ECOLE DE GUERRE

PROMOTION *VERDUN*

2015 -2016

L’Union européenne et la cybersécurité : y a-t-il une cyberstratégie européenne?

Chef de bataillon Frédéric Gerlinger

Sous la direction de

Joseph Henrotin

Chargé de recherche au Centre d'analyse et de prévision des risques internationaux (CAPRI, Paris) et à l’Institut de stratégie comparée (ISC, Paris)

Résumé :

En parallèle de ses stratégies successives pour le numérique qui permettent aux citoyens et entreprises européennes de tirer pleinement profit des NTIC et des possibilités économiques qu'elles offrent, l'UE s'est investie dans la cybersécurité et la cyberdéfense. Dès 2001, elle a commencé à construire sa stratégie dans le domaine en mettant en place un ensemble d'outils législatif, opérationnel et technologique. Aussi la mise en œuvre d'une cyberstratégie européenne efficace semble aujourd'hui possible en raison à la fois de la volonté de l'UE d'investir ce nouveau champ des confrontations et des moyens humains, financiers et industriels dont elle dispose. Pour autant, malgré des avancées significatives dans la cyberprotection de l'Europe, de nombreux défis doivent encore être relevés, le premier étant l'investissement inconditionnel de tous les États membres.

Abstract:

Alongside its successive strategies for the digital that allow citizens and European companies to take full advantage of Information and Communications Technology (ICT) and the economic opportunities they offer, the EU has invested in cyber security and cyber defense. Since 2001, UE built its strategy in the field by establishing a set of legislative, operational and technological tools. Also the implementation of an effective European e-strategy seems now possible due to the EU's willingness to invest this new field of confrontation and human, financial and industrial resources it has. However, despite significant advances in the European cyber protection, many challenges remain ahead, the first of all the unconditional investment of all Member States.

L'Union européenne et la cybersécurité : y a-t-il une cyberstratégie européenne?

L'Union européenne et la cybersécurité : y a-t-il une cyberstratégie européenne?

1 Introduction

La signature du traité de Maastricht le 7 février 1992 et son entrée en vigueur le 1er novembre 1993 furent de nouvelles étapes dans la construction de l'Union européenne (UE). Les questions de sécurité et de défense occupent désormais une place considérable. En effet, la nécessité de coopération et de coordination des efforts entre états membres est un défi pour la sécurité de l'UE au XXIème siècle. Cette volonté s'affirme avec la signature du traité de Lisbonne le 13 décembre 2007 et la mise en place d'une politique de sécurité et de défense commune (PSDC) qui ambitionne le développement d'une défense européenne. C'est dans ce cadre et pour faire face aux menaces croissantes qui pèsent sur le cyberespace que l'UE a élaboré une stratégie de cybersécurité c'est-à-dire « *l'ensemble des pratiques civiles et militaires, publiques et privées, intérieures et extérieures visant à aménager et à utiliser le cyberespace afin de répondre aux objectifs fixés par l'autorité politique pour assurer la prospérité et la sécurité de la communauté des citoyens, en conformité avec les impératifs de souveraineté et d'autonomie de décision nationales, dans le respect des libertés matérielles (économie) et spirituelles (idéologie) »*[1].

En effet, depuis une vingtaine d'années, les réseaux informatiques et Internet en particulier ont connu une croissance exponentielle qui a favorisé la prolifération des menaces et des risques qui pèsent sur le cyberespace. De nouvelles terminologies ont vu le jour, telles que la cybercriminalité, le cyberespionnage ou encore le cyberterrorisme alors que les attaques cyber se multipliaient visant des Etats[2], des organes de presse[3] mais également des particuliers. Les Etats ont été contraints d'investir ce nouveau champ des confrontations soit pour protéger leurs intérêts et ceux de leurs citoyens soit pour tirer profit des multiples possibilités qu'il offre. Cependant l'action des seuls Etats n'est plus suffisante, à l'instar du renseignement, de la lutte contre les réseaux criminels et les groupes terroristes. Il apparait ainsi intéressant d'étudier au niveau supranational les actions qui ont pu être mises en œuvre, en particulier au

[1] Définition donnée par l'Institut français d'analyse stratégique (IFAS) : http://www.strato-analyse.org/fr/spip.php?rubrique68

[2] En 2007, des attaques ont visé les sites gouvernementaux de l'Estonie et la Géorgie en 2008

[3] Attaque de TV5 monde en avril 2015

niveau de l'UE, dans une société dépendante des nouvelles technologies de l'information et de la communication (NTIC).

Les différentes publications sur ce sujet analysent et commentent la diffusion en février 2013 de la stratégie de cybersécurité de l'UE : « *un cyberespace ouvert, sûr et sécurisé* »[4]. Elles insistent sur les enjeux et l'importance d'une telle cyberstratégie tout en mentionnant les difficultés possibles quant à sa mise en œuvre. Il y a cependant peu de documentation sur la construction de cette cyberstratégie et sa mise en œuvre concrète par les états membres de l'UE. Ainsi, nous pouvons nous interroger sur les difficultés effectivement rencontrées mais également sur les succès dans ce domaine.

L'objectif de ce travail est d'étudier à la fois la construction de la politique de cybersécurité européenne depuis 2001 et la manière dont elle est mise en œuvre par les Etats membres de l'UE tout en insistant sur les difficultés rencontrées et les perspectives d'avenir.

