Université catholique de Louvain

Faculté des sciences économiques, sociales, politiques et de communication (ESPO)
Ecole des Sciences Politiques et Sociales (PSAD)

Gouvernance de la cyber-sécurité européenne : Protection des infrastructures d'information critiques

La régulation du réseau d'acteurs impliqués dans la protection des infrastructures d'information critiques

Mémoire réalisé par
Fabio Bianchi

Promoteur(s)
Pr. Pierre Vercauteren

Lecteur
Pr. Tanguy Struye de Swielande

Année académique 2016-2017
Master en Sciences politiques, orientation relations internationales, à finalité spécialisée

Chaussée de Binche, 151 – 7000 Mons, Belgique

Je tiens à remercier mon promoteur, le Professeur Pierre Vercauteren pour le suivi tout au long de ce mémoire et ses conseils avisés afin de mener cette recherche à bien.
Je tiens à remercier mes parents et ma famille pour leur soutien.
Je tiens également à remercier les amis de la Convers, Diego, Luca, Gillian, Jacob pour leur soutien et leurs conseils avec une attention particulière à Jacob pour ses playlists motivantes.
Finalement, je tiens à remercier Margot et ma maman pour le temps consacré à la relecture de ce mémoire.

Résumé

Ce mémoire de recherche en sciences politiques abordera la question de la gouvernance de la cyber-sécurité européenne et en particulier à la protection des infrastructures d'information critiques. Ces infrastructures sont d'une importance capitale pour le bon fonctionnement de notre société. En effet, une défaillance de ces infrastructures aurait de grave conséquences. Ces conséquences, en raison de l'interdépendance existant entre les Etats membres pourraient impacter l'ensemble de l'Union européenne. C'est pourquoi il est essentiel de développer des politiques européennes et d'harmoniser les politiques nationales en matière de cyber-sécurité afin de minimiser au maximum les risques. Cependant, l'Union européenne ne dispose pas de toutes les ressources nécessaires afin d'élaborer et de mettre en œuvre ces politiques. En effet, la protection des infrastructures d'information critiques implique une multitude d'acteurs que ce soit au niveau européen ou national et issus des secteurs public et privé. Afin de parvenir à une mise en œuvre efficace des politiques européennes de protection des infrastructures critiques, l'Union européenne doit amener toutes les parties prenantes à coopérer et à agir dans le sens du bien commun. Ainsi, l'UE exerce un rôle de régulateur du système de gouvernance de la protection des infrastructures d'information critiques. C'est justement cette régulation, ou méta-gouvernance, qui fera l'objet de la question de recherche de ce mémoire, à savoir, « Comment l'Union européenne régule-t-elle le réseau d'acteurs impliqués dans la mise en œuvre des politiques de protection des infrastructures d'information critiques ? ». Afin d'y répondre, les mesures prises officiellement par l'Union européenne seront analysées et ce, en fonction des théories de la méta-gouvernance et plus particulièrement de la typologie des modes opératoires de la méta-gouvernance présentée par Eva Sorensen. Il ressortira de cette analyse les divers modes opératoires de la méta-gouvernance exercée par l'UE en fonction de l'acteur ayant entrepris ces mesures et en fonction de la cible de cette régulation.

Table des matières

Table des annexes

Introduction

Dans le cadre de ce mémoire de recherche en relations internationales, il a été décidé de s'intéresser à la gouvernance de la cyber-sécurité européenne. La cyber-sécurité possédant de nombreux domaines comme, la protection des données personnelles, le cyber-terrorisme, la lutte contre la cyber-pédopornographie et bien d'autres, il a été décidé de se concentrer sur un aspect particulier de la cyber-sécurité : la protection des infrastructures d'information critiques. Ces infrastructures revêtent un caractère essentiel au bon fonctionnement de notre société et au bien-être du citoyen. En effet, une défaillance de ces infrastructures entrainerait de graves conséquences dans la distribution de l'énergie ou encore dans le fonctionnement des administrations par exemple.[1] Ces politiques de sécurité relèvent de l'acteur étatique[2]. Cependant, une des caractéristiques principales d'internet et des réseaux de l'information est d'être sans frontières. Ainsi des politiques nationales non coordonnées ne permettent pas de faire face aux menaces pesant sur les infrastructures d'information critiques. C'est pourquoi, afin d'assurer une protection optimale de ces infrastructures au niveau européen il est essentiel d'avoir une politique européenne de cyber-sécurité. Afin d'y parvenir, les Institutions européennes travaillent depuis le début des années 2000 à l'élaboration de stratégies européennes en matière de cyber-sécurité et en particulier en matière de protection des IIC. Cependant, l'Union européenne ne détient pas toutes les ressources nécessaires à l'élaboration et la mise en œuvre de ces politiques de sécurité. En effet, comme précédemment mentionné, l'élaboration des politiques de sécurité s'effectue au niveau national. Deuxièmement, le secteur privé détient et exploite une grande partie de ces infrastructures d'information critiques. C'est pourquoi, l'UE doit amener tous les acteurs à œuvrer dans l'intérêt commun et ce en conciliant les intérêts individuels de ces acteurs agissant de manière indépendante. Pour ce faire, l'Union européenne dispose de différentes possibilités d'action. C'est justement ces modes d'action qui font l'objet de cette recherche. Ainsi, ce mémoire tentera de répondre à la question suivante : « Comment l'Union européenne régule-t-elle le réseau d'acteurs impliqués dans la mise en œuvre des politiques de protection des infrastructures d'information critiques ? »

Afin de répondre à cette question, la théorie de la méta-gouvernance sera employée comme grille d'analyse et plus particulièrement une typologie des différents modes d'exercice de la

[1] Journal officiel de l'Union européenne (2009), Résolution du Conseil du 18 décembre 2009 sur une approche européenne concerté en matière de sécurité des réseaux et de l'information, 2009/C 321/01

[2] Commission européenne (2013a), 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, JOIN(2013) Final, p.5

méta-gouvernance présentée par Eva Sorensen. La recherche et l'analyse seront orientées en vue de répondre aux trois hypothèses de ce mémoire. Celles-ci sont : 1) L'Union européenne (sous-entendu ici la Commission, le Parlement européen et le Conseil) assure, seule, la régulation du réseau d'acteurs impliqués dans la protection des infrastructures d'information critiques ; 2) Chaque Institution exerce une fonction propre en tant que méta-gouvernant du réseau d'acteurs impliqués dans la protection des infrastructures d'information critiques ; 3) L'Union européenne (sous-entendu ici, les Institutions (Conseil, Parlement et Commission ainsi que l'Agence en charge de la sécurité des réseaux et de l'information – ENISA) exerce son rôle de méta-gouvernant de manière hands-on, en interaction directe avec les acteurs impliqués dans la protection des infrastructures d'information critiques.

La première hypothèse s'intéressera à la capacité des trois institutions européennes à assurer leur rôle de méta-gouvernant. La seconde se concentrera sur le rôle de chacun des méta-gouvernant dans l'exercice de la régulation du réseau d'acteurs. La troisième est en relation directe avec le cadre théorique et s'intéressera à un mode d'action en particulier. Le choix a été fait de ne pas développer une hypothèse concernant les modes d'actions *hands-off* en raison des caractéristiques de la gouvernance européenne[3] et des compétences de l'UE. Ainsi il semblait, au regard de ces éléments, que l'UE agirait de manière *hands-off*. Il est apparu en revanche plus intéressant et plus pertinent dans le cadre de cette recherche, de s'intéresser aux modes d'actions concernant des interactions directes avec les acteurs et une participation au réseau en tant qu'acteur à part entière.

Avant de poursuive cette introduction par la structure de ce mémoire, il est important de préciser les limites de ce mémoire. Ainsi, la première limite de ce mémoire a trait aux consignes de celui-ci. Etant limité dans sa longueur, il était nécessaire de trouver un juste milieu dans les éléments à analyser. La balance devait être faite entre l'analyse d'un nombre important d'éléments et ainsi un meilleur aperçu de la méta-gouvernance exercée par l'UE et une analyse en profondeur de chaque élément réduisant de la sorte le nombres de mesures pouvant être analysées. Il a donc été décidé de limiter l'analyse aux actions entreprises entre 2005 (adoption d'un livret vert concernant un programme de protection des infrastructures critiques[4] et 2013 (adoption d'une stratégie européenne de cyber-sécurité[5]) et de ne pas analyser chaque mesure individuellement. La deuxième limite de ce mémoire a trait au caractère sensible du sujet traité.

[3] BORZEL A.T. (2012), *The European union – a unique governance mix? , in, LEVI-FAUR D.* (2012),, *the oxford Handbook of governance*, Oxford University Press, OXFORD, ch 43

[4] Commission des Communautés européennes (2005), Livret vert sur un programme européen de protection des infrastructures critiques, COM(2005)576 final, Bruxelles

[5] Commission européenne (2013a), *op.cit.*

En effet, la protection des infrastructures critiques relève également des politiques de défense et de sécurité. Pour cette raison, les demandes d'entretien, formelles et informelles, avec les autorités politiques européennes et nationales se sont vues refusées. En raison de ces refus, seules les mesures prises officiellement par l'Union européenne seront analysées. Les relations informelles entre acteurs ne seront donc pas ici traitées. Ainsi, la réponse à la question de recherche ne tiendra compte que des actions entreprises de manière officielle de l'Union européenne.

Ce mémoire sera divisé en trois chapitre. Le premier sera consacré au cadre théorique. Seront présentées les théories de la gouvernance, de la gouvernance en réseau et finalement de la méta-gouvernance avec une attention particulière au travail d'Eva Sorensen.

Le deuxième chapitre sera consacré aux actions entreprises par l'Union européenne dans le cadre de la régulation du réseau d'acteurs impliqués dans la protection des infrastructures d'information critiques. Finalement, le dernier chapitre de ce mémoire sera consacré à l'analyse de tous les éléments précédemment exposés et à la réponse aux hypothèses.

Chapitre 1 : Théorie

Ce premier chapitre sera consacré au cadre théorique du mémoire. La première partie de ce chapitre d'intéressera à la gouvernance de manière générale. Son origine, ainsi que ses différentes significations. La seconde partie présentera un aspect particulier de la gouvernance, la gouvernance en réseau. Cette théorie sera développée en fonctions des travaux de Rhodes, Kooiman ou encore Jacob Torfing et Eva Sorensen. Finalement la troisième partie sera consacrée à la méta-gouvernance ou la gouvernance de la gouvernance. C'est cette théorie et en particulier la conception et la typologie proposée par Eva Sorensen qui fera office de grille d'analyse pour ce mémoire.

1.1 La Gouvernance

S'il y a encore de cela 20 ans, le terme gouvernance ne se referait qu'à un ancien terme de la langue anglaise tombé dans l'oubli, il est devenu à la mode ces dernières années dans le vocabulaire des sciences sociales et de la science politique[6]. Mais que signifie le terme gouvernance ? La gouvernance émerge dans la littérature pour expliquer les processus de décisions collectifs induits par le changement de nos sociétés. En effet, le seul acteur étatique, face à la mondialisation et à la complexification des problèmes, ne peut, à lui seul, gouverner la société. La gouvernance apparait donc pour expliquer et chercher à comprendre la construction de ces décisions collectives.[7] Le terme gouvernance apparait dans le vocabulaire de la science politique dans le milieu des années 1980, il est alors utilisé dans le domaine de l'analyse des politiques publiques et plus particulièrement pour les politiques communales au Royaume-Uni.[8] Cependant, ce mot est déjà utilisé depuis les années 30 aux Etats-Unis en référence à la *corporate governance* et au secteur privé. Il est ensuite utilisé par la Banque Mondiale en termes de *good governance* concernant le développement en Afrique.[9]

Le terme gouvernance revêt un aspect pluri-sémantique en fonction du qualificatif qui le suit et du domaine dans lequel il est employé. Dans ce mémoire, le champ d'utilisation du terme

[6] CHHOTRAY V. STOKER G., (2009) *governance theory and practice : a cross-disciplinary approach*, PALGRAVE MACMILLAN, New York, pp 1-2
[7] *Idem* p2
[8] HERMET G., BADIE B., BIRNBAUM P., BRAUD P.(2005), Dictionnaire de la science politique et des institutions politiques, 6e édition, ARMAND COLIN, Paris, p 138
[9] *ibidem*

gouvernance sera restreint au champ de la science politique. Les sections suivantes présenteront les principaux auteurs et leurs définitions de la gouvernance.

