et ayant mis en place des réponses nationales (France, Royaume-Uni et Allemagne), d'autres ayant mis en place des réponses mais n'ayant pas l'ensemble des outils (Etats baltes, Finlande, Suède) et les autres qui n'auraient pas réellement conscience de la question. Enfin, en terme de coopération internationale, l'étude se focalise sur la complémentarité de la cyberstratégie de l'Union Européenne avec l'OTAN, sans trop détailler les autres relations qui se développent avec d'autres Etats et organisations. La difficulté principale dans cette étude réside dans le fait que le sujet évolue extrêmement rapidement et qu'il est particulièrement difficile d'actualiser les données. De plus, si les textes officiels sont nombreux, leur interprétation reste très variable et leur déclinaison concrète est parfois perfectible et difficile à évaluer. Il s'agit donc de présenter une situation à un instant donné et une position qui peut être subjective compte-tenu du décalage parfois sensible entre les écrits et les actes.

La problématique retenue consiste donc à s'interroger sur le périmètre de la cyberstratégie élaborée par l'UE, sur son efficacité en particulier face à la menace sécuritaire et sur sa complémentarité avec les cyberstratégies des Etats membres et celles des organisations internationales, en particulier de l'OTAN.

Nous nous efforcerons donc dans un premier temps de présenter et d'évaluer la stratégie de cybersécurité de l'UE qui repose sur un partage avec les Etats membres. Nous développerons ensuite son intégration au niveau international et surtout son éventuelle complémentarité avec celle de l'OTAN. Enfin, nous démontrerons comment elle s'intègre dans un cybestratégie plus globale davantage affirmée sur les aspects de gouvernance, de protection des libertés individuelles et d'accès au cyberespace.

1. Une stratégie de cybersécurité partagée avec les Etats membres, pour quelle efficacité ?

1.1. Caractéristiques intrinsèques du cyberespace

Le cyberespace est si complexe et son périmètre si vaste et évolutif qu'il apparait extrêmement difficile de le définir simplement. On trouve dans les nombreuses publications sur le sujet et les textes officiels de l'Union européenne, de l'OTAN, et de nombreux autres pays, différentes définitions mais aucune ne semble aujourd'hui faire l'unanimité. Cette ambiguïté sémantique est révélatrice de la complexité de ce nouveau « milieu » qu'il est particulièrement difficile d'appréhender et de maîtriser dans la mesure où il n'y a déjà pas de consensus sur sa définition.

Dans la directive interarmées française relative à la cyberdéfense[1], le cyberespace est décrit comme un milieu à la fois immatériel et technologique. Il s'appuie sur des infrastructures physiques constituées de machines interdépendantes (ordinateurs, serveurs, téléphones, etc...), sur des logiciels et sur des identités virtuelles (adresse IP[2], pseudonymes, avatar, etc...). Il inclut les données numériques ainsi que les systèmes d'information qui les utilisent. C'est aussi un espace qui n'existe et n'a de sens que par l'information et les données – sous forme numérique – qui y transitent, y sont traitées, stockées et archivées.

Olivier Kempf[3] propose pour sa part une définition plus synthétique et probablement plus universelle : « Le cyberespace est l'espace constitué des systèmes informatiques de toute sorte connectés en réseaux et permettant la communication technique et sociale d'informations par des utilisateurs individuels ou collectifs ».

Le cyberespace présente des caractéristiques intrinsèques assez similaires au milieu aérospatial. Il est ainsi un espace dual et extrêmement transverse qui peut être utilisé à des fins civiles et militaires. En effet, il est omniprésent et constitue désormais un socle sur lequel reposent l'ensemble de nos activités modernes. Il forme également un espace continu, mondial et perméable à toute pénétration en s'affranchissant des frontières physiques des Etats. Par ailleurs, l'effacement des distances, la fluidité des mouvements et la rapidité des déplacements

[1] Etat-Major des armées, *Doctrine interarmées de Cyberdéfense DIA 3-40*, 28 mars 2014, 66 p., p. 17.
[2] Internet Protocol.
[3] KEMPF Olivier, *Introduction à la cyberstratégie,* Economica, 2015, 235 p., p. 16.

dans cet espace offrent une grande liberté d'action et lui confèrent ainsi un caractère universel et stratégique. L'accès facilité et peu coûteux aux technologies du cyberespace le rendent potentiellement accessible au plus grand nombre et nous verrons par la suite comment cela constitue à la fois un progrès et des vulnérabilités. Enfin, à l'instar du milieu aérien avant l'apparition du radar, le cyberespace est à ce stade caractérisé par une certaine opacité : il est en effet difficile d'y détecter et identifier les menaces et même, et ceci est plus préoccupant, les attaques.

1.2. Des menaces multiples

Le cyberespace, sur lequel s'appuie la révolution numérique qui est en marche, est donc omniprésent et il constitue une formidable opportunité de progrès dans les domaines technologiques, économiques et sociaux. Si les caractéristiques intrinsèques évoquées ci-dessus et l'hyperconnectivité exponentielle de nos économies et de nos sociétés permettent très clairement de favoriser ce progrès, elles constituent également de nombreuses vulnérabilités et génèrent des menaces.

Une communication de la commission européenne de 2011[4] décrit différentes natures de menaces que l'on peut classer selon leur finalité :

- finalité d'exploitation, comme dans le cas des «menaces persistantes avancées» (APT[5]) à des fins d'espionnage économique et politique, du vol d'identité, des récentes attaques contre des systèmes informatiques gouvernementaux ;
- finalité de perturbation, comme les attaques par déni de service distribué[6] ou le pollupostage[7] par l'intermédiaire de réseaux zombies[8] et la coupure des moyens de communication ;

[4] Communication de la commission européenne, *Protection des infrastructures d'information critiques*, [COM(2011) 163], 31 mars 2011, 19 p., p. 4.

[5] Dans l'expression *Advanced Persistent Threat*, le mot *Advanced* fait référence à des techniques sophistiquées utilisant des logiciels malveillants pour exploiter des vulnérabilités dans les systèmes ; le mot *persistent* suggère qu'un système de commandement et de contrôle externe suit et extrait des données d'une cible sur une longue période de temps ; le mot *threat* indique une implication humaine dans l'orchestration de l'attaque.

[6] Le déni de service distribué est un type d'attaque très évolué visant à rendre inopérante une machine en la submergeant de trafic inutile.

[7] Publication de pourriels (SPAM) sur Internet, le spam, pourriel ou polluriel est une communication électronique non sollicitée, en premier lieu via le courrier électronique. Il s'agit en général d'envois en grande quantité effectués à des fins publicitaires.

- finalité de destruction. Ce scénario ne s'est pas encore concrétisé mais, compte tenu de l'utilisation de plus en plus généralisée des TIC[9] dans les infrastructures critiques (réseaux électriques et systèmes d'alimentation en eau intelligents, par exemple), il ne peut pas être exclu à l'avenir.

Ces menaces peuvent intervenir sous des formes très variables de conflit et une publication de la division recherche du Defense College[10] de l'OTAN en définit une liste exhaustive : l'hactivisme et du vandalisme, la cybercriminalité, le cyberespionnage, le cybersabotage, et enfin le cyberterrorisme, voire la cyberguerre. Les menaces sont donc extrêmement transverses, multiformes, elles sont capables d'impacter l'ensemble des domaines de nos sociétés qu'ils soient civils ou militaires et constituent à ce titre un enjeu absolument central de sécurité pour l'avenir.

1.3. Le cyberespace européen

On peut tout d'abord souligner que la notion de cyberespace n'est pas clairement définie dans la stratégie de cybersécurité de l'Union européenne publiée le 13 février 2013[11]. Il est en effet uniquement fait référence à la cybersécurité qui consiste à mettre en place « les mesures de sauvegarde et les actions auxquelles il est possible de recourir pour protéger le cyberespace, dans les domaines civil et militaire, des menaces associées à ses réseaux interdépendants et à son infrastructure informatique ou susceptibles de leur porter atteinte ». Si aucune définition explicite du cyberespace n'est établie, on constate qu'il est assez mal distingué du réseau Internet même s'il semble englober les infrastructures dites critiques sans vraiment les définir. Les enjeux concernant le réseau Internet sont en revanche particulièrement mis en avant. Le réseau Internet est ainsi considéré comme la colonne vertébrale de l'activité économique de

---

[8] Les criminels distribuent des programmes malveillants capables de transformer votre ordinateur en « bot » (également appelé zombie). Le cas échéant, votre ordinateur peut réaliser des tâches automatisées sur Internet sans que vous le sachiez. En général, les criminels utilisent les zombies pour infecter un grand nombre d'ordinateurs. Ces ordinateurs forment un réseau ou un réseau de zombies.

[9] Technologies de l'information et des communications.

[10] Research Paper, Semantics matter – *NATO, Cyberspace and future threats*, Research Division of the NATO Defense College, Juillet 2014, 12 p., p. 6.

[11] Communication de la commission européenne, *Stratégie de cybersécurité de l'Union européenne : un espace ouvert, sûr et sécurisé*, [JOIN (2013) 1], 7 février 2013, 21 p.

l'Union et le moteur le plus puissant du progrès. Il représente également un lien social de plus en plus affirmé qui constitue au niveau européen « un forum pour la liberté d'expression et l'exercice des droits fondamentaux »[12].