Pour mener cette étude, nous avons tout d'abord exploité les différentes conventions, décisions cadres et communications de l'UE afin d'étudier la construction de cette stratégie de cybersécurité depuis 2001. Nous avons également consulté plusieurs ouvrages traitant de la cybersécurité et de la cyberdéfense en général et dans lesquels la question de l'UE était abordée. Enfin, les rapports du Sénat français et quelques articles de revues spécialisées nous ont permis d'enrichir nos données et notre analyse sur le domaine.

L'objectif initial de ce mini-mémoire était d'aborder la mise en œuvre de la stratégie européenne de cybersécurité par l'étude de plusieurs pays. Nous avons effectué une étude macroscopique en insistant sur les réussites mais également les lacunes ou les retards dans l'application des différentes décisions et préconisations de l'UE. Ce choix a d'une part été motivé par les difficultés d'accès à la documentation nationale dans un domaine qui demeure sensible voire protégé et d'autre part par la volonté d'expliquer le processus de construction et de mise en œuvre de la stratégie européenne.

Depuis 2001, l'UE a démontré sa volonté d'investir ce nouveau champ des confrontations et dispose aujourd'hui en propre ou avec ses Etats membres des moyens humains, financiers, technologiques et juridiques lui permettant d'aborder l'avenir avec ambition. La mise en œuvre d'une cyberstratégie européenne efficace semble donc aujourd'hui possible. La

[4] Communication conjointe au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions – Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé.

question est de savoir qu'elle a été le processus qui a abouti à cette nouvelle politique et si les états membres la mettent en œuvre en suivant les préconisations de l'institution européenne.

Aussi allons-nous tout d'abord étudier la construction de la politique de cybersécurité de l'UE entre 2001 et 2013 au travers des différents textes élaborés à ce sujet, nous effectuerons ensuite une étude de la cyberstratégie communiquée en février 2013 puis nous évaluerons sa mise en œuvre par les Etats membres de l'UE en insistant sur les succès, les points à améliorer et les perspectives d'avenir.

2 Construction de la cyberstratégie européenne

La construction de la cyberstratégie européenne est un mécanisme complexe qui s'est imposée au cours des années 2000 en raison du développement rapide des NTIC et du cyberespace. La dépendance croissante de nos sociétés à ces nouvelles technologies et le caractère transnational des menaces ont nécessité une réponse collective des Etats en général et de l'UE en particulier.

2.1 Les stratégies du numérique de l'Union européenne avant 2013[5]

A l'instar de la construction européenne, les stratégies du numérique de l'UE trouvent leurs fondements dans la recherche du développement économique, culturel et social. Les stratégies de 2005 et de 2010 cherchent avant tout à exploiter le potentiel économique et social des NTIC. A ce titre, la majorité des mesures proposées (développement de l'accès à l'internet haut débit, du commerce numérique, stimulation de la recherche et de l'innovation, etc.) convergent vers un même objectif : la croissance économique. Les volets sociaux, environnementaux et culturels demeurent présents mais secondaires. Ils visent avant tout à simplifier la vie du citoyen européen (services publics en ligne à l'échelle européenne, etc.) et à favoriser la diffusion de la culture sous toutes ses formes. Dans ce contexte, la sécurité des réseaux et de l'information a uniquement vocation à améliorer la confiance du consommateur dans les NTIC pour favoriser leur développement.

2.2 La sécurité des réseaux et de l'information

La croissance exponentielle des NTIC, encouragée par les pouvoirs publics et l'institution européenne en particulier, a cependant entrainé une dépendance accrue de la société au

[5] COM(2005) 229 : « i2010 - Une société de l'information pour la croissance et l'emploi » du 1er juin 2005 ; COM(2010) 245 : « Une stratégie numérique pour l'Europe » du 19 mai 2010.

numérique. Il devenait par conséquent indispensable de mettre en œuvre des mesures concrètes et de créer des organismes chargés d'assurer la sécurité des réseaux sous peine d'entraver durablement le développement économique et sociétal de l'UE. Les différentes publications[6] relatives à la sécurité des réseaux et de l'Information (SRI) et à la protection des infrastructures d'information critiques (IIC) sont ainsi consacrées à la préparation, la prévention et la sensibilisation des acteurs du numériques (particuliers, entreprises ou encore Etats). Elles visent à protéger l'Europe des cyberattaques et des perturbations en encourageant une meilleure coopération et un partage d'information plus efficace notamment par l'intermédiaire d'organismes tels que les CERT ou l'ENISA. La recherche et le développement (R&D) en matière de sécurité est également encouragé au travers des 6ème et 7ème programme cadre afin de renforcer la résilience des IIC.