Les deux premières définitions présentées sont celle de Le Galès et celle de Stoker. Pour le Galès la gouvernance est : *« un processus de coordination d'acteurs publics et privés, de groupes sociaux, d'institutions destinés à atteindre des buts propres discutés et définis collectivement dans des environnements fragmentés, incertains. »*[10] Stoker, lui, trouve l'essence de la gouvernance dans le fait qu'elle consiste à rechercher la manière dont les décisions collectives prises par les gouvernements et les Etats, ainsi que les politiques et les objectifs stratégiques établis par les entreprises, peuvent être entrepris de manière efficace et légitime[11] et de définir la gouvernance de la sorte : *« Governance is about the rules of collective decision-making in settings where there are a plurality of actors or organisations and where no formal control system can dictate the terms of the relationship between these actors and organisations.»*[12]. De cette definition Stoker met en exergue quatre éléments. Premièrement, les règles, formelles et informelles qui régissent et encadrent et influencent les actions, les decisions et les responsabilités dans le processus de décision[13]. Deuxièmement l'aspect collectif que revêt le processus de decision, celui-ci impliquant une multitude d'acteur agissant selon leurs propores intérets. Parmi cette multitude d'acteurs seuls quelques uns ont la possibilité de prendre l'initiative de cette prise de decision mais l'approbation de la responsabilité en découlant est l'affaire de tous. [14] Le troisième élément souligné par Stoker est celui du « *Decision-making* » qui est, pour lui, la vision stratégique et la mise en œuvre quotidienne des pratiques d'une organisation. [15] Le dernier point ressorti par Stoker est le fait qu'aucun acteur au sein du système de gouvernance ne détient les ressources nécessaires au contrôle du processus de décision via les attributs classiques que sont la légitimité et la coercition. De ce fait, les interactions entre acteurs s'effectuent sur base de négociations, d'influence et de communication. [16]

Suite à ces deux premières définitions mettant l'accent sur les acteurs et les règles entourant la gouvernance, la définition suivante s'intéresse à l'objet de la gouvernance en elle-même. Cette

[10] *Ibidem*
[11] CHHOTRAY V. STOKER G. (2009), *op cit*. P2
[12] *idem*, p3
[13] *Idem* pp3-4
[14] *idem*, p4
[15] *ibidem*
[16] *ibidem*

définition est le fruit du travail de R.A.W Rhodes pour qui la gouvernance signifie : « *a change in the meaning of government, referring to new processes of governing ; or changed conditions of the ordrerd rule ; or new methods by which society is governed.»*[17]. Rhodes a une triple vision de la gouvernance. Ainsi il la divise en trois vagues distinctes : la *network governance* (1ere vague), *la meta-governance* (2e vague) et l'*interpretative governance* (3e vague) [18]. Les deux premières vagues feront respectivement l'objet de la section 1.2 et 1.3 de ce chapitre elles ne seront donc pas développées dans cette partie. La troisième vague est, comme son nom l'indique, d'ordre interprétatif. Elle trouve son essence dans la recherche de compréhension du changement de modèle via un focus sur les acteurs et leurs interprétations des croyances et des pratiques selon un cycle de réforme. [19]

La prochaine conception de la gouvernance est celle de Jan Kooiman. Celui-ci se focalise sur l'aspect « interaction » de la gouvernance. En préambule, il est important d'effectuer une précision sémantique. Kooiman parle dans son travail de *governing*, *governance* et *governability*. Il définit *governing* comme : *« the totality of interactions, in which public as well as private actors participate, aimed at solving societal problems or creating societal opportunities ; attending to the institutions as contexts for these governing interactions ; and establishing a normative foundation for all those interactions.»*[20]. Il définit la gouvernance comme : *«the totality of theoritical conceptions on governing ».*[21], d'ajouter un aspect plus pratique à la définition de la gouvernance qu'il conçoit comme : *«the pattern or structure that emerges in a social-political system as common result or outcome of the interacting intervention efforts of all involved actors »*[22] Enfin, il définit governability comme : *« the total quality of a social-political system to govern itself within the context of broader systems of which it is part. It combines qualities of governing and of governance (in interaction) »*[23]
Pour Kooiman, dans notre société actuelle, l'activité de gouverner, le *governing* pour reprendre son terme, est un ensemble de processus d'interactions entre les acteurs publics et les acteurs impliqués ou cible des actions publiques. Cette constatation résulte du fait que notre société est caractérisée par la complexité, la diversité et la dynamique. Il tire trois constats de ce fait, le

[17] RHODES R.A.W. (2012), *Waves of governance*, *in*, LEVY FAUR D. (2012), *the oxford Handbook of governance*, Oxford University Press, OXFORD, ch 3 p33
[18] *ibidem*
[19] *Idem* p40
[20] KOOIMAN J. (2003), Governing as governance, SAGE, London, p4
[21] *ibidem*
[22] KOOIMAN J. (1994), *Modern governance : new government society interactions*, SAGE, London p 256
[23] *idem*, p 259

premier est que les problèmes sociaux, pour la plus grande partie, sont causés par des interactions entre plusieurs facteurs (et pas toujours connus) et non par un facteur unique. Le deuxième est que les connaissances techniques et politiques du problème et de ses solutions sont dispersées entre plusieurs acteurs. Et troisièmement, les objectifs de l'action publique sont empreints d'incertitude, ils ne sont pas aisés à définir et doivent faire l'objet de révisions constantes.[24]

Les différents modes de gouverner ces sociétés sont donc des processus interactifs et consistent à des actions de *steering, regulating and balancing* de ces interactions le tout au sein d'un environnement qui allie à la fois les rapports hiérarchiques et non-hiérarchiques. Si des nouveaux modes de gouvernance sont plus opportuns et plus attractifs dans cette société, le rôle de l'Etat et ses modes classiques plus *top-down* et formels n'en restent pas moins pertinents dans certaines situations.[25] A l'instar de Rhodes, Kooiman effectue également une triple division de la gouvernance. Cette division s'opère en termes d'ordre. Le 1er ordre correspond aux problèmes et aux opportunités, le 2e ordre correspond aux conditions et au cadre institutionnel de la gouvernance. Enfin le 3e ordre est celui de la méta-gouvernance. [26]

Avant de conclure cette partie consacrée à la gouvernance, une dernière définition de la gouvernance va être présentée. Jusqu'à présent, seule des définitions issues d'auteurs européens ont été exposées. Cette dernière définition est, elle, le fruit d'un auteur américain, James Rosenau. Pour lui, la gouvernance peut être définie comme : « *a system of rule that is as dependant on intersubjective meanings as on formally sanctioned constitutions and charters. […] it works only if it is accepted by the majority (or at leats by the most powerful of those it affects).*»[27]

En conclusion de cette partie, il est opportun de récapituler les principales caractéristiques de la gouvernance mentionnées dans cette section. Ainsi les theories de la gouvernance peuvent être comprises, dans le champ de la science politique, comme un mode alternatif de comprehension des processus de prise de decision impliquant des acteurs publics et privés

[24] *Idem*, p.255
[25] *ibidem*
[26] KOIIMAN J. (2003), *op.cit.*, pp.135-189
[27] ROSENAU J. (1992), *Governance, order and change in world politics*, in, ROSENAU J. and CZEMPIED E.-O. (1992), *Governance without government: order and change in world politics*, UNIVERSITY PRESS, CAMBRIDGE Ch16 p4

intéragissant entre eux via la négociation, l'influence et la communication. Ce système est encadré par des règles formelles et informelles.

Le choix des théories de la gouvernance s'imposait dans ce mémoire. En effet, cette théorie s'inscrit pleinement dans la question de recherche et dans le cas pratique à analyser. Le nombre important d'acteurs publics et privés ainsi que la complexité qui caractérise les politiques de protection des infrastructures d'information critiques rendaient difficile une comprehension optimale du sujet traîté par les theorie classique d'analyse des politiques publiques notemment. Afin d'afiner encore plus notre analyse, un focus sur un concept particulier de la gouvernance sera effectué. En effet, comme mentionné précédemment, la gouvernance revêt un sens different en fonction du qualifictif qui le suit. Le choix a été fait dans ce mémoire de s'intéresser de plus près à la gouvernance en réseau (*network governance).* Cette forme de gouvernance fera l'objet de la section suivante.

1.2 La gouvernance en réseau - *Network governance*

Faire la distinction entre gouvernance et *network governance* peut paraitre superflue tant, dans la littérature, les deux concepts sont liés, alors que les autres champs de la gouvernance sont précisés par l'adjectif les précédant (*corporate, good,…*) et sont reliés non pas aux théories de la gouvernance mais à celles du gouvernement ou encore du *new public management*[28] Cependant, il est intéressant dans le cadre de ce mémoire de s'attarder sur la *network governance* afin d'en comprendre les principales caractéristiques et introduire une nouvelle génération d'auteur dans cette littérature, en l'occurrence dans ce mémoire, Jacob Torfing et Eva Sorensen. Ces auteurs, fortement inspirés par Rhodes dans leur conception de la *network governance,* s'intéressent également aux moyens d'amener le réseau vers une efficacité maximale et ce, par le biais de la méta-gouvernance. Ce concept fera l'objet de la troisième section de cette partie théorique. Pour l'heure définissons la *network governance* et présentons brièvement ses principales caractéristiques à l'aide des travaux de Klijn, Rhodes, Sorensen, Torfing et Kooiman notamment.

Dans la littérature consacrée à la gouvernance en réseau, cohabitent trois traditions de recherche se distinguant sur leur champ académique d'origine ainsi que sur leur objet d'étude.[29] Ces

[28] KLIJN E.-H. (2008), *Governance and Governance Networks in Europe, an assessment of ten years of research on the theme, in ,* Public Management Review, Vol 10 : 4 : 2008, pp 505-525p P 510
[29] *idem*, p512

traditions sont celles des recherches sur le *policy network,* sur l'*inter-organizational service delivery and policy implementation* et enfin sur le *governing network*[30]. Malgré ces différences le concept de réseau est au centre de ces traditions et celles-ci se complètent dans la recherche de la compréhension du fonctionnement des réseaux et de leur gouvernance et ce, de manière globale[31]

Avant de parcourir les différentes approches de la gouvernance en réseau il est opportun de faire une précision sémantique concernant les termes employés par les différents auteurs. Dans la littérature une confusion sémantique peut parfois s'opérer entre les termes *policy network* et *network governance*. Sur ce point, Blanco, Lowndes et Prachett ont apporté un éclaircissement. Ainsi, ils dressent les similitudes et surtout les différences entre ces deux termes. [32] Ismael Blanco a, dans son article concernant les différences entre le *policy network* et *la governernance network*, établi une liste de différences en 8 points. Nous pouvons résumer sa vision de la *Gouvernance Network* comme un nouveau paradigme des politiques, s'inscrivant dans une comparaison passé / présent, insistant sur la différence entre le modèle de réseau et les modèles classiques de la hiérarchie et de marché, ayant un ancrage territorial et multi-scalaire sur des problèmes émergents et/ou sévères, ayant des interactions s'inscrivant sur une logique de confiance, loyauté et réciprocité. Ces relations s'effectuent dans un carde plus formel, institutionnalisé et permettaient divers modes de gouvernance de ce réseau en contradiction avec les modèles hiérarchiques[33].