Sa vulnérabilité est soulignée en évoquant qu'il doit être protégé contre les incidents, actes de malveillance et abus, constat qui conduit à lister les actions à mettre en œuvre par les pouvoirs publics pour garantir un « cyberespace libre et sûr »[13], à savoir : sauvegarder l'accès et l'ouverture, respecter et protéger les droits fondamentaux en ligne, préserver la fiabilité et l'interopérabilité d'Internet et tenir compte du rôle moteur des entreprises compte tenu de la dualité du milieu. On peut à ce stade s'interroger sur l'absence de référence explicite à la notion de sécurité qui n'apparait en filigrane qu'en dernière position dans les principes de la cybersécurité[14] établis dans la stratégie et rappelés ci-dessous :

- les valeurs essentielles de l'UE prévalent dans le monde virtuel autant que dans le monde réel ;
- protection des droits fondamentaux, de la liberté d'expression, des données personnelles et de la vie privée ;
- accès à tous ;
- gouvernance participative, démocratique et efficace ;
- une responsabilité partagée pour assurer la sécurité.

Le cyberespace européen souffre donc avant tout d'une absence de définition précise et s'il apparait très clairement centré sur le réseau Internet, les enjeux de sécurité n'apparaissent en première approche pas prioritaires face aux principes de gouvernance, d'accès et de protection des droits fondamentaux qui prédominent.

[12] Ibid. p. 2.
[13] Ibid. p. 2.
[14] Ibid, p. 3-4.

1.4. La montée en puissance d'une stratégie de cybersécurité

C'est à partir de l'année 2000 que l'Union européenne prend conscience de la nécessité de définir et de mettre en place une politique de cybersécurité. Une première politique européenne[15] comprenant deux volets est donc proposée en 2001. Le premier volet vise à renforcer la sécurité des systèmes d'information et des réseaux de l'ensemble des institutions de l'Union européenne. Le second volet doit permettre d'améliorer la cybersécurité de l'ensemble de l'Union en coordonnant ses efforts avec les Etats membres. En 2003, l'Union définit sa première stratégie européenne de sécurité[16], mais comme le souligne Olivier Kempf[17], les cybermenaces ne faisaient pas partie des menaces prioritaires à cette époque et ce n'est qu'en 2008, que le secrétaire général et haut représentant publie un rapport sur la mise en œuvre de cette stratégie de sécurité et actualise la liste. Désormais, cinq menaces majeures sont dénombrées, dont la cybersécurité. La prise de conscience est donc effective et l'Union initie la création d'institutions dédiées à la cybersécurité. Une Direction « sécurité, sureté et SIC » du secrétariat général du conseil (SGC) est chargée de développer les procédures et standards de sécurité garantissant la protection de l'information circulant sur les réseaux de l'Union. Un CERT[18] de l'Union Européenne est créé, même s'il ne sera réellement opérationnel qu'en 2012, avec pour vocation de superviser tous les réseaux des institutions et agences de l'Union et faire l'interface avec les CERT des Etats membres. Enfin, l'ENISA[19] est créé en 2004 dans le but d'offrir une véritable plateforme d'échange et de partage de l'information aux Etats membres.

C'est en 2013, qu'une véritable stratégie de cybersécurité européenne[20] est élaborée. De portée très générale, elle s'intègre dans la stratégie numérique[21] pour l'Europe de 2010 ayant pour but d'une part, de tirer parti du potentiel qui existe dans l'économie européenne et élargir

---

[15] Communication de la commission européenne, *La sécurité des réseaux et de l'information (SRI) : proposition pour une approche politique européenne*, [COM(2001) 298], 6 juin 2001, 30 p.

[16] Journal official de l'Union Européenne, *Stratégie européenne de sécurité*, 12 décembre 2003, 15 p, http://www.consilium.europa.eu/uedocs/cmsUpload/031208ESSIIFR.pdf

[17] KEMPF Olivier, *Alliances et mésalliances dans le cyberespace*, Economica, 2015, 192 p., p. 109.

[18] Computer Emergency Response Team.

[19] European Network and Information Security Agency.

[20] Stratégie de cybersécurité de l'Union européenne, op. cit.

[21] Communication de la commission européenne, *Une stratégie numérique pour l'Europe,* [COM(2010) 245], 19 mai 2010, http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=URISERV%3Asi0016 .

le marché unique et d'autre part, de sécuriser l'Internet pour établir la confiance. Elle repose sur les cinq axes prioritaires ci-dessous :

- Parvenir à la cyber-résilience en améliorant les disparités des réponses nationales, la coordination en cas d'incidents transnationaux et l'engagement des acteurs privés. L'idée ici étant avant tout d'harmoniser le niveau de cybersécurité de chaque Etat membre considérant que cela constitue « un préalable impératif au développement d'une stratégie européenne »[22].
- Faire reculer considérablement la cybercriminalité en s'appuyant sur la convention du Conseil de l'Europe sur la cybercriminalité, dite convention de Budapest[23] et l'EC3[24] récemment constitué.
- Développer une politique et des moyens de cyberdéfense liée à la politique de sécurité et de défense commune (PSDC) de manière à accroître les synergies tout en évitant les doublons notamment avec l'OTAN. Il s'agit avant tout de promouvoir le dialogue et la coordination entre les acteurs civils et militaires, et maintenir un dialogue avec les partenaires internationaux, notamment l'OTAN. Si ce dialogue existait déjà, « le pas franchi est majeur »[25] dans la mesure où l'Union européenne peut s'occuper de cyberdéfense, ce qu'elle refusait jusque-là.
- Développer les ressources industrielles et technologiques en matière de cybersécurité dans le but de promouvoir un marché unique des produits de cybersécurité afin d'éviter tout risque de dépendance excessive de l'Union aux prestataires non européens en matière d'outils de cybersécurité. Il s'agit donc de développer des labels et d'adopter des standards en vue de créer des certifications de niveau européen. A noter tout de même que comme l'indiquent Vincent Joubert et Jean-Loup Samaan[26], l'encouragement d'un développement de technologies européennes pour le cybersécurité ne s'inscrit ainsi pas tant dans une logique strictement sécuritaire que dans une démarche de relance économique et industrielle en cohérence avec la stratégie « Europe 2020 ».

[22] Observatoire du monde cybernétique, *La stratégie de cybersécurité de l'union européenne*, lettre n°14, DGRIS, février 2013, 13 p., p. 8.
[23] Convention sur la cybercriminalité, Budapest, 23 novembre 2001, 30 p.
[24] European Cybercrime Center d'Europol.
[25] KEMPF Olivier, *La cyberstratégie de l'union européenne*, Sécurité Globale n°24, été 2013, p. 25-40., p. 8.
[26] JOUBERT Vincent, SAMAAN Jean-Loup, *L'intergouvernementalité dans le cyberespace : étude comparée des initiatives de l'Otan et de l'UE*, Revue HERODOTE n°152-153 – 2014/1, p. 261-275., p. 12.

- Instaurer une politique internationale de l'Union européenne, notamment en coordination avec l'OTAN, cohérente en matière de cyberespace et promouvoir les valeurs essentielles de l'Union européenne.

1.5. Mais en grande partie déléguée aux Etats membres

Cette première stratégie de cybersécurité européenne autonome constitue donc une prise de conscience importante et met en place un ensemble de principes tout à fait intéressants pour coordonner les actions. Cela dit, le document[27] admet tout de même que « Les administrations nationales semblent les mieux placées pour organiser la prévention et l'intervention en cas de cyberincident et de cyberattaque et pour établir des contacts et des réseaux avec le secteur privé et le grand public ». En effet, la cybersécurité est un domaine extrêmement sensible dans lequel la notion de confiance est absolument centrale et il est très clairement considéré, par de nombreux Etats membres, comme un domaine souverain et donc d'une certaine manière incompatible avec cette volonté de stratégie commune. De nombreux Etats européens n'ont d'ailleurs pas attendu l'Union européenne pour développer des capacités de cybersécurité et de cyberdéfense. Le Royaume-Uni, l'Allemagne et la France sont à ce stade, les trois membres qui se sont le plus engagés dans ce domaine et qui ont massivement investi[28]. L'UE se retrouve donc partagée entre des actions nationales extrêmement disparates entre les Etats membres et une action commune, avant tout de coordination et de partage de bonnes pratiques, qui semble indispensable mais qui présente un certain nombre de limites.

Tout d'abord, les Etats n'ont pas le même niveau de préparation et compte-tenu des caractéristiques intrinsèques du cyberespace évoquées plus haut et du caractère sans frontières de la menace, cela constitue clairement une faiblesse. En effet, la force d'une chaîne dépend de son maillon le plus faible et la cybersécurité européenne pâtit de cette hétérogénéité du niveau de sécurité atteint par ses Etats membres qui peut s'expliquer par des contraintes économiques ou structurelles mais aussi et surtout souvent par une divergence d'intérêts. De plus, la stratégie actuelle repose avant tout sur la base d'une coopération

[27] Stratégie de cybersécurité de l'Union européenne, op. cit., p. 18.
[28] Soit 2,7 milliards d'euros d'ici 2020 pour le Royaume-Uni, une *« stratégie en matière de cybersécurité pour l'Allemagne »* pour l'Allemagne *établie en 2011 avec un budget et des effectifs en constante augmentation* et plus de 1 milliards d'euros d'ici 2019 pour la France.

volontaire et les agences de l'Union européenne n'ont ainsi aucun pouvoir de contrainte et ne peuvent proposer que des recommandations. En effet, même si une directive[29] dite « SRI[30] » accompagne cette stratégie, il ne s'agit pas d'un règlement et sa déclinaison, sujette à interprétation et arbitrage au niveau des Etats, limite par nature sa portée.