2.3 La lutte contre la cybercriminalité : cadre juridique[7]

Pour renforcer la sécurité des réseaux et de l'information, l'UE s'est doté dès 2001 d'un cadre légal encadrant les activités dans le cyberespace. Elle dispose aujourd'hui d'une législation permettant de poursuivre un certain nombre d'infractions énumérées dans la Convention de Budapest et les décisions cadres de 2005 et 2010. Des dispositions spécifiques relatives à la responsabilité des personnes morales, les compétences juridictionnelles et les échanges d'information ont également été formalisées dans ces textes. L'UE peut ainsi s'enorgueillir d'une véritable réussite dans ce domaine puisque ses initiatives dépassent largement le territoire européen. La Convention de Budapest a en effet été signée par 49 Etats[8] et ratifiée notamment par les Etats-Unis, le Canada ou encore l'Australie. Ces succès doivent cependant être relativisés puisque un certain nombre d'Etats peine toujours à prendre les mesures

[6] COM(2001) 298 : « Sécurité des réseaux et de l'information : proposition pour une approche politique européenne » du 6 juin 2001 ;
COM(2006) 251 : « Une stratégie pour une société de l'information sûre – dialogue, partenariat et responsabilisation » du 31 mai 2006 ;
COM(2009) 149 : relative à la protection des infrastructures d'information critiques (PIIC) : « Protéger l'Europe des cyberattaques et des perturbations de grande envergure : améliorer l'état de préparation, la sécurité et la résilience » de mars 2009 ;
COM(2011) 163 : relative à la protection des infrastructures d'information critiques (PIIC) : « Réalisations et prochaines étapes: vers une cybersécurité mondiale » du 31 mars 2011;

[7] Convention de Budapest sur la cybercriminalité STE n°185 du 23 novembre 2001 ;
Décision cadre 2005/222/JAI du Conseil 24 février 2005 relative aux attaques visant les systèmes d'information;
COM(2010) 517 : Proposition de directive du Parlement européen et du Conseil du 30 septembre 2010 relative aux attaques visant les systèmes d'information.

[8] http://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/185/signatures

nécessaires à la transposition des décisions de l'UE.[9] A titre d'exemple, la Convention de Budapest n'a toujours pas été ratifiée par la Grèce, l'Irlande et la Suède alors que des pays comme la Pologne et le Luxembourg ont attendu 2015 pour le faire.

2.4 **Les structures et outils de cybersécurité de l'Union européenne**

2.4.a L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)[10]

L'Agence européenne chargée de la sécurité des réseaux et de l'information a été créée en mars 2004. Elle avait pour principal objet « *d'assurer un niveau élevé et efficace de sécurité des réseaux et de l'information au sein de [l'Union] et […] de favoriser l'émergence d'une culture de sécurité des réseaux et de l'information dans l'intérêt des citoyens, des consommateurs, des entreprises et des organismes du secteur public de l'Union européenne, contribuant ainsi au bon fonctionnement du marché intérieur* ». [11] L'ENISA s'impose en effet comme le centre d'expertise de l'Union pour les questions de SRI auprès des autorités nationales et des institutions européennes. Elle doit à ce titre faciliter les contacts entre les institutions (nationales et européennes) et les entreprises, favoriser l'échange des bonnes pratiques et promouvoir la coopération entre tous les acteurs du domaine. Les moyens de l'ENISA demeurent cependant modestes avec un budget de 11M€ en 2016 [12] et un effectif d'environ 60 personnes. Son efficacité repose essentiellement sur la bonne volonté des Etats membres de l'UE et leurs moyens propres.[13]

2.4.b Les Computer Emergency Response Teams (CERT)

La SRI s'appuie également sur un réseau de CERT publics et privés. Ces centres d'alerte et de réaction aux attaques informatiques apportent une aide technique aux entreprises et aux administrations. Ils participent également à la prévention en diffusant des informations sur les

[9] COM(2008) 448 : Rapport de la Commission au Conseil fondé sur l'article 12 de la Décision-cadre du Conseil du 24 février 2005 relative aux attaques visant les systèmes d'information

[10] Règlement (CE) 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information ;
COM(2010) 520 : Proposition du Parlement européen et du Conseil modifiant le règlement (CE) 460/2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information.

[11] Règlement (CE) 1007/2008 du Parlement européen et du Conseil du 24 septembre 2008 modifiant le règlement (CE) 460/2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information en ce qui concerne sa durée ;

[12] ENISA work programme 2016.

[13] L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) française dispose d'un budget de 70M€ et d'un effectif de 420 personnes en 2015.

précautions à prendre pour minimiser les risques d'incident. L'objectif initial (2012) était de renforcer la SRI européenne à l'aide d'un réseau de CERT nationaux ou gouvernementaux dans chacun des Etats membres. Si l'Union européenne dispose depuis 2012 d'un CERT pour ses institutions, 2 Etats membres de l'UE n'ont toujours pas créé leur propre centre[14]. La qualité des équipements et les compétences de ces centres demeurent en outre très hétérogènes au sein de l'UE. La coopération et les échanges d'informations entre ces CERT s'effectuent au travers d'organismes tels que le Groupe des CERT gouvernementales européennes (EGC). Une fois encore, tous les pays membres de l'UE ne sont pas présents au sein de ce groupe.[15] La coordination à l'échelle mondiale est quant à elle assurée par le CERT/CC, financé en partie par le gouvernement américain.