Le travail de Rhodes et plus particulièrement sa définition de la *network governance* sera le point de départ de cette partie. Dans ses recherches concernant la gouvernance Rhodes s'est attardé sur le concept de la gouvernance en réseau. Comme pour la gouvernance, la vision de Rhodes sera exposée par la définition ou plutôt la conception qu'il donne de la gouvernance en réseau. Pour lui, cette dernière est comprise comme un modèle alternatif de la compréhension du mode de gouvernent du Royaume-Uni venant palier aux manques des modèles théoriques classiques que sont ceux de la hiérarchie et du marché. [34] Bien que le terme *network governance* ne figure pas encore dans ses travaux, les modèles proposés à savoir, l'*intergovernmental*

[30] i*dem*, pp 511-513
[31] *idem*, p513
[32] BLANCO I. LOWNDES V. PRATCHETT L. (2009), *Policy networks and governance Networks : Towards a greater conceptual clarity*, in Political Studies Review, vol 11, pp 297-308 pp 297-208
[33] *idem*,p 299
[34] RHODES R.A.W. (1997), *Understanding Governance, Policy networks, Governance, Reflexivity and Acountability*, Open University Press, BUCKINGHAM pp.9-13

relations (IGR), la *power-dependance* et les *policy networks*[35] présentent néanmoins des caractéristiques similaires telles que les interactions entre les différents niveaux de pouvoirs ou encore la présence de différentes parties prenantes issues autant du secteur privé que du secteur public[36]. Rhodes identifie ensuite différents usages de la gouvernance, parmi ceux-ci un est à mettre en évidence : *the self-organizing network.*[37] Parmi les différents usages, ce dernier nous intéresse plus particulièrement car ses caractéristiques principales se rapprochent des caractéristiques du système de gouvernance traité dans ce mémoire. Ainsi, cette forme de gouvernance revêt les caractéristiques suivantes selon Rhodes : premièrement, il justifie l'utilisation du terme réseau par la présence d'un nombre important d'acteurs interdépendants.[38] Ensuite, il en donne l'objet central qui est à trouver dans la confiance et la coopération et non pas la compétition des prix comme dans les modèles classiques précédemment cités.[39] Une autre caractéristique centrale mentionnée par Rhodes est celle de l'autogouvernance. A l'instar de Rhodes, reprenons les propos de Kickert concernant ce caractère autogouverné. Ainsi pour Kickert :

> *« the control capacity of government is limited for a number of reasons ; lack of legitimacy, complexity of policy process, complexity and multitude of institutions etc. Government is only one of many actors that influence the course of events in a societal system. Government does not have enough power to exert its will on other actors. Other social institutions are, to a great extent, autonomous. They are not controlled by any single superordinated actor, not even the government. They largely control themselves. Autonomy not only implies freedom, it also implies self-responsibility. Autonomous systems have a much larger degree of freedom of self-governance. Deregulation, government withdrawal and steering at a distance […] zre all notions of less direct government direct regulation and control, which lead to more autonomy and self-governance for social institutions"*[40]

[35] *ibidem*
[36] *ibidem*
[37] *ibidem*
[38] *idem*, p51
[39] *idem*, p52
[40] Définition de Kickert reprise par RAW RHODES *in*, RAW Rhodes (1997), *op.cit.*

Dans la suite de ses travaux, Rhodes s'essaie à une définition de la gouvernance. Pour lui, ce terme est trop large, peut revêtir un trop grand nombre de signification. C'est pouruoi il utilise ce terme en précisant la reference aux réseaux[41] et la définit de la sorte :

1. *Interdependence between organizations. Governance is broader than government, covering non-state actors. Changing the boundaries of the state meant the boundaries between public, private and voluntary sectors became shifting and opaque.*
2. *Continuing interactions between networks members, caused by the need to exchange resources and negotiate shared purpose*
3. *Game-like interactions, rooted in trust and regulated by rules of the game negotiated and agreed by network participants*
4. *A significant degree of autonomy from the state. Networks are not accountable to the state; they are self-organizing. Although the state does not occupy a sovereign position, it can indirectly and imperfectly steer networks.*[42]

D'autres auteurs ont aussi tenté de définir la *network governance.* C'est le cas de Sorensen et Torfing. Notez que cette definition est formetment inspirée de celle de Rhodes. Ainsi pour eux, la *network governance* se définit en cinq points :" *1. A relatively stable horizontal articulation of interdependent, but operationally autonomous actors, 2. Who interact through negotiations, 3. Which take place within a regulative, normative, cognitive and imaginary framework, 5. That is self-regulating within limits set by external agencies and 5. Which contributes to the production of public purpose"*[43]

Pour terminer cette partie sur le réseau, nous allons nous attarder sur un concept clef qui anime ce type de gouvernance. Ce concept est celui de l'interaction. Intéressons-nous au propos de Jan Kooiman qui a fait de l'interaction l'objet central de son travail. Pour lui l'interaction fait figure de ciment entre tous les acteurs, il emploie d'ailleurs le terme d'i*nteractive governance*.[44] Kooiman définit une interaction comme une relation mutuellement influençante entre deux ou plusieurs acteurs ou entités.[45] Il opère une distinction entre deux niveaux d'interaction : le niveau intentionnel *(actor-level)* et le niveau structurel.[46] De cette division, Kooiman nous propose une définition implémentée de l'interaction. Ainsi pour lui elle peut être définie

[41] RAW Rhodes (1997), *op.cit.* p53
[42] *idem* p53
[43] TORFING J. and SORENSEN E. (2008), *Theories of democratic network governance*, Palgrave MacMilllan, Basingstoke p.9
[44] KOOIMAN J. (2003), *op.cit.*, p5
[45] *Idem* p.13
[46] I*dem* pp 13-15

comme : *« a mutually influencing relation between two or more entities. All interactions consist of an intentional and structural level. At the intentional level or action level two process are at work, those between the special interests of those participating in the interaction, and a common interest. At the structural level, entropic and negentropic forces work simultaneously. The action and the structural level mutually influence each other. The activities of governing actors co-influence the structural conditions within which they govern by changing or conserving them, while these structural conditions co-determine these governing activities by enabling or controlling them. »*[47]

Au terme de cette partie consacrée à la gouvernance en réseau il est possible de dresser un portrait général de cette dernière. Ce type de gouvernance apparait pour faire face aux limites des modèles classiques stato-centrés caractérisés par la hiérarchie. Ce modèle alternatif est composé d'une multitude d'acteurs autonomes issus du secteur public et privé et étant interdépendant en termes de ressources. Le réseau connait lui aussi certaines limites quant à son efficacité et représente également un cout pour les acteurs. La caractéristique principale de ces réseaux est le concept d'interaction. En effet, les acteurs composant ce réseau sont en perpétuelle interaction.

Cette brève présentation des principales caractéristiques est importante dans ce mémoire car elle permet d'appréhender de manière éclairer les réseaux et leurs fonctionnement et ainsi de saisir au mieux les différentes stratégies et tactiques afin de maximiser l'efficacité des réseaux qui seront présenter dans la section suivante consacrée à la méta-gouvernance.

La définition retenue dans ce mémoire sera celle de Torfing et Sorensen. En effet, cette dernière reprend les caractéristiques de la conception de Rhodes à propos de la gouvernance en réseau tout en l'actualisant. Cette actualisation donne à cette définition la qualité de s'inscrire pleinement dans l'architecture caractérisant le système de gouvernance en réseau qui sera étudié par la suite. Une caractéristique clef de cette définition ayant motivé ce choix est le fait que cette définition ne soit pas stato-centrée. En effet, Sorensen et Torfing ont une conception societo-centrée de la gouvernance en réseau. Cette orientation se retrouvera dans leur conception de la méta-gouvernance qui sera présentée dans la section suivante.

[47] *idem*, p19

1.3 La méta-gouvernance

Après avoir brièvement présenté les principales caractéristiques de la gouvernance, il est à présent temps de passer à la théorie qui constituera la base analytique de ce mémoire. La méta-gouvernance ou encore la gouvernance de la gouvernance ou encore le *network management*.[48] Dans cette partie seront présentées les différentes conceptions de la méta-gouvernance présentes dans la littérature scientifique.

Avant de poursuivre notre travail sur la méta-gouvernance il est opportun de justifier notre choix. Pourquoi avoir choisi d'analyser la régulation de la politique de cyber-sécurité européenne sous l'angle de la méta-gouvernance ? Ce choix s'est en quelque sorte imposé. Comme précédemment mentionné, la cyber-sécurité européenne et plus particulièrement de la protection des infrastructures d'information critiques, est composées d'un réseau d'acteurs à la fois privés et publics. Comme il sera fait état plus tard dans ce mémoire dans la partie consacrée à protection des infrastructures d'information critiques, aucun des acteurs ne possède les ressources nécessaires pour diriger ce réseau. Cependant, il ressort que l'Union Européenne par le biais de ses institutions et de certaines agences exerce un certain pouvoir pouvant influencer les actions des acteurs et la direction que prennent les évolutions en matière de politique de sécurité. Les théories de la méta-gouvernance nous offrent une grille de lecture pertinente afin de comprendre de quelle manière l'Union européenne exerce ce pouvoir.

Cette partie consacrée à la méta-gouvernance présentera non pas une définition de la gouvernance mais plusieurs visions de celle-ci en fonction des différents auteurs et courant de recherche dans lequel ils s'inscrivent. Donner une définition unanimement acceptée de la méta-gouvernance est impossible, tant ce terme recouvre un large champ d'action. Pour paraphraser Sorensen, la méta-gouvernance est un terme coupole[49]

Le premier auteur abordé sera Jan Kooiman, mentionné précédemment pour son triptyque d'ordre constituant la gouvernance, la méta-gouvernance est pour lui le troisième et dernier ordre. Il conçoit la méta-gouvernance comme le fait d'un méta-gouvernant imaginaire, téléporté hors du système de gouvernance et gardant celui-ci en main de manière normative[50]. Cette action se fait de manière cyclique, le méta-gouvernant influençant les actions des acteurs qui à

[48] Ces différents termes apparaissent au sein de la littérature pour désigner la méta-gouvernance
[49] SORENSEN, E. (2006) *'Metagovernance: the changing role of politicians in processes of democratic choice'*, *in*, The American Review of Public Administration, 36(1):98–114
[50] KOOIMAN J. (2003), *op.cit.*, p110

leur tour influenceront les futures actions des méta-gouvernants.[51] Un aspect important dans la conception de Kooiman est que la méta-gouvernance n'est pas l'apanage de l'Etat ou de l'acteur public en général mais comme l'activité des différents acteurs prenant part au système de gouvernance.[52]

Dans cet exercice qu'est la compréhension de la méta-gouvernance et ce dans son ensemble, deux auteurs se sont employés à recenser les différents courants théoriques présents dans la littérature. Il s'agit d'Eva Sorensen et de Jacob Torfing.[53] Les deux auteurs fournissent une approche théorique de la méta-gouvernance qu'ils divisent en quatre théories distinctes. La différence s'opère sur le mode d'exercice de la méta-gouvernance ainsi que sur l'objet sur lequel elle agit. C'est ainsi qu'ils distinguent les théories de l'*interdepedency,* de la *governmentality,* de l'*interpretation* et enfin de la *governmentality*[54]

Dans la première théorie, le but est d'accroitre l'efficacité du réseau en permettant au processus de négociation existant entre les acteurs de surpasser les obstacles et ainsi de prévenir les conflits pouvant entraver la formulation et la poursuite des buts communs.[55]

Cette forme de méta-gouvernance est effectuée de manière hands-on et l'intervention directe du méta-gouvernant peut s'effectuer via du *process management* et via la participation directe au réseau[56]