Pour améliorer clairement le niveau global de sécurité, il serait indispensable de développer beaucoup plus largement l'échange de renseignements, de communiquer le plus ouvertement possible sur les incidents subis par chaque Etats dans leur sphère civile mais aussi militaire. Or, ce point semble particulièrement délicat lorsqu'il s'agit par exemple d'entreprises privées, peu enclines à afficher leurs vulnérabilités au plus grand nombre. La plus grande difficulté est donc que les Etats opposent souvent la notion de souveraineté à toute velléité d'extension ou de mise en commun de capacités en particulier dans ce domaine considéré comme régalien. Facteur aggravant, les révélations d'Edward Snowden sur les programmes de surveillance des américains ciblant les systèmes et réseaux européens ont démontré l'inefficacité actuelle des mesures de protection mises en place par l'Union et par ses Etats membres. On peut dès lors craindre que « les Etats soient tentés de se replier sur eux-mêmes pour garantir la sécurité de leurs réseaux, délaissant une solution commune qui paraît pour le moment bien futile»[31].

1.6. En étroite collaboration avec le secteur privé

Comme évoqué précédemment, cette stratégie intègre un volet important concernant la protection des installations des infrastructures d'information critiques[32] qui est développé dans son premier axe ayant pour but d'améliorer la cyber-résilience et qui fait l'objet d'une directive[33] SRI dédiée accompagnant la stratégie. Sachant que l'objectif de ce programme est avant tout de garantir un haut niveau commun de sécurité des systèmes d'information pour l'amélioration de la sécurité sur Internet, les réseaux privés et l'information vitale au fonctionnement des sociétés de l'Union européenne, les leviers de contrôle et d'amélioration

[29] Directive du Parlement européen et du Conseil, *Proposition de directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union n°2013/0027*, 7 février 2013 (+ version du 18 décembre 2015), 55 p.
[30] Sécurité des Réseaux et de l'Information.
[31] JOUBERT Vincent, op. cit., p. 13.
[32] PIIC.
[33] Directive du Parlement européen et du Conseil, op. cit.

se situent avant tout dans le secteur privé qui contrôle majoritairement le cyberespace. Concrètement, il s'agit donc de contraindre les Etats membres et les sociétés correspondantes, nommées « opérateurs de services essentiels »[34], à renforcer les mesures de sécurité, de résilience des infrastructures dans les secteurs jugées critiques (transports, énergie, santé, services financiers…) ainsi qu'imposer l'adoption de procédures de gestion du risque et d'obligation de signalisation d'incidents. Peuvent également être concernées, les sociétés de services informatiques y compris magasins d'applications en ligne, les plateformes de commerce électronique, de paiement par Internet et d'informatique en nuage, les moteurs de recherche et les réseaux sociaux. Si ce programme a fait l'objet d'une première publication en 2009, des progrès ont été réalisés depuis et dans ce cadre, une publication de la DGRIS[35] de septembre 2015[36] annonce le lancement du réseau d'alerte CIWIN[37] début 2013. Il s'agit d'un portail numérique permettant aux acteurs européens de la protection d'infrastructures critiques d'échanger de l'information sur les vulnérabilités et menaces, ainsi que sur les bonnes pratiques. Parallèlement, un autre projet, ECOSSIAN[38] a été lancé en 2014. Il porte sur la réalisation d'une plateforme dont l'objectif est d'améliorer la détection et la gestion des cyber-attaques contre les infrastructures critiques, en s'appuyant sur un système d'alerte à l'échelle européenne (SOC ou Security Operation Center) et une base de connaissances collaborative. Enfin, la dernière version de la directive établit également une première liste de ces infrastructures jugées critiques qui est désormais suivie et régulièrement mise à jour.

Le deuxième volet de collaboration avec le secteur privé concerne le quatrième axe de la stratégie consistant à développer au niveau européen des ressources industrielles et technologiques propres. Le cyberespace européen est en effet à ce stade extrêmement dépendant des technologies de l'information fournies par des prestataires non européens et majoritairement américains voire chinois. Or, la confiance, dans ce domaine, ne pouvant jamais être totale, il apparait indispensable que nous nous assurions que les composants et logiciels supportant nos activités critiques et vitales soient « dignes de confiance », sécurisées et qu'ils

[34] Nommés « Opérateurs d'importance vitale » en France.
[35] Direction Générale des Relations Internationales et de la Stratégie.
[36] Observatoire du monde cybernétique, *Les relations transfrontalières et les infrastructures critiques*, lettre n°42, DGRIS, septembre 2015, p. 2-5.
[37] Critical Infrastructure Warning Information Network.
[38] European COntrol System Security Incident Analysis Network.

garantissent la protection des données personnelles. Il s'agit en particulier de pouvoir avoir une confiance totale dans les éléments de sécurité tels que les équipements de chiffrement, les sondes de détection d'intrusion mais aussi tous les systèmes d'informations sensibles que ce soit dans le domaine civil ou militaire, allant même, comme le suggère Pierre Bellanger[39], jusqu'à envisager le développement d'un système d'exploitation européen.

1.7. Une cyberdéfense quasi-absente

Si la notion de cybersécurité dans son sens le plus large est assez bien développée dans la cyberstratégie européenne, elle ne prend pas clairement en compte la notion de cyberdefense. Dans la directive interarmées française relative à la cyberdéfense[40], la cybersécurité est décomposée en deux notions complémentaires. D'une part, la cyberprotection qui consiste à préserver la disponibilité, l'intégrité et la confidentialité de nos systèmes. D'autre part, la cyberdéfense dont l'objectif complémentaire consiste à planifier et à conduire des actions défensives ou offensives dans le cyberespace à la fois pour être en mesure de faire face à une attaque, voire d'y répondre. La stratégie européenne ne distingue pas ces deux volets complémentaires et le périmètre de la cybersécurité « qui vise à préserver la disponibilité et l'intégrité des réseaux et de l'infrastructure ainsi que la confidentialité des informations qui y sont contenues »[41] semble se limiter à la cyberprotection. La cyberdéfense semble, quant à elle, bornée au domaine de la défense et donc de la PSDC alors qu'il est impératif qu'il soit étendu au secteur civil compte-tenu de la dualité du cyberespace.

Cette ambiguïté, à minima sémantique, est révélatrice d'une problématique plus profonde qui s'explique avant tout par des raisons culturelles et historiques. En effet, « l'esprit de l'Europe est avant tout humaniste et n'a jamais eu l'ambition d'être militaire »[42] et l'Union européenne a toujours été avant tout « une puissance civile et la notion de défense lui est donc peu familière malgré le développement de la PSDC dans le traité de Lisbonne »[43]. D'ailleurs, même « si l'article 42.7 établit un devoir d'aide et d'assistance par tous les moyens en leur pouvoir, il précise que l'OTAN, pour les pays de L'Union qui en sont signataires, reste le fondement de leur

[39] BELLANGER Pierre, *Conférence devant l'IHEDN : Enjeux et moyens de notre souveraineté numérique,* 2014.
[40] Etat-Major des armées, op. cit., p. 17.
[41] Stratégie de cybersécurité de l'Union européenne, op. cit., 7 février 2013, p. 18.
[42] KEMPF Olivier, op. cit., p. 108.
[43] Ibid p. 101.

défense »[44]. Ce sentiment s'est même probablement renforcé depuis l'entrée en 2004 dans l'Union des pays européens se reposant presque intégralement sur l'OTAN pour leur défense. Par conséquent, même si la notion de cyberdéfense est évoquée dans la stratégie et qu'il s'agit déjà d'une avancée majeure, les actions concrètes relatives à une véritable activité de cyberdéfense de l'Union européenne ne sont clairement pas mises en avant, l'Union ayant semble-t-il tendance à se considérer comme un acteur mineur dans ce domaine. Au final, comme le souligne l'observatoire du monde cybernétique, « la cyberdéfense reste la grande absente de la stratégie européenne. Si le document précise vouloir développer une politique et des moyens de cyberdéfense, en liaison avec la politique de sécurité et de défense commune (PSDC), il reste muet sur les modalités de ce développement » [45].

Au-delà de la simple évocation de la notion de cyberdéfense et de la volonté affichée de l'Europe, on peut tout de même constater quelques avancées concrètes. Il s'agit tout d'abord de l'intégration, dans la stratégie de 2013, de la cyberattaque dans le système de cohésion de sécurité et de défense, mis en place par l'article 222 du traité de Lisbonne, qui constitue en soi une véritable prise de conscience de la menace. Comme le souligne Olivier Kempf[46], c'est d'autant plus remarquable que l'Alliance atlantique se refusait pour sa part jusqu'en 2014 à inclure les cyberattaques sous la couverture de l'article 5 du traité de l'Atlantique Nord. Deuxième avancée concrète, quelques Etats membres, dont la France, participe activement aux travaux capacitaires initiés et conduits par l'AED[47] dans le domaine de la cyberdéfense, où existe une « Project Team » dédiée à ce sujet. Ceci reste à ce stade relativement embryonnaire pour la partie défense, un peu moins pour la partie de lutte contre la cybercriminalité mais le comité directeur de l'AED a fixé 16 priorités dans son plan de développement capacitaire incluant des capacités de cyberdéfense[48].