2.4.c Le Centre européen de lutte contre la cybercriminalité (EC3)

Le caractère transnational des menaces cybernétiques, l'ampleur et le nombre de victimes concernées par certaines affaires rendaient les forces de police nationales de plus en plus démunies. L'UE s'est par conséquent dotée depuis janvier 2013, dans les locaux d'Europol à La Haye, d'un centre européen de lutte contre la cybercriminalité et dispose ainsi d'une structure judiciaire. L'EC3 se concentre sur les activités de fraude, d'espionnage, d'exploitation sexuelle et de maltraitance infantile en ligne et sur la criminalité touchant aux infrastructures critiques et aux systèmes d'information de l'UE. L'EC3 met également à la disposition des États membres un service d'assistance (help desk) à la lutte contre la cybercriminalité et propose son expertise dans le cadre d'enquêtes communes réalisées à l'échelle de l'Union. L'EC3 est aujourd'hui pleinement opérationnel comme le montre le succès de plusieurs opérations évoquées dans le rapport annuel 2014 d'Europol[16].

2.4.d Système européen de partage d'informations et d'alerte (SEPIA)

La résilience de l'UE face aux menaces cybernétiques ne repose pas uniquement sur des structures spécialisées. La Commission européenne a en effet identifié que les Etats membres avaient un rôle majeur à jouer dans la SRI en assurant un niveau élevé d'information et de sensibilisation des particuliers et des PME. L'objectif étant de les rendre acteurs de leurs propres sûreté et sécurité. A ce titre, l'UE a mandaté l'ENISA pour promouvoir le

[14] Chypre et Irlande : http://www.bsa.org/~/media/Files/Policy/Security/EU/study_eucybersecurity_fr.pdf.

[15] 13 membres : dont le CERT-UE, la Suisse et la Norvège. Pour l'UE : Allemagne, Autriche, Belgique, Danemark, Espagne, France, Finlande, Pays-Bas, Royaume-Uni, Suède ;

[16] Europol Review 2014 du 8 septembre 2015;

développement d'ici 2013, d'un système européen de partage d'informations et d'alerte (SEPIA) destiné aux PME et aux particuliers. Celui-ci doit reposer sur des CERT nationaux et gouvernementaux en vue d'intégrer les systèmes nationaux de partage d'informations et d'alerte. Pour autant, ce projet initié en 2006, n'a toujours pas vu le jour. Une étude[17] de faisabilité du déploiement de ce système datée de décembre 2013 donne pourtant une nouvelle feuille de route qui devrait aboutir à une mise en service au mieux en 2017. La bonne volonté de la Commission européenne est une fois de plus confrontée au manque d'investissement des pays membres de l'UE et à l'inertie des projets européens.

3 La cyberstratégie européenne de 2013 : Les cinq priorités de la cyberstratégie européenne et les directives associées[18]

Depuis 2001, l'Union européenne a mis en place un certain nombre de structures et de politiques lui permettant de construire une cyberstratégie cohérente et ambitieuse. Cette démarche, qui demeure néanmoins perfectible, a franchi une nouvelle étape en 2013 avec la publication d'une véritable stratégie de cybersécurité à l'échelle européenne. La portée et la crédibilité de cette initiative ont été renforcées par une directive destinée à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union. Ces deux publications ont identifié cinq priorités destinées à rendre le cyberespace « *ouvert, sûr et sécurisé* ».

3.1 Parvenir à la cyber-résilience

Le renforcement de la cyber-résilience européenne repose principalement sur un développement des moyens des pouvoirs publics et du secteur privé et l'amélioration de la coopération entre les acteurs de la SRI. La sensibilisation, l'éducation et la formation des particuliers et des entreprises demeurent également une priorité. L'objectif étant de faire face aux cyber-risques et aux menaces de dimension transnationale et de contribuer à une intervention européenne coordonnée en cas d'urgence. A ce titre, la Commission demande aux Etats membres d'adopter une stratégie nationale et de se doter d'une autorité nationale compétente en matière de SRI disposant des ressources techniques, financières et humaines suffisantes pour s'acquitter de cette tâche. Ces autorités constituent avec la Commission

[17] EISAS – European Information Sharing and Alerting System: Deployment Feasibility Study - December 2013.

[18] COM (2013) 1 : Communication conjointe au Parlement européen, au Conseil et au Comité économique et social européen et au Comité des régions. Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé. - 7 février 2013.

COM (2013) 48 : Proposition de directive du Parlement européen et du Conseil concernant les mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union du 7 février 2013.

européenne un réseau *(« réseau de coopération »*) chargé de coopérer dans la lutte contre les risques et incidents touchant les réseaux et les systèmes informatiques. Cette collaboration se concrétise par la diffusion de messages d'alerte rapide, d'informations sur ces alertes et les interventions coordonnées en cours et par l'organisation d'exercices de SRI au niveau de l'Union. Les Etats devront également mettre en place des CERT chargés de la gestion des incidents et des risques. Un programme de transfert de connaissances et de capacités entre les Etats membres doit également être mis en place afin d'homogénéiser les outils et les compétences dans l'ensemble de l'Union.

3.2 **Faire reculer considérablement la cybercriminalité**

Les cybercriminels et leurs réseaux de plus en plus sophistiqués ignorent les frontières faisant chaque jour plus d'un million de victimes dans le monde.[19] L'Union européenne doit par conséquent se doter des outils et des moyens appropriés pour s'y opposer et adopter une approche transnationale coordonnée et collaborative pour être efficace en matière de SRI. Cela nécessite une législation solide et efficace mais également des moyens judiciaires. L'UE demande par conséquent à ses Etats membres de ratifier et de faire appliquer les dispositions de la convention de Budapest de 2001. Les pays de l'UE doivent également se doter d'unités anticybercriminalité nationales qui pourront bénéficier à la fois de l'expertise du EC3 et de programmes de financement européen permettant de recenser leurs insuffisances et de renforcer leurs moyens d'enquête et de lutte.