La deuxième théorie, celle de la *governability*, considère la méta-gouvernance comme essentielle, comme une condition *sine qua none* à l'efficacité du réseau. Sans cette régulation, le réseau est caractérisé par son instabilité due aux comportements individualistes des acteurs mais également dû au caractère négocié des interactions entre les acteurs.[57] Le but de cette forme de méta-gouvernance est donc de réduire cette instabilité en mettant en lumière et en accroissant les interdépendances entre les acteurs.[58] C'est de manière hands-off que s'exerce cette forme de méta-gouvernance via le design institutionnel Elle implique la construction de règles du jeu au travers duquel les acteurs agissent et en tentant d'utiliser ces règles en vue d'atteindre leurs buts et de maximiser leurs intérêts[59]

---

[51] *idem*, pp 111-112
[52] KOOIMAN J. And JENTOFT S.(2009), *Meta-governance : values, norms and principles, and the making of hard choices", in* Public administration, Vol 87, No 4 pp. 818-836 p823
[53] SORENSEN E. and TORFING J. (2008) *Theoretical approches to metagovernance in* TORFING J. and SORENSEN E. (2008), *Theories of democratic network governance*, Palgrave MacMilllan, Basingstoke (version Kindle)
[54] *idem*, emplacement 3269
[55] *idem*, emplacement 3281
[56] *ibidem*
[57] *idem*, emplacement 3322
[58] *ibidem*
[59] *ibidem*

La troisième forme de méta-gouvernance, celle de l'*integration*, quant à elle s'intéresse à l'acteur en lui-même. En effet, pour les chercheurs s'inscrivant dans ce courant de pensée, la nature de l'acteur, son identité politique et sa capacité, sont l'aspect le plus important afin d'atteindre l'efficacité maximale du réseau. La méta-gouvernance sera donc ici consacrée à la formation stratégique et au développement de ces capacités et identités.[60] Elle s'exerce ici de manière *hands-off* et ce en cherchant la formation de règles institutionnelles, de normes et de logique d'appartenance au sein du réseau[61] mais également via un *storytelling* des meilleures pratiques et ce en créant des significations communes grâce à des symboles et rituels communs[62] Ici le but est donc d'influencer la perception du contexte dans lequel les acteurs évoluent mais également la perception qu'ils ont d'eux-mêmes et des autres acteurs.[63]

Mais cette forme de méta-gouvernance ne joue pas que sur les identités, elle s'intéresse aussi aux capacités des acteurs. Ainsi afin de soutenir les acteurs, cette méta-gouvernance exercée de manières *hands-off* vise à soutenir le réseau en lui fournissant les ressources nécessaires à la bonne poursuite de son autorégulation. Et pour cela, le méta-gouvernant opère un façonnement stratégique et une transformation des droits politiques. Elle peut également être pratiquée de manière *hands-on* en supportant le développement d'un savoir-faire politique et des capacités générales d'apprentissage des acteurs avec pour but final la création d'une communauté politique forte.[64]

Finalement, la quatrième théorie présentée par Torfing et Sorensen est celle de la *governmentality*. Les auteurs définissent le terme comme : « *the institutionalized collective mentalities that define what governance is an how it is performed »*[65] Cette théorie de la méta-gouvernance (ou régulation de l'autorégulation comme l'appellent les auteurs de ce courant de pensée) tire son essence des gouvernements libéraux modernes pour lesquels gouverner c'est diriger à distance sans être impliqué directement dans la chose publique.[66] Ainsi cette méta-gouvernance consiste en la création de partenariats, d'audience, de négociations ainsi que d'une liberté d'action et de choix. Elle cherche aussi la création de règles, standards et autres indicateurs de performance et divers *modus operandi* hiérarchiques et mécanismes de contrôle.[67] Ainsi, cette méta-gouvernance vise à la mobilisation de toutes les ressources

[60] *idem*, emplacement 3381
[61] *ibidem*
[62] *idem*, emplacement 3381-3388
[63] *ibidem*
[64] *idem*, emplacement 3395
[65] *idem*, emplacement 3428
[66] *idem*, emplacement 3441
[67] *ibidem*

possibles des acteurs. Elle s'effectue de manière logiquement (selon son inspiration libérale) de manière *hands-off.*

Tableau 1.differences between the four governance network theories[68]

Approaches to metagovernance	Interdependency theory	Governability theory	Integration theory	Governmentality theory
Perspective Form Efficiency	Descriptive Hands-on Low	Prescriptive Hands-off High	Prescriptive Hands-off High	Descriptive Hands-off High

Sorensen et Torfing ne sont pas les seuls à avoir tenté de théoriser la méta-gouvernance. Ainsi McGuire et Agranoff en 2001[69] se posent sept questions principales de recherches concernant la méta-gouvernance (ou network management comme ils l'appellent). Ces questions de recherches ont pour but de comprendre les différents facteurs et processus au sein des réseaux. Dans leurs recherches sont mis en lumière 4 comportements (ou tâches) managériaux. Ils identifient ainsi quatre comportements principaux à savoir, l'activation, le f*raming*, la mobilisation et le *synthesizing*.[70] Ces quatre comportements se différencient sur leur *modus operandi* et sur l'aspect du réseau qu'ils tentent d'influencer. Ainsi l'*activation* consiste en l'identification des ressources et des acteurs adéquats à activer, à mobiliser afin d'accroitre l'efficacité du réseau. Si l'on parle d'activation, il existe également la désactivation qui peut venir soit après l'échec d'une activation préalable, soit lorsque le méta-gouvernant identifie un acteur non essentiel à l'efficacité du réseau voire un acteur entravant celle-ci.[71] Le deuxième comportement qu'ils identifient est celui du *framing*. Ce comportement vise à influencer les règles et les normes régissant le réseau ainsi qu'à modifier la perception des différents acteurs impliqués dans ce réseau.[72] Le troisième comportement qu'ils identifient est celui du *mobilizing.* Celle-ci peut se rapprocher du comportement de l'activation dans le sens où il vise à mobiliser des acteurs ou des groupes d'acteurs en vue de les faire atteindre les buts communs. Cependant on peut les différencier sur un point essentiel. La mobilisation fait du facteur humain un aspect principal. Ainsi le méta-gouvernant insistera sur des comportements tels que l'inspiration ou la motivation.[73] Finalement le dernier comportement identifié est celui du

[68] *idem* emplacement 3495
[69] AGRANOFF R. And MCGUIRE M. (2001), Big questions in public management research, *in*, Journal of public administration research and theory : J-Part, Vol 11, N°3 pp 295-326 p 297
[70] *idem*, pp 297-301
[71] *idem*, pp 297-298
[72] *idem* p 299
[73] *idem* p300

synthesizing. Si le but du méta-gouvernant est de trouver le moyen de faire parvenir le réseau à son efficacité maximum, les acteurs impliqués, eux, tendent à atteindre leurs intérêts personnels et à maximiser leurs profits. Ainsi ce quatrième comportement vise à concilier les stratégies de tous les acteurs dans le but de les amener vers l'efficacité maximale du réseau. Ce comportement vise à diminuer le cout des interactions entre les acteurs afin de les améliorer.[74]
La littérature concernant la méta-gouvernance est assez riche concernant les divers comportements que le méta-gouvernant peut adopter. La méta-gouvernance peut être vue comme une « boite à outil »[7576] à disposition des gouvernements (compris dans le sens de ceux qui gouvernent). Les paragraphes suivant présenteront brièvement deux autres typologies de méta-gouvernance. La première par Hood et Margetts et la seconde par Edelenboos et Klijn.
Les premiers cités identifient une typologie de quatre « outils » à disposition des gouvernements. La typologie *(NATO) Nodality, authority, treasure, et organizational capability*[77] Les différents outils reprennent le panel des ressources et des attributs dont disposent les gouvernements afin de réguler le réseau.[78] Comme ce fut précédemment mentionné, il existe deux courants dans la méta-gouvernance, les stato-centrés et les sociéto-centré. Cette typologie ses rapproche du courant stato-centré dans le sens où elle s'intéresse au gouvernement, à ses ressources et ses capacités ayant trait au fait qu'il soit gouvernement.[79]

La deuxième typologie précédemment mentionnée est celle de Edelenbos et Klijn. Ces derniers identifient deux manières d'effectuer la méta-gouvernance ou le *network management*[80] comme ils préfèrent l'appeler. Le *process managin / desing* et le *institutional design*[81]. La différence entre les deux se situe sur l'aspect du réseau qui vient à être régulé. Dans le premier cas on joue sur les interactions entre les acteurs en combinant quatre principes clefs que sont l'*openess,* le *safety,* le *progress* et enfin le *content.* Ces principes clefs sont combinés dans chaque stratégie que peut entreprendre le méta-gouvernant. Ces stratégies vont de l'activation d'acteurs et de ressources jusqu'à la production de confiance ou de connaissance communes en passant par le

[74] *idem* p301
[75] HOOD C. and MARGETTS H. (2007), *The Tools of Government in the Digital Age*, Palgrave MacMillan, London
[76] SORENSEN E. (2006), *'Metagovernance: the changing role of politicians in processes of democratic choice', in,* The American Review of Public Administration, 36(1):98–114
[77] HOOD C. and MARGETTS H. (2007), *Op.cit.*
[78] BAKER K. And STOKER G. (2012), *Metagovernance and nuclear power in Europe, in* Journal of European Public Policy 19 : 7 (1026-1051) p1029
[79] *ibidem*
[80]KLIJN E.-H. and EDELENBOS J. (2008), *Meta-governance as Network Management, in,* TORFING J. and SORENSEN E. (2008), *op.cit.*
[81] *ibidem*

pilotage des interactions.[82] Le design institutionnel quant à lui, s'effectue de manière indirecte, et vise à modifier les règles institutionnelles du réseau et de cette manière influencer les interactions et amener le réseau vers une efficacité optimale.[83]

La fin de cette partie sera consacrée à un auteur déjà mentionné plutôt, Eva Sorensen. Cette dernière nous offre une typologie, une « boite à outils »[84] pour utiliser ses termes. Dans cette « boite à outils » Sorensen identifie quatre moyens d'exercer la méta-gouvernance. Cette typologie vient conclure cette partie consacrée à la théorie. En effet, c'est cette dernière qui sera utilisée lors de notre analyse.

Eva Sorensen identifie quatre moyens d'exercer la méta-gouvernance, le *hands-off framing of self-governance,* le *hands-off storytelling,* le *hands-on support and facilitation* et finalement le *hands-on participation*[85]. Derrière chacune de ces pratiques se cachent différents *modus operandi*. Les prochains paragraphes seront consacrés à l'explication de chacun de ces quatre modes opératoires.