Comme le souligne Olivier Kempf[49], cette stratégie de cybersécurité ne constitue ainsi ni une totale nouveauté, ni un aboutissement mais il s'agit d'un texte novateur qui marque une vraie prise de conscience et des ambitions relativement solides. Elle constitue en effet une voie

[44] Traité de Lisbonne, article 42.7, 410 p., 1er décembre 2009, p.40.
[45] Observatoire du monde cybernétique, op. cit., p. 10.
[46] KEMPF Olivier, op. cit., p. 33.
[47] Agence Européenne de Défense.
[48] KEMPF Olivier, op. cit., p. 102.
[49] KEMPF Olivier, op. cit., p. 2.

moyenne pour assurer des tâches de protection, de sécurité et même de défense et elle réussit à ménager les grands équilibres tout en traçant des objectifs de court et de moyen terme. L'affirmation de responsabilités partagées entre le niveau national et le niveau européen est mentionnée et les acteurs privés sont intégrés dans la stratégie. De plus, Les organes d'exécution sont mis en place et renforcés, ainsi que les instruments juridiques qui soutiennent l'ensemble. Cependant des ambiguïtés sémantiques demeurent avec notamment une distinction peu claire entre cybersécurité et cyberdéfense et la répartition des responsabilités entre les différents acteurs demeure peu précise.

Enfin, si cette stratégie ambitionne d'élever le niveau moyen de cybersécurité de l'Europe, elle souligne également l'importance de la coopération entre Etats et avec les organisations internationales et régionales dont l'OTAN.

2. Une stratégie de cybersécurité s'intégrant au niveau international et en complémentarité avec celle de l'OTAN ?

En effet, l'importance de la coopération entre Etats mais aussi avec les organisations internationales et régionales est assez largement soulignée compte-tenu de la nature de cette menace extrêmement transverse et sans frontières. Mais sachant que l'OTAN, qui dispose de 22 membres en commun avec l'UE, semble également s'investir dans le domaine, quelle complémentarité est envisageable ?

2.1. Une coopération internationale nécessaire mais difficile

Le cinquième axe de la cyberstratégie européenne concerne la coopération en particulier avec l'OTAN et l'instauration d'une politique internationale en matière de cyberespace. Par nature l'Europe a pour principal objectif d'encourager les relations transfrontalières dans le but de renforcer les collaborations économiques et technologiques dans différents domaines comme l'énergie, le transport, les communications, les finances, les médias…etc. Ces échanges dans le cyberespace constituent très clairement une menace transfrontalière et il apparait donc indispensable de développer une coopération permettant d'y faire face.

De par la nature duale et sans frontière du cyberespace, cette stratégie nécessitent de mettre en place et d'entretenir un dialogue et un partage, nous l'avons vu, avec les Etats membres

mais aussi et plus largement avec d'autres pays étrangers et des organisations régionales et internationales. De plus, si la dualité entre civil et militaire caractérise le cyberespace, les menaces qui en résultent sont souvent difficilement imputables. Un certain degré de coopération pourrait donc à la fois contribuer au recueil de renseignements, mais aussi à réduire la part d'incertitude.

L'opacité du cyberespace permet toutes les manœuvres occultes et toutes les manipulations dans toutes les couches car il n'y a jamais d'ami, ni d'ennemi absolu. S'allier dans le domaine cyber suppose le partage de l'information et ce partage peut signifier un affaiblissement potentiel puisque l'on perd de l'opacité. Dans le cyberespace, il s'agit donc de s'allier à celui avec lequel on est le plus disposé à partager ses secrets et surtout ses vulnérabilités qui constituent ses faiblesses. On peut souligner que c'est l'inverse dans le système traditionnel des alliances où il s'agit plus souvent de partager ses forces. C'est donc probablement pour ces raisons que cette stratégie de coopération dans le domaine de la cybersécurité semble perfectible dans la mesure il apparait clairement plus réaliste de privilégier les coopérations en bilatéral, plus facile à maîtriser qu'en multinational dans la mesure où cela restreint l'espace de confiance.

2.2. Des coopérations plutôt bilatérales que multilatérales

Le domaine cyber est donc un domaine considéré, par de nombreux Etats membres, comme souverain où la notion de confiance, très relative, est tout à fait centrale. En complément de la coopération mise en place par l'Union européenne avec l'ensemble de ses Etats membres, dans le cadre de sa cyberstratégie, des coopérations plus spécifiques se sont donc développées en bilatéral. Il s'agit souvent d'alliances de circonstance avec une stratégie des petits pas, plus conforme au besoin de maitrise de l'espace de confiance de chacun.

Le Livre blanc français de la défense et de la sécurité nationale de 2013 évoque par exemple ce point tout en soulignant le besoin de renforcer la stratégie européenne dans ce domaine : « toute politique ambitieuse de cyberdéfense passe par le développement de relations étroites entre partenaires internationaux de confiance. Les relations seront approfondies avec nos partenaires privilégiés, au premier rang desquels se placent le Royaume-Uni et l'Allemagne. Au niveau européen, la France soutient la mise en place d'une politique européenne de

renforcement de la protection contre le risque cyber des infrastructures vitales et des réseaux de communications électroniques ».

Les exemples de coopération multilatérale sont nombreux. La France coopère par exemple avec le Royaume-Uni dans le cadre des accords de Lancaster House. En effet, un des 13 domaines de coopération concerne les cyberattaques et il s'agit de travailler sur le renforcement de la résilience des deux systèmes nationaux et communs. La France échange également avec l'Allemagne[50] et les premiers pas concernent l'harmonisation des standards et la labellisation des produits et services fiables dans les deux pays. La coopération avec la Belgique[51] se développe aussi largement notamment vis-à-vis du cyberterrosisme suite aux récents attentats qui ont touché les deux pays. Enfin, les échanges se sont multipliés avec les Etats-Unis, en premier lieu au sujet de la protection des données personnelles qui constitue un volet important de la cyberstratégie européenne, mais également en matière de formation et d'exercices. Une coopération s'est ainsi développée sur le sujet avec pour principal objectif de partager l'information et les bonnes pratiques entre spécialistes, écoles militaires et universités françaises et américaines.

2.3. Une politique affirmée de l'OTAN en matière de cybersécurité

C'est lors de la guerre au Kosovo en 1999 que l'OTAN prend véritablement de conscience de la menace cyber. L'OTAN est en effet confrontée à sa première attaque cyber d'envergure et son infrastructure du réseau Internet est attaquée en mars 1999 par des hackers serbes[52]. Le sujet de la menace cyber est évoqué pour la première fois lors du sommet de Prague en 2002 et il mentionné dans la déclaration. Mais son traitement est avant tout abordé sous l'angle technique et l'OTAN passe un contrat en 2003 avec la société FINMECCANICA pour mettre en place le NCIRC[53]. Il ne sera pleinement opérationnel que fin 2012 et a en charge de coordonner les capacités de réponse technique et opérationnelle pour assurer la protection des propres systèmes d'information et de communication de l'OTAN. Les cyberattaques de 2007 contre l'Estonie vont accélérer les choses d'autant plus que la république balte était désormais

[50] http://www.lepoint.fr/chroniqueurs-du-point/guerric-poncet/cyberdefense-berlin-et-paris-vont-elles-reveiller-l-europe-21-01-2015-1898242_506.php
[51] https://actupolicing.com/2016/02/05/la-france-et-la-belgique-renforcent-leur-cooperation-antiterroriste/
[52] Research Paper, Semantics matter, op. cit., p. 3.
[53] NATO Computer Incidence Response Capability.

pleinement alliée. En effet, la première politique de cyberdéfense est approuvée au sommet de Bucarest en avril 2008, signe que le sujet est désormais traité au plus haut niveau, et deux organismes dédiés à la cyberdéfense sont créés. D'une part, l'autorité de gestion de la cyberdéfense[54] en charge de la coordination des activités de cyberdéfense et d'autre part, le centre d'excellence de cyberdéfense de l'OTAN en Estonie. Par la suite, un nouveau concept stratégique de l'OTAN[55] est adopté lors du sommet de Lisbonne en novembre 2010 et deux articles sont consacrés à la cyberdéfense. L'OTAN franchit une étape majeure le 7 juin 2011 avec l'approbation par les ministres de la défense d'une politique OTAN de cyberdéfense et d'un plan d'actions associé régulièrement révisé depuis. Enfin, la montée en puissance de la cyberdéfense dans l'OTAN se concrétise lors du sommet de Galles en mai 2014 avec le placement d'une agression cyber majeure dans le cadre de l'article 5, celui de la défense collective. Comme le souligne Olivier Kempf, « il s'agit d'un pas important même si rien n'est dit sur le seuil[56] ».

Cette politique cyberdéfense de l'OTAN repose sur quatre domaines d'actions[57]. Dans un premier temps, l'OTAN doit coordonner les travaux au niveau opérationnel et elle s'appuie pour cela sur le CDMA. Le NCIRC, qui appartient à la NCIA[58], assure pour sa part la fourniture des services techniques et opérationnels assurant la cybersécurité, il planifie les exercices, notamment l'exercice annuel Cyber Coalition et assure l'interface avec les organisations internationale dont l'Union européenne. Cette politique prévoit également l'aide aux alliés avec la possibilité d'envoyer une équipe de réaction rapide[59] pour intervenir en cas de besoin sur les interconnexions entre les réseaux de l'OTAN et les réseaux nationaux. Troisième volet, la recherche et la formation au travers notamment du centre d'excellence pour la cyberdefense homologué en 2008 avec onze pays participants dont la France. Enfin, l'OTAN prévoit d'aider les partenaires au cas par cas.

[54] CDMA - Cyber Defense Management Authority.
[55] *Concept stratégique pour la défense et la sécurité des membres de l'Organisation du Traité de l'Atlantique Nord*, Sommet de Lisbonne, 2010, 42 p.
[56] KEMPF Olivier, op. cit., p. 93.
[57] KEMPF Olivier, *L'OTAN et la cyberdéfense, article n°III.6,* Chaire de cyberdéfense et cybersécurité de l'école de Saint-Cyr, mai 2013, 8 p., p. 6.
[58] NATO Communication and Information Agency.
[59] RRT.