3.3 **Développer une politique et des moyens de cyberdéfense liée à la politique de sécurité et de défense commune (PSDC)**

Le développement de la cyberdéfense européenne vise à accroître la résilience des infrastructures critiques d'Etat, de défense ou d'information dont dépendent les membres de l'UE. Il doit également assurer une protection des réseaux dans un contexte de missions et d'opérations de PSDC. Pour ce faire, la Commission européenne charge le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité de promouvoir le développement de moyens et de technologies de cyberdéfense propres à l'Union. Un dialogue permanent doit être établi entre l'UE, l'OTAN, les différentes organisations internationales et

[19] COM (2013) 1 : Communication conjointe au Parlement européen, au Conseil et au Comité économique et social européen et au Comité des régions. Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé. - 7 février 2013.

les centres d'excellence multinationaux afin d'échanger les bonnes pratiques et les informations.

3.4 Développer les ressources industrielles et technologiques en matière de cybersécurité

La SRI repose également sur la qualité des produits et services issus des technologies de l'information et de la communication (TIC) disponibles sur le marché européen. L'UE cherche ainsi à mettre en place des exigences de performance en matière de cybersécurité d'un bout à l'autre de la chaîne des produits TIC. Le secteur privé doit par conséquent être incité à garantir un niveau élevé de cybersécurité en mettant en place des normes et des labels SRI. L'efficacité et la qualité des produits doivent pouvoir être reconnues et valorisées. L'UE entend également profiter du programme européen pour la recherche et le développement « *Horizon 2020* » pour dynamiser le secteur des TIC.

3.5 Instaurer une politique internationale de l'Union européenne cohérente en matière de cyberespace et promouvoir les valeurs essentielles de l'UE

L'UE doit élaborer une politique internationale cohérente en matière de cybersécurité qui visera à promouvoir un cyberespace ouvert, libre et respectant les valeurs essentielles de l'Union[20]. En coopération avec les organisations[21] les plus actives dans ce domaine, les Etats-Unis, le secteur privé et la société civile, l'UE doit encourager les efforts pour élaborer « *des règles de conduite et des mesures de confiance* » sans toutefois créer de nouveaux instruments juridiques internationaux concernant les questions inhérentes au cyberespace.

4 Enjeux et perspectives d'avenir

4.1 Le nouveau projet de directive sur la sécurité des réseaux et de l'information

Le 18 décembre 2015, le Coreper (Comité des Représentants) est parvenu à un accord avec le Parlement européen sur un nouveau projet de directive visant à renforcer la sécurité des réseaux et de l'information au sein de l'UE. Cette directive devrait être adoptée au printemps 2016. Elle prévoit d'imposer aux fournisseurs de services essentiels (énergie, transport, eau, secteurs bancaires et de santé, etc.) et aux prestataires de services numériques la mise en place de l'ensemble des mesures permettant de faire face aux cyberattaques. Ces opérateurs auront

[20] Dignité humaine, liberté, démocratie, égalité, état de droit, respect des droits fondamentaux, etc.

[21] Conseil de l'Europe, OCDE, ONU, OSCE, OTAN, UA, ANASE, OEA, etc.

également l'obligation de signaler aux autorités compétentes et aux CERT les incidents auxquels ils auront été confrontés. Cette directive prévoit également la généralisation des CERT dans tous les pays de l'UE, l'adoption d'une stratégie nationale en matière de SRI définissant clairement les objectifs stratégiques et les mesures politiques et réglementaires à prendre pour assurer et maintenir un niveau élevé de sécurité. Ce texte doit ainsi consolider la stratégie de 2013 et continuer à promouvoir la coopération et la coordination européenne en matière de cybersécurité. On constate cependant que cette directive reprend un certain nombre de sujets déjà évoqués en 2013. Il sera par conséquent intéressant de voir si la Commission envisage des mesures contraignantes pour obliger les Etats membres à se conformer rigoureusement à cette directive.

4.2 **Les limites et difficultés de la mise en œuvre de cette cyberstratégie**

4.2.a Les stratégies et les agences de cybersécurité nationales

Les textes européens de 2013 demandaient à tous les Etats membres de se doter en autres d'une stratégie et d'une agence de cybersécurité. Ils n'ont cependant été que partiellement appliqués. En effet, 9 pays (cf annexe) n'ont toujours pas adopté de stratégie nationale. En outre, la qualité de ces stratégies demeure très hétérogène d'un pays à l'autre. Seuls 16 pays disposent d'une véritable agence de cybersécurité sur le modèle de l'ENISA européenne ou de l'ANSSI française. Les autres pays s'appuient sur des CERT nationaux à l'exception de l'Irlande et de Chypre qui ne disposent ni de l'un ni de l'autre. Pour autant, les progrès sont considérables, puisque sous l'impulsion de la Commission européenne, 12 pays se sont dotés d'une stratégie nationale depuis 2013.