Premièrement le *Hands-off framing of the self-governance*. Ce type de méta-gouvernance est exercé via le façonnage du contexte (économique, politique, financier, …) au sein duquel le réseau évolue. Considéré comme *hands-off* en raison de la non intervention directe du méta-gouvernant, cette forme de méta-gouvernance peut s'exercer de manière forte en tentant d'influencer directement les acteurs en modifiant le design institutionnel et les règles du jeu ou de manière moins forte en définissant les objectifs généraux et le cadre budgétaire tout en laissant la liberté d'action aux acteurs.[86]

Deuxièmement, le *storytelling,* également exercé de manière *hands-off* tire son essence du constructivisme social. Il se concentre sur la construction d'identité et de contenu social et politique via un façonnage des intérêts des acteurs. Sorensen recense divers moyens de l'exercer comme par exemple la construction d'imaginaire, de contenu concernant les relations ami-ennemis, ou en produisant une certaine attente chez les acteurs via la construction d'image du futur commun. Cette forme de gouvernance est une forme assez puissante de méta-gouvernance

[82] *idem*, p203
[83] *idem*, pp 206-211
[84] SORENSEN E. (2006), *op.cit.*, p101
[85] *ibidem*
[86] i*bidem*

car elle a un fort potentiel d'influence sur les acteurs en vue de les amener vers des stratégies communes et *de facto* vers des buts communs[87]

Troisièmement, le *support and facilitation to self-governing actors*. Cette dernière se pratique de manière *hands-on* car le méta-gouvernant est en interaction directe avec les acteurs. Cette forme de méta-gouvernance ne vise pas à influencer le réseau mais, comme son nom l'indique, à supporter et promouvoir les activités entreprises par un groupe spécifique d'acteurs du réseau.[88]

Et finalement la quatrième forme décrite par Sorensen est celle de la *participation.* Pour exercer cette forme de méta-gouvernance, le méta-gouvernant doit se défaire de ses prérogatives et de sa position de supérieur hiérarchique. Il rentre et agit dans le réseau comme un acteur lambda et doit user de ses ressources pour tenter d'influencer le réseau. Cette forme est de ce fait qualifiée de *Hands-on.*[89]

Comme précédemment mentionné, cette typologie sera la base théorique de ce mémoire. Elle nous permettra de mettre en lumière les différentes pratiques de l'Union Européenne dans sa régulation du réseau d'acteurs impliqués dans la cyber-sécurité et plus particulièrement dans le domaine des infrastructures critiques. Cette typologie n'est pas le fruit d'un choix hasardeux ou arbitraire. Ce choix a été posé en fonction des caractéristiques inhérentes au réseau étudié ainsi qu'à celles du méta-gouvernant étudié, à savoir, l'Union européenne. Ainsi, comme il le sera exposé plus loin dans ce mémoire, l'Union européenne ne dispose pas de toutes les compétences requises pour réguler le réseau, notamment une des compétences capitales en matière de cyber-sécurité, la sécurité, qui est l'apanage des Etats membres[90]. La caractéristique d'internet de n'appartenir à « personne » et de ne pas tomber sous le joug du pouvoir public oblige l'Union européenne à collaborer avec la constellation d'acteurs concernés par la problématique afin d'en assurer au mieux la sécurité. [91] Une dernière raison au choix de cette typologie est à trouver dans le fait que cette typologie est celle s'inscrivant pleinement dans l'élaboration de cette recherche. En effet, les autres typologies présentées s'intéressent fortement aux ressources mobilisées, aux négociations entre les différents acteurs et rentrent avec précision dans la classification des diverses méthodes de méta-gouvernance. Or dans cette recherche il est plus question de comprendre les stratégies employées par les différentes institutions et non pas de

[87] *ibidem*
[88] *idem*, p102
[89] *ibidem*
[90] Commission européenne (2013a), p.5
[91] *idem* p3

creuser en profondeur chaque mesures en analysant ressources et interactions. Ce sont ces trois raisons, qui ont principalement orienté le choix vers la typologie de Sorensen.

1.4 Méthodologie

La typologie de Eva Sorensen sus-présentée constituera la base analytique, la grille de lecture utilisée dans ce mémoire. Les données empiriques seront issues d'une recherche documentaire et seront constituées des documents officiels produits par la Commission, le Conseil et le Parlement européen. A cela s'ajouteront les données récoltées des différents rapports produits par les agences européennes impliquées dans la cyber-sécurité ainsi que des différents documents de travail produits par les institutions.

Une récolte de donnée via entretien fut envisagée, mais le sujet ayant trait à la sécurité des infrastructures critiques et débordant également dans le domaine de la défense, aucune demande d'entretien, formelle ou non, n'a trouvé issue favorable. C'est pourquoi le choix a été fait de se concentrer sur une recherche documentaire minutieuse.

La recherche sera articulée autour de trois hypothèses, à savoir : 1) L'Union européenne (sous-entendu ici la Commission, le Parlement européen et le Conseil) assure, seule, la régulation du réseau d'acteurs impliqués dans la protection des infrastructures d'information critiques ; 2) Chaque Institution exerce une fonction propre en tant que méta-gouvernant du réseau d'acteurs impliqués dans la protection des infrastructures d'information critiques ; 3) L'Union européenne (sous-entendu ici, les Institutions (Conseil, Parlement et Commission ainsi que l'Agence en charge de la sécurité des réseaux et de l'information – ENISA) exerce son rôle de méta-gouvernant de manière hands-on, en interaction directe avec les acteurs impliqués dans la protection des infrastructures d'information critiques.

L'analyse sera menée de la sorte : De la recherche documentaire seront mis en lumières les différentes actions, stratégies, tactiques, mesures mises en place par l'Union Européenne. Afin de répondre à la première hypothèse, un recensement des différents acteurs impliqués dans l'élaboration et la mise en place de la méta-gouvernance sera effectuée.

Dans un second temps, les différentes mesures seront classées en fonction de leurs types, et de leurs cibles, et ce, selon la typologie de Sorensen. Le propos n'est pas ici d'analyser les mesures une par une mais de regrouper les différentes mesures en fonction des quatre classes et de les mettre en parallèle avec les auteurs de ces mesures afin de répondre à la deuxième hypothèse concernant le rôle des institutions.

Finalement, un focus sera effectué sur les pratiques *hands-on* des méta-gouvernant afin de répondre à la troisième hypothèse.
Les éléments analysés le seront sur une période allant de l'année 2005 jusqu'à l'année 2013.
Finalement, la réponse à la question centrale de ce mémoire, à savoir, « Comment l'Union européenne régule-t-elle le réseau d'acteurs impliqués dans la mise en œuvre des politiques de protection des infrastructures d'information critiques ? », pourra être donnée en fonction des acteurs visés par les mesures de l'UE, des types de stratégies employée officiellement afin de réguler ce réseau et en fonction des rôles joués par chacune des institutions. Dans les limites imposées à ce mémoire, il était impossible de s'intéresser à l'ensemble de la sécurité européenne ou encore à chaque mesure en particulier. Le propos ici est d'avoir un aperçu global de cette régulation.

En conclusion de ce chapitre consacré au cadre théorique de ce mémoire, un rappel des principaux éléments sera effectué. Ainsi, la théorie de la gouvernance s'inscrit dans une volonté de palier aux lacunes des théories classiques concernant la compréhension des processus de décisions prenant place dans nos sociétés modernes caractérisées par une complexification de la chose publique et par la multiplication des acteurs impliqués dans sa gestion.
Parmi les différentes théories concernant la gouvernance qu'offre la littérature scientifique, celle consacrée à la gouvernance en réseau ressort comme la plus adaptée dans le cadre de ce mémoire. En effet, cette *network governance* est caractérisées par une multitude d'acteurs issus du secteur public et privé, agissant de manière autonome, mais étant interdépendants en termes de ressource. Cette autonomie des acteurs induit que ces derniers agissent en fonction de leurs propres intérêts, et ce, parfois au détriment de l'intérêt commun. Afin de réguler ce réseau d'acteurs et d'amener les individualités à agir dans un sens commun et de la sorte améliorer l'efficacité du réseau, un acteur ressort et s'érige en tant que méta-gouvernant.
Les théories de la méta-gouvernance s'intéressent donc aux acteurs et à leurs actions visant à réguler le réseau sans pour autant nuire à l'autonomie d'action des acteurs. Ainsi la méta-gouvernance peut être considérée comme la régulation d'un réseau caractérisé par l'autorégulation. C'est ce cadre théorique, et en particulier la typologie des modes opératoires de la méta-gouvernance données par Sorensen, qui servira de grille de lecture dans ce mémoire. Cette typologie identifie quatre modes d'exercice de la méta-gouvernance. Deux le sont de manière *hands-off ,* le *framing* et le *storytelling.* Les deux autres l'étant de manière *hands-on,* le *support and facilitation* et la participation.

Le cadre théorique et la méthodologie de ce mémoire étant présentés, le prochain chapitre présentera les principaux éléments concernant la régulation de la gouvernance de la protection des infrastructures d'information critiques. Ces éléments serviront de matériaux à analyser dans le troisième chapitre de ce mémoire.

Chapitre 2 : La Protection des Infrastructures d'information critiques (PIIC)

Après avoir présenté les théories de la méta-gouvernance et avoir présenté le cadre théorique qui sera utilisé lors de l'analyse, ce nouveau chapitre exposera le matériau empirique à analyser. La première partie de ce chapitre s'intéressera aux prémices de la cyber-sécurité européenne début des années 80. Cette brève introduction trouve son utilité dans le fait qu'elle présente le premier cadre institutionnel au sein duquel évolueront les acteurs impliqués dans la protection des infrastructures d'information critiques. La deuxième partie de ce chapitre s'intéressera à la protection des infrastructures critiques et plus particulièrement aux actions des institutions européennes et de l'ENISA en leur qualité de méta-gouvernant. Il a été choisi, dans un souci de respect des consignes de longueur du mémoire et dans un souci de faisabilité de la recherche, de se concentrer sur cinq moments/actions majeurs : 1) le programme européen de protection des infrastructures critiques ; 2) le Plan de protection des infrastructures d'information critiques ; 3) La stratégie européenne de cyber-sécurité de 2013 ; 4) l'ENISA, cette partie sera divisée en deux. Premièrement la gestion de l'ENISA par l'UE et deuxièmement, les actions de l'ENISA en tant que méta-gouvernant ; et finalement 5) la dernière division comportera diverses actions des institutions européennes ne rentrant pas dans un plan d'action propre à la protection des infrastructures critiques mais comportant un intérêt certain concernant la méta-gouvernance de cette dernière.

2.1 La genèse de la cyber-sécurité

Bien que la cybercriminalité soit un phénomène relativement récent, apparaissant avec l'Internet et évoluant en fonction de l'évolution des nouvelles technologies, et s'accélérant de nos jours avec des attaques de plus en plus nombreuses et lourdes de conséquences[92]. Bien que la lutte face à cette forme de criminalité paraisse récente et s'intensifie depuis une dizaine d'année, celle-ci faisait déjà partie des préoccupations de nos dirigeants depuis les années 80. Ces derniers ayant cerné le caractère sans frontières de ce problème et du potentiel danger représenté par le flux de donnée circulant via ce réseau. Ainsi en 1981 fut établie une première convention internationale intitulée « Convention pour la protection des personnes à l'égard du

[92] Commission européenne (2013a), *op.cit.*, pp 2-3

traitement automatisé des données à caractère personnel »[93] .Cette convention est établie par le Conseil de l'Europe, à Strasbourg, le 28 janvier 1981.

Seize ans plus tard, ce sont les membres du G8 réunis à Birmingham qui consacrent un point à la cyber-sécurité dans leur « déclaration sur les drogues et la criminalité »[94] en 1997. Cependant, il faut attendre 2001 et la « Convention sur la cybercriminalité » dite « Convention de Budapest »[95] du Conseil de l'Europe pour avoir un vrai instrument international contraignant concernant la lutte contre la cybercriminalité et la protection des utilisateurs et des réseaux. Enfin, en 2002 le Conseil et le Parlement européen adoptent une directive-cadre concernant un cadre réglementaire commun en matière de réseau et de service de communications électroniques[96]

2.2 La protection des infrastructures d'information critiques (PIIC)

Dans cette section sera présenté le matériau empirique qui fera l'objet d'une analyse dans le prochain chapitre. Seront présentés ici les actions de l'UE en vue de réguler le réseau d'acteurs impliqués dans la PIIC. Comme déjà mentionné, ce matériau empirique est issu des documents officiels de l'Union européenne et donc les éléments analysés seront des mesures et actions officielles. Des éléments concernant des actes non-officiels, informels, comme il est possible de retrouver dans les interactions entre acteurs n'ont pu être obtenus en raison de la sensibilité du sujet traité. Dans cette section les faits exposés seront divisés en cinq parties. La première concernant le programme européen de protection des infrastructures critiques (EPCIP), la deuxième, le plan de protection des infrastructures d'information critiques, la troisième, le stratégie européenne de cyber-sécurité de 2013, la quatrième étant consacrée à l'Agence européenne chargée de la sécurité des réseaux et de l'information, et finalement, la cinquième partie sera consacrées à des actions et mesures prises isolément car n'entrant pas dans une des sections précédentes mais relevant quand même d'un intérêt pour notre analyse. Les éléments présentés dans la suite de ce chapitre se déroulent dans une fenêtre de temps allant de 2005 à

[93] Conseil de l'Europe (1981), Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, STE n°108, Strasbourg

[94] Centre de documentation sommet G7-G8 (1998), Déclaration sur les drogues et la criminalité du 16 mai 1998, Document en ligne, URL : http://g7.sciencespo-lyon.fr/spip.php?article71

[95] Conseil de l'Europe (2001), Convention sur la cybercriminalité, STE n°185, Budapest

[96] Journal officiel des Communautés européennes (2002), directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive « cadre »), Bruxelles

2013. D'autres mesures furent prises avant et après cette date mais ne seront pas prises en compte pour notre analyse, comme cela a été précisé dans un chapitre antérieur.
Préalablement à la présentation de ces cinq parties, une section consacrée à la définition des infrastructures critiques et d'informations critiques sera présentée dans un soucis de compréhension des éléments qui seront ultérieurement exposés.