En synthèse, on constate que la politique de l'OTAN dans le domaine cyber est clairement centrée sur la défense de ses propres réseaux et l'intégration de ce domaine dans le processus de planification de ses opérations. Si l'on se réfère aux notions définies au 1.7, on peut en conclure que l'OTAN se focalise donc sur la cyberprotection et n'évoque que très peu la notion de cyberdéfense et les raisons sont avant tout d'ordre politique. En effet, comme cela est souligné dans la revue HERODOTE de 2014[60], « si le principe de défendre les réseaux propres de l'Alliance est agréé par les 28 Etats membres, l'idée d'un rôle accru et plus englobant de l'organisation dans le domaine est encore loin de susciter un consensus dans une organisation qui ne peut décider sans unanimité ». De plus, certains pays comme la France, l'Allemagne et le Royaume-Uni ont massivement investi dans le domaine et ne souhaitent pas voir leur souveraineté s'effriter en raison d'une mutualisation de leurs ressources avec les autres alliés. Enfin, il n'y a actuellement pas d'accord sur la problématique des capacités offensives compte-tenu notamment du flou juridique entourant ce type d'opérations.

2.4. Une volonté de coopération avec l'Union Européenne mais un partage flou des responsabilités

L'OTAN, comme l'Union Européenne démontre une volonté affirmée de coopération. En effet, l'Union européenne prévoit, dans le cadre du troisième axe prioritaire de sa cyberstratégie consacré au développement d'une politique et des moyens de cyberdéfense, « d'étudier les différentes possibilités de conjuguer les efforts de l'Union européenne et de l'OTAN pour accroître la résilience des infrastructures critiques d'Etat, de défense ou d'information dont dépendent les membres des deux organisations »[61]. De son côté, l'OTAN déclare en 2012 au sommet de Chicago avoir pour objectif de « coopérer avec l'Union européenne, l'ONU et l'OSCE en vue d'accroître la coopération concrète »[62]. Si cette coopération ambitionne d'accroître les synergies y compris dans le domaine militaire, les deux organisations semblent avoir à cœur d'éviter les doublons et la redondance entre leurs activités et leurs capacités de cyberdéfense. Cela a notamment été souligné par un expert de l'Agence Européenne de Défense[63] qui déclare que « les capacités de cyberdéfense qui pourront être employées par l'UE dans le cadre de

[60] JOUBERT Vincent, op. cit. p. 13.
[61] Stratégie de cybersécurité de l'Union européenne, op. cit., p. 12.
[62] KEMPF Olivier, op. cit., p. 92.
[63] JOUBERT Vincent, op. cit., p. 271.

missions PSDC seront cohérentes avec les besoins opérationnels et ne devraient pas reproduire les capacités OTAN existantes, ce ne serait dans l'intérêt de personne ».

Mais si cette volonté de coopérer est clairement affirmée, les textes restent assez flous sur le partage des tâches et les actions concrètes. On comprend en effet qu'il y a bien des travaux en commun entre l'Union européenne et l'OTAN, notamment dans le domaine capacitaire, mais qu'il apparait difficile de trouver des axes d'effort concrets notamment dans le domaine militaire. La raison principale est ici aussi en grande partie liée à la notion de souveraineté, chère à la majorité des Etats membres des deux organisations. En effet, comme le soulignent Vincent Joubert et Jean-Loup Samaan dans la revue HERODOTE[64] : « Une certaine confusion règne sur les rôles de l'OTAN et de l'Union européenne dans le domaine, notamment en ce qui concerne la sphère militaire », « in fine, c'est surtout la question de la souveraineté nationale qui constitue une ligne rouge de la coopération intergouvernementale et qui freine les efforts tant de l'OTAN que de l'UE ». Ce silence des textes sur les détails de cette coopération est probablement révélateur et comme le précise Olivier Kempf, cette « prudence diplomatique suggère de vrais différends, qui reposent peut-être sur des intérêts profonds et les celer n'est pas la meilleure façon de les résoudre »[65]. Ainsi, ce flou a au moins le mérite de ne pas cadrer, ni trop restreindre le niveau de coopération afin de laisser une large marge de manœuvre, qui pourrait constituer un espoir pour le développement de cette coopération et de la complémentarité des deux organisations dans le domaine. On peut tout de même souligner quelques avancées concrètes avec notamment la signature le 10 février 2016 d'un arrangement technique[66] entre la capacité OTAN de réaction aux incidents informatiques (NCIRC) et le centre d'alerte et de réaction aux attaques informatiques (CERT-UE) de l'Union européenne. L'objectif étant de fixer un cadre pour l'échange d'informations et le partage de bonnes pratiques entre les équipes d'intervention, il s'agit, comme l'a expliqué Pedro Serrano, adjoint du Service européen pour l'action extérieure[67], d'un développement très important pour la coopération opérationnelle entre les deux organisations.

[64] JOUBERT Vincent, op. cit., p. 271, p. 16.
[65] KEMPF Olivier, op. cit., p. 15.
[66] Communiqué OTAN, L'OTAN et l'Union européenne renforcent leur coopération en matière de cyberdéfense, 10 février 2016, http://www.nato.int/cps/fr/natohq/news_127836.htm .
[67] Id.

2.5. Une possible complémentarité avec l'OTAN ?

Si cette coopération manque pourtant visiblement un peu de consistance, une complémentarité entre les deux organisations semble pourtant possible. D'un côté, l'OTAN est par nature une alliance militaire défensive, qui même si elle s'est en pratique très engagée dans les opérations durant les deux dernières décennies, est revenue à une logique défensive, son ADN, depuis 2014. Son action dans le cyberespace pourrait donc utilement se focaliser sur ce qu'elle sait faire de mieux : défendre ses réseaux et développer l'interopérabilité pour faciliter les opérations militaires interalliées de gestion des crises. L'Union européenne, quant à elle, qui est une puissance avant tout civile, dispose d'une gamme beaucoup plus étendue d'instruments réglementaires, politiques, économiques et sociaux qui peuvent lui permettre de répondre plus efficacement à la nature duale des défis du cyberespace. En effet, partant du constat que le cyberespace, notamment la grande majorité des infrastructures d'importance vitale, est majoritairement contrôlé par des compagnies privées, l'Union européenne présente l'avantage de disposer de moyens contraignants qui peuvent être mobilisés vis-à-vis des entreprises, l'OTAN n'ayant que peu de prises sur ce type d'acteurs. Si sa priorité consiste très clairement à renforcer la résilience des infrastructures critiques, elle dispose également de nombreux leviers permettant d'agir dans les domaines économiques et sociaux et développe une approche donc moins militaire que l'OTAN mais beaucoup plus globale.

Dans le domaine de la gestion des crises, cette approche globale de l'Union présente de sérieux atouts pour développer plus en avant son concept de réforme du secteur de sécurité et y intégrer un volet cybersécurité, à la fois préalable et complémentaire avec les actions dans les domaines de la gouvernance et du développement économique. Cette possible complémentarité entre les deux organisations rencontre d'ailleurs un écho avec notre actualité qui conduit à rapprocher les notions de sécurité et de défense. La dualité du cyberespace impose très clairement que ces deux notions ne soient pas dissociées et la coopération entre l'OTAN et l'Union européenne parait donc, à ce titre, plus que jamais nécessaire.

Mais si l'Union européenne semble avoir pris conscience de l'importance de cette coopération internationale et avec l'OTAN pour conjuguer les efforts et améliorer le niveau de cybersécurité, elle affiche une cyberstratégie beaucoup plus globale, davantage affirmée en terme de gouvernance et de protection des libertés fondamentales.

3. Une stratégie de sécurité qui s'intègre dans une stratégie plus globale, davantage affirmée en terme de gouvernance et de protection des libertés fondamentales

L'Union européenne s'est donc investi pour contribuer à améliorer la cybersécurité de ses Etats membres et cherche à développer une certaine complémentarité avec l'OTAN. Mais cette stratégie de cybersécurité ne constitue qu'un maillon de la cyberstratégie de l'UE qui intègre également et surtout des considérations économiques mais aussi de gouvernance de l'Internet, de protection des libertés individuelles et enfin d'accès universel.

3.1. Promouvoir la bonne gouvernance de l'Internet

En effet, un des principaux axes de la stratégie de cybersécurité de l'Union européenne, établie en 2013, consiste à « instaurer une politique internationale cohérente en matière de cyberespace et à promouvoir les valeurs essentielles de l'Union »[68] et en particulier une bonne gouvernance de l'Internet. Il s'agit pour l'Europe de favoriser une gouvernance de l'Internet permettant de garantir un espace à la fois ouvert, libre et sûr.