4.2.b Régulation juridique du cyberespace

Les législateurs européens ont une grande responsabilité dans la mise en place d'une SRI efficace. En effet, il leur appartient de définir le cadre légal qui permettra aux acteurs publics et privés de disposer des outils nécessaires pour relever les futurs défis de cybersécurité. L'UE dispose aujourd'hui de plusieurs textes dans ce domaine. Seuls 3 Etats[22] n'ont toujours pas ratifié la Convention de Budapest de 2001. Pour autant, tous les pays ne disposent pas d'un cadre juridique solide en matière de cybersécurité à l'instar de la Belgique, du Danemark ou

[22] http://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/185/signatures;

de la Pologne[23]. Cette lacune apparait comme une véritable faiblesse dans la SRI européenne puisque les cyberdélinquants peuvent ainsi agir en toute impunité à partir de pays ne disposant ni de réglementation ni de législation appropriées. Il est par conséquent primordial d'homogénéiser les dispositifs législatifs des pays européens malgré les réticences de certains Etats qui militent pour un internet totalement libéralisé.

4.2.c Règles, normes et standards

L'UE souhaite mettre en place un système de normes garantissant une cybersécurité d'un bout à l'autre de la chaîne des produits TIC. Or, le monde numérique n'est aujourd'hui pas gouverné par une seule entité. Il existe en effet une multitude d'acteurs publics et privés qui interviennent dans le développement du cyberespace. Les difficultés rencontrées dans ce domaine sont par conséquent nombreuses. Tout d'abord, la majorité des leaders mondiaux sont des sociétés américaines (Google, Apple, etc.) qui ont leurs propres visions stratégiques et imposent leurs propres règles. En outre, l'influence européenne dans l'internet et le numérique en général demeure limitée et il semble ainsi illusoire de vouloir imposer des normes européennes sans l'obtention préalable d'un consensus international. Enfin, la multiplication des normes et des référentiels peut également nuire à l'interopérabilité entre des systèmes d'origines hétéroclites.

4.2.d Des alliances difficiles

L'opacité offerte par le cyberespace permet aux Etats de dissimuler leurs forces mais également leurs faiblesses et leurs vulnérabilités. Si les alliances classiques permettent de réunir des capacités et des moyens pour augmenter un rapport de force face à un ennemi commun, dans le cyberespace, les coopérations reposent d'abord sur le partage d'informations. Hors dans un contexte de concurrence économique exacerbée, où l'information représente une valeur marchande, la communication de ses faiblesses mais également le partage de sa technologie et de ses techniques constituent un véritable risque. Les différentes affaires rendues publiques ces dernières années[24] démontrent la fragilité des alliances dans un domaine où nos partenaires militaires, politiques et commerciaux peuvent constitués une menace pour nos intérêts.

[23] Moins de la moitié des pays européens disposent d'un cadre juridique considéré comme au moins suffisant : http://www.bsa.org/~/media/Files/Policy/Security/EU/study_eucybersecurity_fr.pdf.

[24] Affaire Snowden sur le programme Prism américain en 2013, espionnage de l'Elysée par les USA entre 2006 et 2012, révélation en 2013 de la mise sur écoute du téléphone portable de la chancelière allemande par la NSA, etc.

4.3 **Des succès encourageants**

4.3.a Une coopération qui se met en place

L'efficacité de la lutte contre la cybercriminalité repose essentiellement sur la coopération et la coordination entre les différents pays européens. En effet, la multiplication des menaces cybernétiques et leur caractère transnational obligent aujourd'hui la communauté européenne à se mobiliser et à collaborer. La mise en place d'organismes tels que l'ENISA ou l'EC3 a permis à l'UE de disposer des outils lui permettant d'améliorer la coordination entre les moyens nationaux des Etats membres. Cette coopération est aujourd'hui effective dans le domaine judiciaire où l'EC3 joue un rôle prépondérant dans les affaires pan-européennes. La création ces dernières années des CERT dans presque tous les pays européens permet à l'UE de s'appuyer sur un réseau complet d'alerte et de réaction aux attaques informatiques sur l'ensemble de son territoire. Enfin, la multiplication des exercices européens de cybersécurité a permis de mettre en place et de consolider des procédures tout en entrainant l'ensemble des acteurs européens du domaine face à une cybercrise majeure en Europe.

4.3.b Entrainements et exercices au niveau européen

Les différentes stratégies du numérique et de cybersécurité de l'UE insistaient sur la nécessité de mettre en place des exercices nationaux et européens pour améliorer l'efficacité des organismes de SRI et la coordination entre les différentes structures nationales et européennes. Pour autant, en 2015, seuls 16 pays[25] organisaient des exercices nationaux de cybersécurité. L'UE procède pour sa part à un exercice biannuel du niveau pan-européen depuis 2010[26]. Au cours de l'exercice Cyber Europe 2014, 200 organisations et 400 professionnels de la cyber-sécurité originaires de 29 pays [27] européens ont testé leur réactivité face à plus de 2000 cyber-incidents. Cet exercice visait « *à tester entre autres les procédures destinées à partager des informations opérationnelles sur les cyber-crises en Europe, à améliorer les capacités nationales de réponse aux cyber-crises, à explorer les effets d'échanges multiples et parallèles entre le privé et le public ainsi qu'au sein du privé au*

[25] Allemagne, Autriche, Belgique, Bulgarie, Danemark, Estonie, Finlande, France, Grèce, Irlande, Italie, Lettonie, Pays-Bas, Royaume-Uni, Slovaquie, Suède : http://www.bsa.org/~/media/Files/Policy/Security/EU/study_eucybersecurity_fr.pdf

[26] Cyber Europe 2010 avec la participation de 22 Etats membres de l'UE, 70 experts des organismes publics participants ont collaboré pour contrer plus de 300 cyber-attaques simulées : 4 novembre 2010.