2.2.1 Infrastructures (d'information) critiques - définition

Cette partie sera consacrée à la définition de certaines notions qui seront rencontrées dans les prochaines sections. Ainsi seront définis ici les concepts d'Infrastructure critiques européennes / nationale, infrastructures d'information critiques.

Ainsi, une infrastructure critique peut être définie comme :*« un point, système, ou partie de celui-ci, située dans les Etats membres, qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, et dont l'arrêt ou la destruction aurait un impact significatif dans un Etat membre du fait de la défaillance de ces fonctions »*[97]
Une infrastructure critique européenne (ICE) est : *« une infrastructure critique située dans les Etats membres dont l'arrêt ou la destruction aurait un impact considérable sur deux Etats membres au moins. L'importance de cet impact est évaluée en termes de critères intersectoriels. Cela inclut les effets résultant des dépendances intersectorielles par rapport à d'autres types d'infrastructures. »*[98]
Une infrastructure d'information critique est une infrastructure dans le domaine des technologies de l'information et de la communication (TIC), offrant des biens et services d'importance capitale, ou servant de base à d'autres infrastructures critiques et dont la perturbation ou l'arrêt aurait de graves incidences sur les fonctions vitales de la société.[99]

[97] Journal officiel de l'Union européenne (2008a), Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection, Bruxelles, p.77
[98] *ibidem*
[99] Commission des Communautés européennes (2009), Communication de la Commission au Parlement européen, au Conseil, au comité économique et social européen et au comité des régions relative à la protection des infrastructures d'information critiques : « protéger l'Europe des cyberattaques et des perturbations de grande envergure : améliorer l'Etat de préparation, la sécurité et la résilience », COM(2009)149 final, Bruxelles p.2

Après avoir défini ces concepts, qui seront récurrents dans les prochaines sections de ce mémoire, le matériau empirique de cette recherche peut être exposé.

2.2.2 L'EPCIP

Le premier élément présenté est le Programme européen de Protection des Infrastructures critiques. Ce programme trouve son origine en 2005 avec l'adoption par la Commission d'un livret vert[100] Ce document n'est pas ciblé en particulier sur les infrastructures d'information critiques. Cependant, il inclut ces dernières dans la définition et dans le recensement qu'il effectue des infrastructures critiques. C'est pourquoi il a été jugé pertinent de prendre ce document en compte dans les éléments à analyser dans ce mémoire. Outre ce document, le programme de protection dans son entièreté est orienté vers les infrastructures critique en général et non pas sur celle de l'information en particulier. Cependant, à l'instar de la justification faite pour le livret vert, l'EPCIP s'avère pertinent dans notre objet d'étude car il inclut les infrastructures d'information critiques et que ce dernier est un premier pas vers le plan d'action ciblé sur la protection des infrastructures d'information critiques qui sera exposé dans la section suivante de ce chapitre. Cette précision effectuée, la présentation du livret vert et du plan qui en découle peut être effectuée.

Ainsi, dans le livret vert, la Commission présente différents scénarios, en réponse à la demande du Conseil, visant à mettre en place l'EPCIP et le CIWIN. Ce document marque la deuxième phase d'un processus de consultation sur l'établissement d'un programme européen de protection des infrastructures critiques. Les différentes options présentées aux acteurs impliqués dans la protection des infrastructures critiques sont les objectifs généraux du futur programme, les types de risques auxquels il devra faire face, quels types d'infrastructures doivent être considérées comme critiques, européennes ou nationales ainsi que les responsabilités et les rôles à jouer par les autorités publiques et le secteur privé.[101] La Commission espère par ce document, obtenir des contributions et une participations concrètes des parties intéressées sur les options décrivant les différents aspects d'un futur programme de

[100] Commission des Communautés européennes (2005), Livret vert sur un programme européen de protection des infrastructures critiques, COM(2005) 576 final, Bruxelles
[101] *idem*, pp 3-19

protection. En fonction des résultats de ce processus de consultation, la Commission pourrait présenter en 2006 un ensemble de mesures sur l'EPCIP.[102]

Ainsi, comme le prévoyait la Commission dans son livret vert, cette dernière adopte en 2006 une communication concernant un programme de protection des infrastructures critiques.[103]

Cette communication *« expose les principes, les procédures et les instruments proposés pour mettre en œuvre l'EPCIP(...) »*[104]et présente un cadre communautaire pour la protection des infrastructures critiques (IC)[105]. Ce programme sera basé sur six principes clefs : La subsidiarité, la complémentarité, la confidentialité, la coopération des acteurs concernés, la proportionnalité et l'approche sectorielle.[106] Le plan présenté est un plan en trois volets. Le premier volet « Stratégie consécutives de l'EPCIP », sera une plateforme stratégique facilitant la coordination et la coopération des acteurs.[107] Le second volet « Protection des infrastructures critiques européennes (ICE), visera à réduire la vulnérabilité de ces ICE.[108] Le troisième et dernier volet « Soutien relatif aux ICN », est d'ordre national et visera à aider les Etats membres dans la protection de leurs infrastructures nationales.[109]

Dans cette communication, la Commission prévoit aussi la création d'un réseau d'alerte concernant les infrastructures critiques, le CIWIN.[110] En 2008, la Commission adopte une proposition de décision du conseil concernant ce réseau d'alerte[111]. Cependant, après plusieurs années de procédures la proposition est retirée en 2012 car elle ne revêt plus un caractère d'actualité.[112]

Les principales mesures présentées par la Commission concernant la mise en œuvre de l'EPCIP furent adoptées par le Conseil dans sa résolution relative à une société de l'information sûre en Europe[113]

[102] Commission des communautés européennes (2005), *op.cit.*
[103] Commission des Communautés européennes (2006a), Communication de la Commission sur un programme européen de protection des infrastructures critiques, COM(2006)786 final
[104] *idem,* p2
[105] *ibidem*
[106] *idem,* p3
[107] *idem,* p10
[108] *idem,* p11
[109] *idem,* p12
[110] *idem,* p5
[111] Commission des communautés européennes (2008), proposition de décision du Conseil relative au réseau d'alerte concernant les infrastructures critiques (CIWIN), COM(2008) 676 final, Bruxelles
[112] Journal officiel de l'Union européenne (2012), retrait de propositions de la Commission qui ne revêtent plus d'un caractère d'actualité, (2012/C J56/06)
[113] Journal officiel de l'Union européenne (2007a), Résolution du conseil du 22 mars 2007 relative à une stratégie pour une société de l'information sûre en Europe, 2007/C 68/01

La dernière mesure prise en compte dans cette section consacrée à l'EPCIP est une directive adoptée par le Conseil en 2008 et relative à la reconnaissance des infrastructures critiques.[114] Cette directive, *« constitue la première étape d'une approche progressive visant à recenser et désigner les ICE, ainsi qu'à évaluer la nécessité d'améliorer leur protection(…) »*[115] cette directive a pour objet, comme le stipule son article premier, la création d'une procédure de recensement et de désignation des infrastructures européennes, ainsi qu'une approche commune pour évaluer la nécessité d'améliorer leur protection et ce dans le but final de contribuer à la protection des personnes[116] Cette directive se concentre sur les infrastructures dans le secteur de l'énergie et du transport. Cependant, elle reste pertinente dans ce mémoire car elle offre une méthode de recensement des infrastructures critiques pouvant être étendue à d'autres secteurs comme celui de l'information et des réseaux lors de sa prochaine révision comme en fait état son acrticle 3 alinéa 3[117] Cette directive adopte également une série de mesures concernant le recensement adoptées par la Commission dans sa communication de 2006 sur un plan de protection des infrastructures critiques européennes.[118] Finalement la directive institue aussi la création d'un plan de sécurité des opérateurs (PSO)[119]
Comme mentionné à plusieurs reprise, cette section se consacre aux infrastructures critiques en général, la prochaine section s'intéressera au des mesures prises dans le cadre de la protection des infrastructures d'information critiques en particulier.

2.2.3 Plan de protection des infrastructures d'information critiques (PIIC)

Cette section présentera les actions et mesures prises par les Institutions européennes concernant le plan d'action protection des infrastructures d'information critiques. Ce plan est présenté pour la première fois par la Commission dans une communication qu'elle adopte en 2009[120]

[114] Journal officiel de l'Union Européenne (2008), Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection.
[115] *Idem* p75
[116] *idem* p77
[117] *idem* p78
[118] Commission de communautés européennes (2006a), *op.cit.*
[119] Journal officiel de l'Union européenne (2008), *op.cit*, pp 81-82
[120] Commission des Communautés européennes (2009), Communication de la Commission au Parlement européen, au Conseil, au comité économique et social européen et au comité des régions relative à la protection des infrastructures d'information critiques : « protéger l'Europe des cyberattaques et des perturbations de grande envergure : améliorer l'Etat de préparation, la sécurité et la résilience », COM(2009)149 final, Bruxelles

Cette communication établit un programme d'action articulé autour de cinq axes et visant à assurer un niveau de sécurité des infrastructures d'information critiques optimal.[121]
Ces cinq axes sont[122] : Préparation et prévention : garantir un état de préparation à tous les niveaux ; Détection et réaction : fournir des mécanismes d'alerte rapide adéquats ;
Atténuation et récupération : renforcer les mécanismes de défense des infrastructures d'information critiques dans l'UE ; Coopération internationale : promouvoir les priorités de l'UE sur le plan international ; Critères pour le secteur des TIC : soutenir la mise en œuvre de la directive concernant le recensement et la désignation des infrastructures d'information critiques

Afin de maximiser la sécurité de ces infrastructures d'information critiques, il est important que tous les acteurs aillent dans la même direction. A l'heure de cette communication, le constat était posé qu'à la fois les acteurs privés que les acteurs publics ne s'impliquaient pas de la même manière dans la sécurisation des infrastructures et ce, malgré des précédentes directives et stratégies mise en place.[123]
Ainsi, il a été constaté au sein des Etats membre des différences en termes d'approche de cette sécurité mais également en termes de préparation et de compétence. Or, dû à l'interconnexion des infrastructures, un Etat membre défaillant peut rendre vulnérable l'ensemble du réseau. C'est pourquoi, par le biais notamment de cette communication, la Communication veut amener une prise de conscience et amener une certaine harmonie au sein de l'UE en termes de sécurité de ces infrastructures d'information critiques.[124]
L'UE reconnait également que ces nouveau enjeux et nouveaux objectifs amènent dans leur sillage un besoin de nouvelles structures de gouvernance, ainsi tout en rappelant qu'*in fine* c'est aux Etats membres que revient la responsabilité d'établir les politique des sécurité au niveau national, cette sécurité dépend fortement du secteur privé, principal détenteur des infrastructures d'information critique et qui influe également sur la demande et l'offre de solution de sécurité à destination de ces infrastructures. C'est pourquoi il est important que des partenariats entre le public et le privé s'établissent au niveau national mais surtout au niveau européen en raison, notamment, des raisons d'interconnexion précédemment citées.[125]

[121] *idem* p2
[122] *ibidem*
[123] *idem* pp3-6
[124] *idem* p6
[125] *ibidem*

Une condition essentielle au bon fonctionnement à la fois de cette stratégie mais également de cette gouvernance de la sécurité des infrastructures d'information critiques est la disponibilité des informations pour tous les acteurs.[126]
Ainsi pour chaque axe, la Commission propose une série d'objectif à atteindre et une série de mesures à prendre par les acteurs impliqués dans la PIIC afin de rejoindre ces objectifs. Les mesures seront présentées ici de manière générale, la liste complète des mesures est à trouver en annexe (Annexe 1).