L'Internet né dans les années 60 aux Etats-Unis a connu un succès grandissant, 40% de la population mondiale s'y connecte aujourd'hui[69] et si l'Europe héberge le plus de personnes connectées, l'Internet que nous utilisons est très largement américain et porté par de grands acteurs privés qui défient les Etats. Ainsi, si aucune autorité centrale ne gouverne directement l'Internet, c'est un ensemble d'organismes (IETF[70], IAB[71], ICANN[72]…) qui participent à une forme d'autorégulation du réseau dont la gouvernance est tout de même de fait américaine[73]. Or, Internet est très clairement devenu le socle du développement de nos sociétés, il révolutionne les modèles économiques et sociaux et constitue donc à ce titre un facteur important de vulnérabilité compte tenu de notre dépendance à son égard. Les révélations d'Edward Snowden en 2013 ont d'ailleurs transformé l'Internet, devenu outil de surveillance, en un sujet politique et les Etats-Unis, jusque-là « garants » de la liberté en ligne, ont perdu leur crédibilité

[68] Stratégie de cybersécurité de l'Union européenne, op. cit., p. *16.*
[69] MORIN-DESAILLY Catherine, *L'Europe au secours de l'Internet : démocratiser la gouvernance de l'Internet en s'appuyant sur une ambition politique et industrielle européenne*, Note de synthèse du rapport sénatorial n°696, 8 juillet 2014, 6 p., p. 1.
[70] Internet Engineering Task Force.
[71] Internet Architecture Board.
[72] Internet Corporation for Assigned Names and Numbers.
[73] MORIN-DESAILLY Catherine, op. cit., p. 2.

morale sur l'Internet. Il s'agit donc pour l'Europe de militer pour une gouvernance plus équilibrée, plus démocratique, et de promouvoir une appropriation citoyenne de l'Internet. Pour l'Europe, cette gouvernance rénovée doit permettre de garantir que la croissance exponentielle de la connectivité mondiale ne s'accompagne pas de censure, ni de surveillance de masse. L'Union ambitionne donc d'encourager les efforts pour élaborer des règles de conduite et de réaffirmer « l'importance de toutes les parties prenantes dans le modèle actuel de gouvernance Internet, en soutenant une approche de gouvernance participative[74] ».

3.2. Pérenniser les activités économiques

Mais si la stratégie de cybersécurité européenne vise un cyberespace libre et sûr, les enjeux sont avant tout économiques comme cela est souligné par Vincent Joubert et Jean-Loup Samaan[75] : « l'encouragement d'un développement de technologies européennes pour le cybersécurité ne s'inscrit ainsi pas tant dans une logique strictement sécuritaire que dans une démarche de relance économique et industrielle en cohérence avec la stratégie Europe 2020 ». Dans ce cadre, l'Europe a élaboré une stratégie numérique pour l'Europe[76] ayant pour principaux objectifs de tirer parti du potentiel qui existe dans l'économie européenne et élargir le marché unique mais aussi de sécuriser l'Internet pour instaurer un climat de confiance. Les actions concrètes consistent en un certain nombre de mesures d'harmonisation telles que le commerce électronique, l'itinérance ou encore la carte d'identité et la signature électroniques.
La stratégie de cybersécurité européenne décline donc également cette volonté de sécuriser le cyberespace, véritable colonne vertébrale de l'activité économique de l'Union. Elle confirme notamment que le cyberespace, qui ne se limite pas à l'Internet mais intègre les infrastructures dites critiques, est devenu « le nerf de la croissance et une ressource critique dont dépendent tous les secteurs économiques »[77]. Il constitue en effet les systèmes complexes qui permettent à l'activité économique de s'exercer dans des secteurs clés comme la finance, la santé, l'énergie et les transports. Le bon fonctionnement de ces systèmes informatiques est assurément devenu un enjeu stratégique pour nombre d'entreprises qui doivent impérativement pouvoir compter sur leur disponibilité, leur intégrité et leur confidentialité.

[74] Stratégie de cybersécurité de l'Union européenne, op. cit., p. 4.
[75] JOUBERT Vincent, op. cit., p. 12.
[76] Une stratégie numérique pour l'Europe, op. cit.
[77] Stratégie de cybersécurité de l'Union européenne, op. cit., p. 2.

3.3. Garantir les libertés individuelles

Mais si l'Union européenne a bien pris conscience des enjeux liés au cyberespace et aux impératifs de sécurité, sa stratégie souligne très clairement que cette sécurisation ne doit pas se faire au détriment des libertés individuelles. Il s'agit donc pour l'Europe de trouver un équilibre entre sécurité et liberté en garantissant notamment les droits fondamentaux consacrés par la Charte des droits fondamentaux de l'Union européenne. L'Europe considère en effet que le cyberespace représente un lien social de plus en plus affirmé qui constitue au niveau européen « un forum pour la liberté d'expression et l'exercice des droits fondamentaux »[78]. Sa cyberstratégie fixe donc deux impératifs que sont la liberté d'expression et la protection des données personnelles. La liberté d'expression est principalement associée à la bonne gouvernance d'Internet évoquée au paragraphe 3.1 et au principe d'accès universel que l'Europe défend. Concernant la protection des données personnelles, les enjeux sont considérables compte-tenu du développement du big data avec des données qui constituent très clairement l'or noir du XXIème siècle.

Cette préoccupation relative à la protection des données personnelles n'est pas nouvelle et l'Union européenne a instauré un certain nombre de règlements et directives depuis 1995. Il s'agit notamment de demander aux États membres de « prévoir la protection des données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau »[79]. Cette directive de 1995 institue également le G29[80] qui a en charge de coordonner l'activité des différentes autorités de protection des données personnelles. Or, le niveau de protection des droits individuels est, dans les faits, très variable entre les Etats membres et le scandale Prisme a révélé les nombreuses failles qui pouvaient encore exister. L'Union européenne travaille donc depuis 2012 sur l'élaboration d'un règlement général accompagné d'une nouvelle directive ayant vocation à être plus globaux et surtout plus contraignants. L'ambition de l'Europe est ici beaucoup plus importante, tout d'abord, car contrairement à une directive, un règlement s'applique directement à tous les Etats membres. D'autre part, car contrairement aux textes existants qui n'établissent

[78] Stratégie de cybersécurité de l'Union européenne, op. cit., p. 2.
[79] Directive 95/46/E relative à la protection des données personnelles, 24 octobre 1995, 20 p., article 17.
[80] Groupe de travail Article 29 sur la protection des données.

finalement que des recommandations, ce règlement général prévoie des sanctions financières et d'avantage de pouvoir pour les organismes de contrôle. A l'issue de négociations semble-t-il laborieuses depuis 2012 compte-tenu de la difficulté à trouver un compromis entre sécurité et liberté, le conseil de l'Europe a approuvé ce règlement général le 8 avril 2016 qui devrait donc bientôt entrer en vigueur pour être applicable à compter du printemps 2018[81].

Etant donné le caractère sans frontière du cyberespace, il ne s'agit pas seulement de protéger les données en Europe mais aussi et surtout d'assurer un niveau élevé de protection des données lors de leur transfert vers un pays tiers. Le règlement général évoqué ci-dessus couvre donc également le transfert de données à caractère personnel à des pays tiers ou à des organisations internationales. Parallèlement, l'Union européenne a conclu un certain nombre d'accords bilatéraux fixant les règles relatives à ces transferts de données personnelles. Il s'agit par exemple de l'accord du 2 février 2016 entre le département du commerce américain et la commission européenne qui fait suite à l'invalidation le 6 octobre 2015, par la Cour de justice de l'Union européenne, du dispositif Safe Harbor[82]. Cet accord permet de gagner du temps et permet aux sociétés de continuer à échanger des données, en attendant les conclusions du G29 qui doit réétudier tout le document. Les difficultés principales dans cet accord sont que la sphère de sécurité ne concerne que les échanges commerciaux alors qu'il devrait également traiter des données internationales et notamment celles entre les sociétés privées et les agences de renseignement. En effet, certaines entreprises américaines ont développé du business avec les agences de renseignement alors que cela est impossible en Europe. Le risque principal pour les européens provient de l'hégémonie des Etats-Unis sur le stockage des données de l'Internet et il apparait donc essentiel de règlementer ces transferts entre le monde privé et les agences de renseignement.

3.4. Promouvoir un accès universel à l'Internet

La stratégie de cybersécurité de l'Union européenne repose, nous l'avons vu, sur trois piliers : la sécurité, la liberté mais aussi l'ouverture. Si l'ouverture n'est pas une fin en soi, elle se révèle absolument complémentaire avec les deux premiers piliers pour permettre à l'Union

[81] Site web Europe, *Le règlement général sur la protection des données*, http://www.consilium.europa.eu/fr/policies/data-protection-reform/data-protection-regulation/
[82] Sphère de sécurité

européenne de défendre son idée d'un cyberespace constituant un espace de liberté et de droits fondamentaux.

En effet, comme l'indique un rapport du parlement européen[83], « Internet est devenu au XXI^{ème} siècle un élément central de la vie quotidienne de ses 2,4 milliards d'utilisateurs dans le monde ». Cette hyperconnectivité exponentielle des systèmes, des citoyens et maintenant même des objets, conduit à une forte dépendance de nos sociétés à Internet, qui doit donc impérativement être sécurisé. Si en plus d'être sécurisé, Internet est libre, il peut permettre aux citoyens d'accéder plus facilement à leurs droits fondamentaux comme la liberté d'expression, d'information, la liberté d'association et autres droits civils. Par conséquent, comme cela est affirmé dans la stratégie de cybersécurité de l'Union, élargir l'accès à l'Internet au plus grand nombre pourrait très clairement contribuer à « faire avancer les processus de démocratisation et promouvoir les réformes démocratiques dans le monde »[84]. C'est pourquoi un accès universel à internet en Europe, avec une norme minimale de service, devrait être un objectif public et c'est précisément la position que l'UE porte également au niveau international. Ceci est par ailleurs tout à fait cohérent avec le concept d'approche global que l'UE s'efforce de développer pour améliorer sa capacité de résolution des crises internationales consistant à agir sur le triptyque gouvernance, sécurité et développement économique. Enfin, comme le souligne le rapport parlementaire, l'UE est un moteur mais elle n'est pas la seule à porter ces valeurs. Ainsi, en 2011, plus de cent pays dans le monde avaient déjà adopté des politiques nationales de promotion de l'accès à haut débit. Des organes comme la Commission sur le haut-débit pour le développement numérique, projet conjoint de l'UIT[85] et de l'Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO), encouragent l'élaboration de telles politiques.