[27] Dont 26 pays membres de l'UE.

niveau national et international »[28]. Il a permis de démontrer que l'Europe disposait aujourd'hui des procédures et de la coordination nécessaires pour dissiper une cyber-crise majeure. La prochaine édition de Cyber Europe qui se déroulera à l'automne 2016 devrait être le plus grand exercice de cybersécurité au monde. Aussi l'Europe est en passe d'atteindre collectivement son objectif même si individuellement, les Etats membres ont encore une marge de progrès significative.

4.3.c La recherche et le développement

Dans le cadre d'une stratégie de cybersécurité globale et exhaustive, il est impératif de poursuivre les efforts déjà consentis[29] dans le domaine de la R&D et de l'innovation. La stratégie de 2013 s'appuie à ce titre sur le programme « Horizon 2020 » pour élaborer les différents outils et instruments qui permettront de lutter efficacement contre les activités criminelles et terroristes qui visent le cyberespace. Ce programme européen de 79 Mds € pour la période 2014-2020 doit entre autres *« promouvoir une politique industrielle forte, un secteur européen des TIC fiable, favoriser le marché intérieur et limiter la dépendance de l'Europe vis-à-vis des technologies étrangères »*[30]. Cette politique de financement doit bien évidemment être complétée par les investissements des secteurs public et privé des différents Etats membres. L'UE a par conséquent parfaitement pris en compte les problématiques de cybersécurité et de cyberdéfense au travers du programme « Horizon 2020 » même si les volumes financiers restent faibles par rapport au financement total de R&D en Europe[31] et dans certains pays asiatiques[32].

5 Conclusion

En parallèle de ses stratégies successives pour le numérique qui offrent aux citoyens et entreprises européennes les capacités et moyens de tirer pleinement profit des NTIC et de leurs perspectives économiques, l'UE s'investit dans la cybersécurité et la cyberdéfense. Dès 2001, elle a construit sa stratégie dans le domaine en mettant en place les outils nécessaires à sa mise en œuvre sur le plan législatif avec la Convention de Budapest, sur le plan

[28] https://www.enisa.europa.eu/news/enisa-news/prs-in-french/le-plus-grand-exercice-de-cybersécurite-en-europe-a-lieu-aujourd2019hui.

[29] Dans le cadre des différents Programmes cadres de recherche et développement technologique (PCRDT).

[30] COM (2013) 1 : Communication conjointe au Parlement européen, au Conseil et au Comité économique et social européen et au Comité des régions. Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé. - 7 février 2013.

[31] Environ 2% du PIB de l'UE

[32] Notamment Japon et Corée du Sud.

opérationnel avec la création de l'ENISA, des CERT et du Centre européen de lutte contre la cybercriminalité ou encore au niveau technologique particulièrement en Recherche et Développement.

Malgré les progrès dans l'élaboration d'une stratégie commune de cybersécurité et de cyberdéfense et la volonté affichée par l'UE de poursuivre l'intégration européenne dans ce domaine, les avancées demeurent lentes et fastidieuses. L'établissement de compromis et de consensus entre 28 Etats membres souligne cette difficulté. En effet, le délai nécessaire entre l'élaboration d'une stratégie par la Commission européenne, sa validation par le Conseil puis sa transformation en résolution législative par le parlement européen demeure considérable. De plus, la mise en œuvre de ces directives par les pays de l'Union est soumise à la volonté et aux capacités techniques des Etats membres. Enfin les réticences en matière de partage d'information ne favorisent ni la coopération ni l'amélioration des procédures et des politiques de cybersécurité des pays européens.

En conclusion, la mise en œuvre d'une cyberstratégie européenne semble aujourd'hui possible. La volonté de l'UE d'investir ce nouveau champ des confrontations et les moyens humains, financiers et industriels dont elle dispose, lui permettent d'aborder l'avenir avec ambition.

Bibliographie

Les articles, rapports et communications :

- COM(2001) 298 : « Sécurité des réseaux et de l'information : proposition pour une approche politique européenne » du 6 juin 2001 ;
- Convention de Budapest sur la cybercriminalité STE n°185 du 23 novembre 2001 ;
- Règlement (CE) 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information ;
- Décision cadre 2005/222/JAI du Conseil 24 février 2005 relative aux attaques visant les systèmes d'information ;
- COM(2005) 229 : « i2010 - Une société de l'information pour la croissance et l'emploi » du 1er juin 2005 ;
- COM(2006) 251 : « Une stratégie pour une société de l'information sûre – dialogue, partenariat et responsabilisation » du 31 mai 2006 ;
- Règlement (CE) 1007/2008 du Parlement européen et du Conseil du 24 septembre 2008 modifiant le règlement (CE) 460/2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information en ce qui concerne sa durée ;
- COM(2009) 149 : relative à la protection des infrastructures d'information critiques (PIIC) : « Protéger l'Europe des cyberattaques et des perturbations de grande envergure : améliorer l'état de préparation, la sécurité et la résilience » de mars 2009 ;
- COM(2010) 245 : « Une stratégie numérique pour l'Europe » du 19 mai 2010.
- COM(2010) 517 : Proposition de directive du Parlement européen et du Conseil du 30 septembre 2010 relative aux attaques visant les systèmes d'information.
- COM(2010) 520 : Proposition du Parlement européen et du Conseil modifiant le règlement (CE) 460/2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information.
- COM(2011) 163 : relative à la protection des infrastructures d'information critiques (PIIC) : « Réalisations et prochaines étapes: vers une cybersécurité mondiale » du 31 mars 2011;
- 4ème séminaire IHEDN de Bruxelles : Vers une cyberstratégie européenne ? 28 juin 2012.