Concernant la préparation et la prévention, la Commission enjoint les acteurs compétents à définir un niveau de capacités et de service minimum pour les équipes d'intervention d'urgence (CERT) ; encouragera la coopération entre les secteurs publics et privé, et notamment en termes de bonnes pratiques ou sur les exigences minimales de sécurité ; la Commission entend créer un forum européen des Etats membres qui servira d'arène de partage d'information et de débat.[127]

Concernant la détection et la prévention, la Commission entend soutenir la création d'un système européen de partage d'information et soutien déjà, dans le cadre du projet européen « prévention, préparation et gestion des conséquences en matière de terrorisme et autres risques liés à la sécurité » [128], deux projet prototypes.[129]
En matière d'atténuation et de récupération, la Commission demande aux Etats membres d'établir des plans nationaux de réaction en cas d'urgence ainsi que l'élaboration d'exercices de préparation, elle encourage également la tenue d'exercices paneuropéens de réactions aux incidents. Elle met également en lumière le besoin de coopération et les interdépendances existant et demande aux Etats membres une coopération accrue de leur CERTs[130]
Le quatrième axe concerne la coopération internationale, cette dernière, ne rentrant pas en compte dans notre analyse, ne sera pas présentée dans cette partie.

[126] *idem* p7
[127] *idem*, pp 9-10
[128] Journal officiel de l'Union européenne (2007b), Décision du Conseil du 12 février 2007 établissant pour la période 2007-2013, dans le cadre du programme général « sécurité et protection des libertés » le programme spécifique « prévention, préparation et gestion des conséquences en matière de terrorisme et autres risques liés à la sécurité », Bruxelles
[129] Commission des Communautés européennes, *op.cit.*, p10
[130] *idem*, *p*p 10-11

Finalement en matière de critères pour les IICE la Commission demande aux Etats membres, avec son soutien, d'élaborer des critères de reconnaissances communs de ces infrastructures d'information critiques.[131]

Suite à ce plan adopté par la Commission, le Conseil adopte une résolution en 2009 relative à une approche européenne concertée en matière de sécurité des réseaux et de l'information.[132] Cette dernière consacre une série de mesures adoptées par la Commission dans son plan d'action visant à la mise en œuvre de ce dernier. Dans cette résolution, le Conseil reconnait l'importance que revêtent les IIC pour la société et les évolutions technologique toujours plus nombreuses et plus rapides pouvant poser problème pour la sécurité.[133] Le Conseil admet également les lacunes en matière de coopération notamment entre les différents acteurs, ces dernières entravant la possibilité d'atteindre un niveau de sécurité élevé[134]. Finalement, en raison des éléments précédemment cités, elle adopte une série de mesures et de recommandations en direction de la Commission, des Etats membres, de l'ENISA, et des autres acteurs impliqués, notamment ceux du secteur privé.[135]. Les mesures consacrées dans cette résolution sont à trouver en annexe (ANNEXE 2).

En 2011, la Commission adopte de nouveau une communication concernant le plan d'action de protection des infrastructures d'information critiques.[136] Ce document vise deux objectifs. Premièrement, la Commission y dresse une liste des mesures déjà prises et des différentes avancées dans la mise en œuvre du plan d'action adopté en 2009[137]. Deuxièmement, elle y fait une série de recommandations et dresse une liste de mesures à prendre afin de poursuivre la mise en œuvre de ce plan et ce, de manière efficace, afin d'atteindre un niveau élevé de protection des IIC.[138]

Ainsi on y apprend que dans les différents axes constituant le plan d'action, le Forum européen des Etats membres a été mis en place et rencontre un certain succès en terme de résultat mais

[131] *idem*, p12
[132] Journal officiel de l'Union européenne (2009), Résolution du Conseil du 18 décembre 2009 sur une approche européenne concerté en matière de sécurité des réseaux et de l'information, 2009/C 321/01
[133] *idem*, pp 1-2
[134] *idem*, pp 2-3
[135] *dem*, pp 3-4
[136] Commission européenne (2011), communication de la commission au parlement européen, au conseil, au comité économique et social européen et au conseil des régions relative à la protection des infrastructures d'information critiques "réalisation et prochaines étapes : vers une cybersécurité mondiale", COM(2011) 163 final, Bruxelles
[137] *idem*, pp 5-7, 11-18
[138] *idem*, pp 7-18

également en terme d'approbation par les Etats-membres[139]. On y apprend également que parmi les mesures concernant la mise en place de méthodologie de reconnaissance des IIC, l'élaboration de critères minimum de sécurité, la préparation d'exercices nationaux et paneuropéens, la réalisation de plan nationaux d'urgences, les Etats membres, soutenu par l'ENISA ont effectué des progrès significatifs[140] Les éléments concernant l'ENISA seront développés ultérieurement dans une partie dévolue exclusivement à cette agence.
Concernant la poursuite de la mise en œuvre de ce plan, la Commission, s'appuyant sur des résultats encourageants entend poursuivre ses efforts et demande à l'ENISA, aux Etats membres ainsi qu'au secteur public de poursuivre également leurs différentes entreprises et de renforcer encore la coopération entre tous les acteurs.[141]

Cette section constitue, avec la section ultérieure consacrée à l'ENISA, les principales mesures prises et actions entreprises par les institutions européennes concernant la protection des infrastructures d'information critiques et en particulier les actions de l'UE en vue de réguler le réseau et tenter d'amener celui-ci vers une efficacité maximale.

2.2.4 Stratégie européenne de cyber-sécurité de 2013

En 2013, la Commission européenne a publié une communication destinée à établir une stratégie européenne de cyber-sécurité.[142] Préalablement à la présentation de cette stratégie, il est important de justifier la sélection de cette dernière dans le matériau empirique de ce mémoire. En effet, si cette stratégie ne cible pas précisément la protection des infrastructures d'information critiques, elle propose des modifications et des évolutions en termes de gouvernance. Ainsi le contexte général, et les « règles » régissant les relations entre les différents acteurs se voient modifiées et ce, toujours dans un but d'accroitre l'efficacité de la sécurité. Le cadre et le contexte générale de la cyber-sécurité européenne étant modifié, cela impacte *de facto* l'environnement au sein duquel évoluent les acteurs impliqués dans la protection des infrastructures d'information critiques.

[139] *idem*, p13
[140] *idem*, pp 7-18
[141] *ibidem*
[142] Commission européenne (2013a), Communication conjointe au parlement européen, au Conseil, au comité économique et social européen et au comité des régions, Stratégie de cyber-sécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé, JOIN(2013) Final

Dans ce document, la Commission précise certains principes de cyber-sécurité que doivent respecter les acteurs. Ainsi, ces derniers sont tenus de respecter les valeurs essentielles de l'UE même dans le cyberspace. En ce compris la protection des droits fondamentaux, de la liberté d'expression, la protection des données personnelles ainsi que la protection de la vie privée.[143]
La commission insiste aussi sur le fait que toutes les parties prenantes à la sécurité du cyberespace et des TIC (secteur public et privé) doivent s'intégrer dans un modèle de gouvernance, participatif, démocratique et efficace mais également endosser les responsabilités qui leur incombent en tant qu'acteur de ce réseau[144]
La stratégie proposée par la Commission s'articule autour de cinq axes prioritaires :
Parvenir à la cyber-résilience ; Faire reculer considérablement la cybercriminalité ; Développer une politique et des moyens de cyberdéfense liée à la politique de sécurité et de défense commune (PSDC) ; Développer les ressources industrielles et technologiques en matière de cyber-sécurité ; Instaurer une politique internationale de l'UE cohérente en matière de cyberespace et promouvoir les valeurs essentielles de l'UE[145]

La Commission précise que par cette stratégie, l'UE n'entend pas outrepasser ses droits et prendre la place des Etats membres, c'est toujours à ces derniers qu'il incombe de s'occuper des problèmes de sécurité dans le cyberespace.[146]
Les prochaines lignes seront consacrées à la présentation des différentes recommandations et mesures à entreprendre présentées dans cette stratégie. La présentation, à l'instar de la présentation des précédents programmes et plan d'action, se fera de manière générale.

Premier axe : parvenir à la cyber-résilience
La commission présente une série de mesure à destination des acteurs impliqués, ainsi la Commission invite le Parlement européen et le Conseil à adopter rapidement la proposition de directive sur un niveau élevé de sécurité commun des réseaux et de l'information dans l'Union[147]

[143] *idem* p4
[144] *ibidem*
[145] *idem* p5
[146] *ibidem*
[147] *idem* p8

L'ENISA est invitée à continuer à aider les Etats membres ainsi que les institutions européennes dans le développement de moyen de cyber-résilience via l'acquisition de compétences en la matière ainsi qu'à l'élaboration d'exercices paneuropéens de simulation de cyber-incidents.[148]
La Commission s'adresse également aux entreprises en les invitant à investir dans un niveau élevé de sécurité, à élaborer des bonnes pratiques en la matière et à développer le partage d'information avec les pouvoirs publics[149]

Deuxième axe : faire reculer considérablement la cybercriminalité

Afin de parvenir à cet objectif, la Commission insiste sur le fait qu'il faut une législation solide et efficace et à cette fin, la Commission entend enjoindre les Etats membres à ratifier la convention de Budapest. [150]
La Commission identifie également un autre moyen d'atteindre ce but, à savoir, disposer de moyens opérationnels accrus pour combattre cette cybercriminalité.[151]
La Commission entend dans ce sens soutenir financièrement via différents programmes (ex : En 2013 le programme « prévenir et combattre la criminalité » ou après 2013 le « Fonds pour la sécurité intérieure »[152]), les Etats membres afin de recenser leurs faiblesses et de les améliorer mais également les organes servant de lien entre le monde académique et entrepreneurial[153] Elle entend également collaborer avec EC3, le Centre européen de lutte contre la cybercriminalité et avec Eurojust afin d'aligner les approches politiques[154]

La Commission insiste également sur le fait qu'il est nécessaire d'avoir une meilleure coordination au niveau européen entre les secteurs de la justice, les acteurs publics et privés[155]
A ce titre, la Commission s'engage à soutenir différents organismes dans leurs taches de facilitation et de support des acteurs du réseau comme l'EC3 ou des bureaux d'enregistrement des noms de domaine[156]

[148] *ibidem*
[149] *ibidem*
[150] *idem p10*
[151] *ibidem*
[152] *ibidem*
[153] *ibidem*
[154] *ibidem*
[155] *idem* pp 10-11
[156] *idem* p11

Elle donne également une série de direction et d'objectif à atteindre pour les organismes judiciaires comme l'EC3, le CEPOL et Eurojust. Elle les encourage à collaborer étroitement et à fournir des données relatives aux menaces et aux moyens opérationnels pour y faire face[157]

Troisième axe : Développer une politique et des moyens de cyberdéfense s'inscrivant dans le cadre de la politique de sécurité et de défense commune (PSDC)

Dans cette stratégie, la Commission met l'accent sur le fait que la sécurité du cyberespace revêt également un aspect défense. En effet, afin de faire face à tous les types de menaces et en particulier celle pesant sur les infrastructures critiques menaçant l'intégrité des Etats, il est important de développer des synergies entre les approches civiles et militaires[158]