3.5. Quelles perspectives ?

Si la stratégie de cybersécurité européenne formalise une prise de conscience importante de l'Union européenne à propos des enjeux du cyberespace et fixe le cadre et les axes prioritaires - pour un cyberespace ouvert, sûr et sécurisé- elle n'est pas suffisante. En effet, les directives et

[83] Rapport du Parlement européen, *Le droit d'accès à l'Internet*, 4 mars 2014, 18 p., p. 5.
[84] Stratégie de cybersécurité de l'Union européenne, op. cit., p. 16.
[85] Union internationale des télécommunications.

règlements associés peinent à voir le jour tant le compromis est difficile à trouver entre liberté, sécurité dans le cyberespace et souveraineté des Etats membres.

Dans le domaine de la sécurité, il s'agit tout d'abord de la directive SRI. Les travaux ont débuté en 2013 lors de l'élaboration de la stratégie de cybersécurité et si les négociations ont semble-t-il été difficiles, le projet a été approuvé de manière informelle par le comité des représentants permanents le 18 décembre 2015[86]. Même si certains Etats membres ont remis en cause le périmètre d'application de la directive du fait de l'impact sur leur souveraineté et leur économie, cette directive, qui devrait entrer en vigueur d'ici l'été 2016, constituera certes un compromis mais tout de même une avancée majeure. En effet, elle a pour objet de décliner de manière très concrète les mesures à prendre pour notamment sécuriser les infrastructures dites critiques. Elle fixera en particulier les règles permettant aux Etats membres de recenser les opérateurs qui fournissent des services essentiels et de leur imposer des mesures de gestion du risque informatique ainsi qu'une remontée systématique des cyber-incidents aux autorités.

Dans le domaine des libertés individuelles, il s'agit du règlement relatif à la protection des données personnelles approuvé le 8 avril 2016 par le conseil de l'Union européenne et qui devrait donc bientôt entrer en vigueur pour être applicable à compter du printemps 2018. Il aura fallu 4 ans pour trouver un compromis et le dossier parallèle très médiatisé du PNR[87], qui est reste bloqué dans l'attente des négociations sur ce règlement, est tout à fait révélateur des difficultés des Etats membres à partager l'information. Ce partage de renseignement est pourtant crucial, en particulier dans le domaine de la cybersécurité, et d'autant plus compte-tenu du contexte sécuritaire actuel en Europe. A noter que le Parlement vient enfin d'adopter le 14 avril 2016 ce registre européen des données des passagers aériens[88].

Dans le domaine de la défense, la politique de sécurité et défense commune semble clairement en panne et l'Union européenne n'investit guère plus à ce stade que dans ce qui parait le plus facile : le développement capacitaire. En effet, il permet de renforcer les capacités de certains

[86] Site web Europe, *Le règlement général sur la protection des données*, http://www.consilium.europa.eu/fr/policies/data-protection-reform/data-protection-regulation/.
[87] Passenger Name Record.
[88] http://www.lexpress.fr/actualite/monde/europe/ce-que-le-pnr-europeen-doit-apporter-dans-la-lutte-contre-le-terrorisme_1782915.html.

Etats membres dans le cadre de coopérations multilatérales « à la carte » en restant bien à l'écart des préoccupations opérationnelles et donc sans risque de compromettre la si chère souveraineté des Etats. Ce développement capacitaire comprend un volet cyberdéfense qui fait partie des 16 priorités fixées par l'AED et dont les travaux sont notamment conduits en cohérence avec les développements nationaux et ceux de l'OTAN[89].

Enfin, via à vis de l'OTAN, la déclaration du prochain sommet de l'OTAN pourrait, d'après certains experts de l'OTAN, formaliser la reconnaissance par les pays membres de l'OTAN que le cyberespace est le 5eme terrain de conflictualité après la terre, l'air, la mer et l'espace. Ce changement est censé donner aux commandants opérationnels la possibilité de mobiliser des ressources cyber, y compris nationales, dans le cadre de la planification ou la conduite d'une opération. Ainsi l'OTAN n'aurait pas de capacité offensive mais pourrait en intégrer si les nations en mettaient à sa disposition. Cependant, avec des capacités militaires alors plus complètes, il est peu probable que de nombreux pays européens sortent de leur posture habituelle qui consiste à faire reposer leur sécurité sur l'Alliance, y compris maintenant pour la cyberdéfense.

Ainsi, compte-tenu de plus de la sensibilité du domaine de la cyberdéfense, perçu comme relevant de la souveraineté des Etats, Il apparait fort probable que l'Union européenne continue de développer sa stratégie de cybersécurité autour d'une logique d'approche globale. Il s'agit ainsi pour l'Union de se focaliser avant tout sur la protection des infrastructures critiques, la gouvernance de l'Internet et le respect des libertés fondamentales. Dans le domaine de la cyberdéfense, qui devrait rester plutôt à la main des Etats et de l'OTAN, l'Union ne devrait pas aller au-delà du développement capacitaire au travers de coopérations multilatérales « à la carte ».

[89] http://www.eda.europa.eu/docs/default-source/eda-factsheets/cyber-defence-factsheet.

CONCLUSION

Nos sociétés sont désormais confrontées à une dépendance technologique qui s'est considérablement amplifiée durant les dernières décennies notamment au travers de l'avènement de l'informatique et, surtout, de la révolution numérique. Cette dernière a en particulier donné vie à un nouveau milieu, le cyberespace, qui a généré de nouvelles menaces qui ont la particularité d'être accessibles au plus grand nombre, sans frontières et à ce stade caractérisées par une certaine opacité. Les enjeux de sécurité sont considérables, tant ces menaces sont capables d'ébranler nos systèmes politiques, judiciaires, économiques et sociaux, et de nombreux pays et organisations dans le monde ont développé des stratégies et des capacités de cybersécurité.

L'universalité de cette menace est telle qu'une coopération entre les Etats et les organisations semble indispensable. L'UE a ainsi élaboré en février 2013 une stratégie de cybersécurité de l'Union Européenne, de portée très générale, qui repose avant tout sur un partage de responsabilités avec les Etats membres. L'Union européenne se dote peu à peu de structures ayant pour ambition de faire face aux menaces cybernétiques visant ses réseaux et ses infrastructures critiques mais les administrations nationales semblent être considérées comme mieux placées pour organiser la prévention et l'intervention en cas de cyberattaque et pour établir des contacts et des réseaux avec le secteur privé et le grand public. Ce texte novateur marque une vraie prise de conscience et une volonté affichée de promouvoir l'harmonisation du niveau de cybersécurité de chaque Etat et de coordonner le partage d'information.

Mais la plus-value réelle de cette stratégie de cybsersécurité parait toute relative avec une UE, souvent limitée à un rôle de coordinateur, sans réels pouvoirs de contraintes. De plus, le niveau de sécurité entre les Etat membres est très disparate et le principe de souveraineté qui prédomine, limite fortement l'échange de renseignements et le partage de bonnes pratiques pourtant essentiels. Enfin, la notion de cyberdéfense est quasiment absente et se limite à quelques petits projets de développement capacitaire, quelques formations et l'organisation d'exercices. Si l'Union européenne se considère en effet comme un acteur mineur sur ce dernier point, cela provient en particulier de sa nature profonde de « puissance civile » face à une OTAN dont c'est le cœur de métier. Cela est probablement aussi révélateur d'un échec plus

large de la Politique de sécurité et de défense commune, vraisemblablement en panne depuis plusieurs années.

Consciente du besoin de coopération dans ce domaine, l'UE a intégré sa stratégie dans un cadre international et développe un certain nombre de coopérations. Compte-tenu de la sensibilité de la notion de confiance dans le domaine de la cybersécurité, ces dernières sont majoritairement bilatérales avec une stratégie des « petits pas », rappelant d'ailleurs la méthode Monnet-Schuman qui fut à la base de l'intégration européenne, dont la création de la CECA[90] en 1951 en est la première réalisation concrète. Mais cela n'empêche pas l'Union de rechercher également à développer des relations privilégiées avec certaines organisations internationales ou régionales et en particulier avec l'OTAN. Si cette volonté ne suffit aujourd'hui pas pour concrétiser la mise en place de processus commun permettant de véritablement conjuguer les efforts, une complémentarité entre ces deux organisations semble tout de même possible. En effet, l'OTAN, sur laquelle de nombreux membres de l'Union se reposent pour garantir leur défense, pourrait se focaliser d'un part, sur la défense de ses réseaux propres au titre de la défense collective. Elle pourrait d'autre part concentrer ses efforts sur le développement de l'interopérabilité et sur la planification opérationnelle dans le cadre de la gestion des crises en intégrant idéalement des capacités offensives permettant une action complémentaire dans le cyberespace. L'Union européenne, pourrait quant à elle développer l'approche globale avec des instruments règlementaires permettant avant tout de renforcer la sécurité de ses infrastructures critiques et services essentiels en agissant sur le secteur privé. Dans le domaine opérationnel de gestion des crises, elle pourrait développer plus en avant le concept de réforme du secteur de sécurité en y intégrant les aspects liés à la cybersécurité et en complémentarité avec ses actions dans les domaines du développement et de la gouvernance.