- Rapport d'information au nom de la commission des affaires étrangères, de la défense et des forces armées sur la cyberdéfense : **Sénateur Jean-Marie BOCKEL** – 18 juillet 2012.
- COM (2013) 1 : Communication conjointe au Parlement européen, au Conseil et au Comité économique et social européen et au Comité des régions. Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé. - 7 février 2013.
- COM (2013) 48 : Proposition de directive du Parlement européen et du Conseil concernant les mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union du 7 février 2013.
- Rapport n°491 du Sénat sur la stratégie européenne de cybersécurité, déposé par les **Sénateur Jean-Marie BOCKEL et Jacques BERTHOU** - 10 avril 2013.
- Sécurité globale : La cyberstratégie de l'Union européenne. **Olivier KEMPF** - Eté 2013.
- Sécurité globale : La cyberdéfense : un enjeu global et une priorité stratégique pour le ministère de la défense. **Contre-amiral Arnaud COUSTILLIERE** – Eté 2013.
- EISAS – European Information Sharing and Alerting System : Deployment Feasibility Study - December 2013;
- Résolution législative du Parlement européen du 13 mars 2014 sur la proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union (COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)) ;
- Tableau de bord de la cybersécuritté dans l'UE : vers un cyberespace européen sécurisé – BSA de 2015 ;
- ENISA Cyber Europe 2014 – After Action Report du 23 septembre 2015
- Europol Review 2014 du 8 septembre 2015;
- European Defence Matters, Magazine issue 9 : European secure cyberspace : our common realm – 26 Novembre 2015.
- Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union - 18 décembre 2015

<u>Les ouvrages :</u>

- Introduction à la cyberstratégie – Economica, 2012 : **Olivier KEMPF**.

- Cyberstratégie, l'art de la guerre numérique – Nuvis-phebe Editions, 2012 : **Bertrand BOYER**.
- Alliances et mésalliances dans le cyberespace – Economica, 2014: **Olivier KEMPF**.
- Cybertactique : Conduire la Guerre Numerique – Nuvis-phebe Editions, 2014 : **Bertrand BOYER**.
- Gagner les cyberconflits : au-delà du technique – Economica, 2015 : **François-Bernard HUYGHE, Olivier KEMPF, Nicolas MAZZUCCHI**.

ANNEXE

Tableau de maturité des politiques de cybersécurité des Etats membres de l'UE en 2015[33]

	CERT national	Stratégie nationale	Agence	Autorité nationale	Convention de Budapest	
					Signature	Ratification
Allemagne	X	2011	X	x	23/11/2001	09/03/2009
Autriche	X	2013	X	En cours	23/11/2001	13/06/2012
Belgique	X	2012	X	x	23/11/2001	20/08/2012
Bulgarie	X		CERT	x	23/11/2001	07/04/2005
Chypre		2013		En cours	23/11/2001	19/01/2005
Croatie	X		CERT	x	23/11/2001	17/10/2002
Danemark	X		X	x	22/04/2003	21/06/2005
Espagne	X	2013	X	x	23/11/2001	03/06/2010
Estonie	X	2014	CERT	x	23/11/2001	12/05/2003
Finlande	X	2013	X	x	23/11/2001	24/05/2007
France	X	2011	X	x	23/11/2001	10/01/2006
Grèce	X		CERT	x	23/11/2001	
Hongrie	X	2013	X	x	23/11/2001	04/12/2003
Irlande					28/02/2002	
Italie	X	2014	CERT	x	23/11/2001	05/06/2008
Lettonie	X	2014	CERT	x	05/05/2004	14/02/2007
Lituanie	X	2011	CERT	x	23/06/2003	18/03/2004
Luxembourg	X	2013	X	En cours	28/01/2003	16/10/2014
Malte	X		X	x	17/01/2002	12/04/2012
Pays-Bas	X	2013	X	En cours	23/11/2001	16/11/2006
Pologne	X	2013	CERT	En cours	23/11/2001	20/02/2015
Portugal	X	DRAFT	X	x	23/11/2001	24/03/2010
République Tchèque	X	2011	X	x	09/02/2005	22/08/2013
Roumanie	X	2013	X	x	23/11/2001	12/05/2004
Royaume-Uni	X	2011	X	x	23/11/2001	25/05/2011
Slovaquie	X	2008	CERT	x	04/02/2005	08/01/2008
Slovénie	X		CERT	x	24/07/2002	08/09/2004
Suède	X		X	x	23/11/2001	

[33] : http://www.bsa.org/~/media/Files/Policy/Security/EU/study_eucybersecurity_fr.pdf