Enfin, cette stratégie de cybersécurité européenne s'inscrit dans une stratégie beaucoup plus globale, davantage affirmée en terme de gouvernance et de protection des libertés fondamentales, comme la protection des données personnelles et l'accès universel à l'Internet. En effet, Internet est devenu un élément tellement central pour le développement économique

[90] Communauté Européenne du Charbon et de l'Acier.

et social, qu'il ne faut pas seulement le sécuriser mais aussi l'ouvrir au plus grand nombre tout en garantissant les libertés individuelles. La plus-value et la complémentarité de cette cyberstratégie européenne pourrait donc également être de contribuer à instaurer un cyberespace de confiance permettant à la fois un développement économique plus sécurisé et un développement social garantissant la liberté d'expression et l'exercice des droits fondamentaux, contribuant indirectement au processus de démocratisation.

En conclusion, on assiste donc à une sorte de réactivation de l'approche réaliste, caractérisée par l'importance de premier plan des intérêts nationaux et la prédominance de la notion de souveraineté des Etats, qui freine les cyberstratégies de l'UE et de l'OTAN. Cela pose bien évidemment question dans la mesure où cela apparaît tout à fait incompatible avec les caractéristiques notamment duale et sans frontières des cybermenaces. Enfin, cette tendance est en totale contradiction avec la volonté affichée de développer plus largement la coopération bien qu'elle ne reste à ce stade dans les faits que très embryonnaire.

L'Union européenne et l'OTAN sont donc toutes les deux confrontées à deux difficultés majeures : un niveau très disparate de leurs Etats membres en terme de cybersécurité ainsi que des positions très variables quant à l'assurance de leur défense y compris dans le cyberespace. Si le rapprochement en marche entre sécurité et défense semble inexorable, il pourrait garantir une certaine cohérence pour la cybersécurité compte-tenu de la dualité du cyberespace. Un rapprochement encore plus marqué entre les deux organisations, dont 22 des membres sont communs, pourrait alors s'avérer indispensable. Reste à savoir si l'UE sera en mesure de relancer la PSDC qui pourrait constituer le support idéal pour optimiser la complémentarité avec l'OTAN et garantir au final toute la plus-value de l'approche globale indispensable pour faire face aux enjeux à venir.

SOURCES ET BIBLIOGRAPHIE

1. SOURCES FRANCE :

- ANSSI, *Stratégie pour la France pour la défense et la sécurité des systèmes d'information*, Paris, 15 février 2011, 24 p.
- *Le Livre Blanc sur la Défense et la Sécurité Nationale (LBDSN)*, La documentation française, 29 avril 2013, 160 p.
- Etat-Major des armées, *Doctrine interarmées de Cyberdéfense DIA 3-40*, 28 mars 2014, 66 p.
- *Projet de loi pour une république numérique,* projet issu de la consultation citoyenne adopté en première lecture à l'assemblée nationale le 26 janvier 2016.
- *Stratégie nationale de sécurité numérique*, 16 octobre 2015, 44 p.
- *Loi 2013-1168 relative à la loi de programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale*, 18 décembre 2013 modifiée le 30 novembre 2015, 32 p.

2. SOURCES UE :

- Directive 95/46/E relative à la protection des données personnelles, 24 octobre 1995, 20 p.
- Communication de la commission européenne, *La sécurité des réseaux et de l'information (SRI) : proposition pour une approche politique européenne*, [COM(2001) 298], 6 juin 2001, 30 p.
- Journal official de l'Union Européenne, *Stratégie européenne de sécurité*, 12 décembre 2003, 15 p, http://www.consilium.europa.eu/uedocs/cmsUpload/031208ESSIIFR.pdf
- Communication de la commission européenne, *Une stratégie pour une société de l'information sûre*, [COM(2006) 251], 31 mai 2006, http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=URISERV%3Al24153a
- Journal official de l'Union Européenne, *Directive 2008/114/CE concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection*, 8 décembre 2008, 8 p.
- Traité de Lisbonne, article 42.7, 410 p., 1er décembre 2009, p.40.

- Journal official de l'Union Européenne, *Directive 2009/140/CE modifiant les directives 2002/21/CE relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques, 2002/19/CE relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion, et 2002/20/CE relative à l'autorisation des réseaux et services de communications électroniques*, 25 novembre 2009.
- Communication de la commission européenne, *Une stratégie numérique pour l'Europe,* [COM(2010) 245], 19 mai 2010, http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=URISERV%3Asi0016
- Communication de la commission européenne, *Protection des infrastructures d'information critiques*, [COM(2011) 163], 31 mars 2011, 19 p.
- Communication de la commission européenne, *Stratégie de cybersécurité de l'Union européenne : un espace ouvert, sûr et sécurisé*, [JOIN (2013) 1], 7 février 2013, 21 p.
- Directive du Parlement européen et du Conseil, *Proposition de directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union n°2013/0027*, 7 février 2013 (+ version du 18 décembre 2015), 55 p.
- Communiqué de presse, *Directive et règlement relatif à la protection des données*, 12 mars 2014, 2 p.
- Rapport du Parlement européen, *Le droit d'accès à l'Internet*, 4 mars 2014, 18 p.
- Journal official de l'Union Européenne, *Règlement n°910/2014 relatif à l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur,* 23 juillet 2014, 42 p.
- Stratégie pour un marché unique numérique en Europe, [COM(2015) 192], 5 mai 2015, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52015DC0192&from=EN
- Site web Europe, *Le règlement général sur la protection des données*, http://www.consilium.europa.eu/fr/policies/data-protection-reform/data-protection-regulation/

3. <u>SOURCES OTAN :</u>

- Première politique de cyberdefense, janvier 2008.
- *Concept stratégique pour la défense et la sécurité des membres de l'Organisation du Traité de l'Atlantique Nord*, Sommet de Lisbonne, 2010, 42 p.

- *Document conceptuel sur la cyberdéfense de l'OTAN* – C-M(2011) 0020.
- *NATO Policy on Cyber Defence*, C-M(2011)0042 – NATO DR, 8 juin 2011.

4. BIBLIOGRAPHIE :

Références bibliographiques :

- BABINET Gilles, *L'ère numérique, un nouvel âge de l'humanité*, 2014, 236 p.
- BOYER Bertrand, *Cyberstratégie : l'art de la guerre numérique*, Nuvis, 2015, 235 p.
- KEMPF Olivier, *Introduction à la cyberstratégie, Economica*, 2015, 235 p.
- KEMPF Olivier, *Alliances et mésalliances dans le cyberespace*, Economica, 2015, 192 p.
- KEMPF Olivier, *La cyberstratégie de l'union européenne*, Sécurité Globale n°24, été 2013, p. 25-40.
- LASBORDES Pierre, *La sécurité des systèmes d'information : un enjeu majeur pour la France,* Rapport public de La documentation française, 26 novembre 2005, 195 p.
- MORIN-DESAILLY Catherine, *L'Union européenne, colonie du monde numérique*, Rapport sénatorial n°443, 20 mars 2013, 158 p.
- MORIN-DESAILLY Catherine, *L'Europe au secours de l'Internet : démocratiser la gouvernance de l'Internet en s'appuyant sur une ambition politique et industrielle européenne*, Note de synthèse du rapport sénatorial n°696, 8 juillet 2014, 6 p.
- MYRLI SVERRE, *L'OTAN et la cyberdéfense*, Rapport de l'assemblée parlementaire de l'OTAN n°173 DSCFC 09 F bis, 2009, 11p.
- VENTRE Daniel, *Cyberattaque et cyberdéfense*, 2011, 312 p.
- VENTRE Daniel, *Cyberespace et acteurs du cyberconflit*, 2011, 288 p.
- Rapport DAS, *Etude sur la cyberdéfense et la cybersécurité au sein des institutions européennes*, 2011, 43 p.

Articles / Revues :

- ARCIONI S., *Apport des théories de la gouvernance des entreprises pour définir une gouvernance du cyber*, 2012, 26 p.
- RÖHRIG W., *Viewpoints : Cyber Security an Cyber Defence in the European Union*, 11 juin 2014, https://www.eda.europa.eu.
- KEMPF Olivier, *L'OTAN et la cyberdéfense, article n°III.6,* Chaire de cyberdéfense et cybersécurité de l'école de Saint-Cyr, mai 2013, 8 p.

- NATO Research Paper, Semantics matter – NATO*, Cyberspace and future threats*, Research Division of the NATO Defense College, Juillet 2014, 12 p.
- Communiqué OTAN, L'OTAN et l'Union européenne renforcent leur coopération en matière de cyberdéfense, 10 février 2016, http://www.nato.int/cps/fr/natohq/news_127836.htm
- Observatoire du monde cybernétique, *La stratégie de cybersécurité de l'union européenne*, lettre n°14, DGRIS, février 2013, 13 p.
- Observatoire du monde cybernétique, *Les relations transfrontalières et les infrastructures critiques*, lettre n°42, DGRIS, septembre 2015, p. 2-5.
- JOUBERT Vincent, SAMAAN Jean-Loup, *L'intergouvernementalité dans le cyberespace : étude comparée des initiatives de l'Otan et de l'UE*, Revue HERODOTE n°152-153 – 2014/1, p. 261-275.
- VENTRE Daniel, *Lutte et enjeux de gouvernance dans le cyberespace mondial*, Les grands dossiers de la diplomatie n°23, novembre 2014, 4 p.

Congrès / Conférences :

- 4e séminaire IHEDN de Bruxelles, *Vers une cyberstratégie européenne ?*, 28 juin 2012, IHEDN Paris, 145 p.
- BELLANGER Pierre, *Conférence devant l'IHEDN : Enjeux et moyens de notre souveraineté numérique,* 2014.