A ce titre, l'UE par le biais de la Commission et plus particulièrement de l'ENISA s'engage à poursuivre une série d'objectif comme la définition d'exigences de cyberdéfense opérationnelle au niveau européen ainsi que la promotion du développement technologique en la matière, l'élaboration d'un cadre politique européen en matière de cyberdéfense, la promotion du dialogue et de la coordination entre tous les acteurs impliqués.[159]

Quatrième axe : Développer les ressources industrielles et technologiques en matière de cyber-sécurité

La Commission dresse le constat que malgré un haut niveau dans la recherche et le développement, les solutions sécurités en matière de TIC ainsi que les produits TIC sont majoritairement produits à l'étranger et l'UE risque de devenir dépendant de pays tiers[160]

Afin de ne pas devenir dépendant de tiers, la Commission s'engage dans cette stratégie à mettre en place une plateforme public-privé en matière de sécurité des réseaux de l'information (SRI) et d'utiliser les travaux de cette dernière en vue de proposer dans un laps de temps d'un an une série de recommandations afin d'assurer la sécurité le long de la chaine de valeur. Elle propose également de recenser les différentes pratiques que pourraient utiliser les fournisseurs de TIC afin d'informer les autorités sur les faiblesses des produits[161]

Toujours dans un but de l'élaboration de normes de sécurité optimales, la Commission invite l'ENISA à collaborer avec tous les secteurs et les organismes impliqué de produire une série de

[157] *idem* pp 11-12
[158] *idem* p.12
[159] *ibidem*
[160] *idem* p13
[161] *idem* p14

recommandations concernant l'adoption de normes et de bonnes pratiques en matière de SRI autant dans le public que dans le privé.[162]

La Commission invite finalement le secteur public mais surtout les entreprises à élaborer, de leur propre initiative, des normes de sécurité solides, ainsi que des normes de performance et labels afin d'informer le « consommateur » du niveau de sécurité des produits.[163]

Toujours dans cette volonté d'amener les moyens européens à un niveau optimal, la Commission entend dans cette stratégie inviter tous les acteurs, que ce soit du monde académique, du secteur public ou privé, à collaborer et à développer des bonnes pratiques en matière de développement de la sécurité informatique au sein du marché, de recenser les besoins du marché ainsi que des incitants avec le monde de l'assurance par exemple afin d'encourager la sécurisation optimale de tous les produits et services TIC[164]

Le cinquième et dernier axe ayant trait à l'aspect international, il ne fera pas l'objet d'une présentation dans ce mémoire.

Cette stratégie est accompagnée d'une proposition de directive[165] reprenant une série de mesures présentées dans la communication et ayant pour but d'institutionnaliser celles-ci et d'enjoindre les Etats membres à les adopter au sein de leurs cadres législatifs nationaux respectifs. Ainsi elle entend s'ériger en cadre légal européen au sein du quel pourra s'inscrire une réelle coopération et une réelle coordination entre les différents acteurs.[166] Concernant plus particulièrement la cyber-sécurité des infrastructures critiques, il est fait état, au moment de la proposition de cette directive en 2013, que les acteurs responsables de ces infrastructures et des services essentiels, hormis les entreprises de télécommunication, ne sont pas tenu à des obligations de sécurité et de mesures concernant la gestion des risques en rapport avec l'importance qu'ils revêtent pour la société.[167]

La présente section présentera les mesures prises dans cette directive et plus particulièrement celles visant à réguler le réseau d'acteur.

---

[162] *ibidem*
[163] *ibidem*
[164] *idem* p15
[165] Commission européenne (2013b), 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)48 final, Bruxelles
[166] *idem* p3
[167] *ibidem*

Dans son premier article, la directive précise son objet et son but. Ainsi le premier article déclare :

« 1. La présente directive établit des mesures visant à assurer un niveau commun élevé de sécurité des réseaux et de l'information (SRI) dans l'Union.

2. À cette fin:

(a) elle fixe des obligations à tous les États membres en ce qui concerne la prévention et la gestion de risques et incidents touchant les réseaux et systèmes informatiques ainsi que les interventions en cas d'événement de ce type;

(b) elle crée un mécanisme de coopération entre les États membres, destiné à garantir une application uniforme de la présente directive dans l'Union et, le cas échéant, un traitement et une intervention coordonnés et efficaces en cas de risques et d'incidents touchant les réseaux et systèmes informatiques ;

(c) elle établit des exigences en matière de sécurité pour les acteurs du marché et les administrations publiques. (…) »[168]

Il est important de préciser que cette directive, comme le stipule son article 24, est à destination des Etats membres.[169] Si cette directive revêt un caractère essentiel dans la mise en œuvre de la stratégie de cyber-sécurité européenne, elle n'a, au moment d'écrire ces lignes, toujours pas été adoptée et fait encore l'objet de débat au sein des différentes institutions européennes.[170]

Finalement, toujours en 2013, la parlement européen et le Conseil adoptent une nouvelle directive[171] venant remplacer la directive cadre de 2005[172]. Celle-ci vise à *« rapprocher le droit pénal des Etats membres dans le domaine des attaques contre les systèmes d'information en fixant des règles minimales concernant la définition des infractions pénales et les sanctions applicables »*[173] elle vise également à *« renforcer la coopération entre les autorités compétentes »*[174] Cette directive enjoint les Etats membres à adopter des mesures législatives concernant la reconnaissance ainsi que la sanction concernant divers types d'infractions liées aux réseaux de l'information. (L'accès illégal à des systèmes d'information, l'atteinte illégale à l'intégrité d'un système en sont deux exemples) Elle enjoint également les Etats membres à

[168] *idem* p19
[169] *idem* p30
[170] Eur-Lex.europa.eu, Procédure 2013/0027/COD, URL : http://eur-lex.europa.eu/procedure/FR/202368 (Consulté le 20/05/2017)
[171] Journal officiel de l'Union européenne (2013), Directive 2013/40/UE du Parlement européen et du Conseil du 12 aout 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil.
[172] Journal officiel de l'Union européenne (2005), *op.cit.*
[173] Journal officiel de l'Union européenne (2013), *op.cit.*, p8
[174] *ibidem*

définir les responsabilités, les compétences en la matière, ainsi que de se munir d'entité opérationnelles, dites « point de contact » afin de permettre l'échange de données relatives à ces infractions et ce, de manière efficace.[175]

Pour conclure cette section, il est important de préciser qu'en raison du caractère récent de cette stratégie et du délai des procédures législatives européennes, il n'est pas possible de présenter les mesures concrètes ayant découlées de cette stratégie. Comme précisé précédemment, c'est une des raisons justifiant l'arrêt de l'analyse à l'année de 2013. Cependant, cette stratégie est intéressante dans ce mémoire car elle permet de mettre en lumière des interactions entre les institutions européennes et entre celles-ci et l'ENISA.

2.2.5 L'ENISA

Outre les différents plans et stratégies proposés par les institutions européennes, l'Agence européenne chargée de la sécurité des réseaux et de l'information semble, aux vues des recommandations faites dans les différents textes, un acteur important dans cette régulation et cette gestion de la gouvernance de la protection des infrastructures d'information critiques. Cette section présentera à la fois le travail de l'ENISA et son rôle dans le réseau d'acteur impliqués dans la protection des ICC mais également sur la gestion de l'ENISA par les institutions européennes. C'est d'ailleurs par cet aspect que cette section débutera.

L'ENISA est créée en 2004 par le Conseil et le Parlement européen[176] et ce, suite à une proposition de la Commission.[177]. Partant du constat (en 2003), que de plus en plus d'individus utilisent des outils connectés, que ceux-ci ne sont plus exclusivement réservés aux informations et que des systèmes indispensables au bon fonctionnement de notre société, tel l'approvisionnement en eau ou en électricité, dépendent des réseaux, de l'internet[178]. La Commission soulève l'importance que revêt la sécurité des réseaux de l'information[179]. La Commission dresse le constat qu'à ce moment, en 2003, il n'existait pas encore de coopération systémique entre les Etats membres en matière de sécurité des réseaux, ni de mécanismes de

[175] *idem,* pp 12-14
[176] Journal officiel de l'Union européenne (2004), règlement (CE) n°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, Strasbourg
[177] Commission des Communautés européenne (2003), Proposition de règlement du Parlement européen et du Conseil instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information, COM(2003)63 final, Bruxelles
[178] *idem,* p2
[179] *ibidem*

réaction permettant une réponse efficace aux attaques et que le cadre juridique variait en fonction des Etats[180] (ce problème s'accentuera lors de l'élargissement de l'UE). L'UE doit donc se doter d'un instrument capable d'accroitre l'efficacité de la sécurité et de la protection des réseaux au niveau européen. Ainsi, le Parlement le Conseil et la Commission entendent créer un organisme doté d'une personnalité juridique et venant en aide à la fois à la Commission mais également aux Etats membres[181], ceux-ci ayant un rôle et des compétences importantes en la matière en vertu du rôle attribué aux organismes nationaux dans la directive-cadre sur les communication électroniques[182]. Comme précédemment mentionné, à la suite de cette proposition de la Commission, le Parlement européen et le Conseil adoptent en 2004 un règlement visant à instituer l'Agence européenne chargée de la sécurité des réseaux et de l'information.[183] Dans ce règlement, se retrouvent de manière claire, les objectifs et les tâches qui incombent à cette agence. Ainsi, à titre d'exemple, on retrouve en l'article deux, les objectifs tels que, *« renforcer la capacité de la communauté, des Etats membres et du secteur des entreprises de prévenir les problèmes de sécurité des réseaux et de l'information de les gérer et d'u faire face »*[184] ou encore l'objectif de *« prêter assistance et fournir des conseils à la Commission et aux Etats membres sur les questions liées à la sécurité des réseaux et de l'information (...) »*[185]. L'article 3 quant à lui consacre les tâches à accomplir par l'agence afin de rejoindre ses objectifs. Ainsi à titre d'exemple les tâches qui incombent à l'agence sont, la collecte d'informations en vue d'analyser les risques, le renforcement de la coopération entre les acteurs impliqués dans la sécurité des réseaux et de l'information ou encore faciliter la coopération entre la Commission et les Etats membres en vue d'arriver à des méthodes communes de prévention et de réponse aux problèmes.[186] Suivant les recommandations émises par le secteur privé et public et reprises dans la Communication de la Commission concernant la création de l'ENISA[187], le règlement limite dans le temps la durée d'existence de l'agence à 5 ans à dater de sa date d'institution, le 14 mars 2004[188].

[180] *idem*, p3
[181] *idem*, p5
[182] Journal officiel des Communautés européennes (2002), *op.cit.*
[183] Journal officiel de l'Union européenne (2004), *op.cit.*
[184] *idem*, p4
[185] *ibidem*
[186] *idem*, p5
[187] Commission des Communautés européennes (2003), *op.cit.*
[188] Journal officiel de l'Union européenne (2004), *op.cit.*, p.11

Dû à cette limitation d'existence dans le temps, en 2007, la Commission adopte une proposition de règlement visant à rallonger la durée d'existence de l'agence.[189] Cette proposition tient compte de l'évaluation faite de l'ENISA et présentée par la Commission au parlement et au Conseil[190]. Une de ces recommandations était la prolongation du mandat de l'ENISA[191]. Ainsi, en 2008, suite à cette proposition de la Commission, le Parlement européen et le Conseil adoptent un règlement modifiant l'article 27 du règlement de 2004 instituant l'ENISA et porte de la sorte la durée d'existence de l'agence à huit ans.[192] Se rapprochant une nouvelle fois de la date d'expiration du mandat de l'ENISA, la Commission adopte en 2010 une nouvelle proposition de règlement concernant la durée de l'ENISA[193]. Dans cette proposition, la Commission souligne l'importance que revêt l'ENISA et notamment son rôle de soutien aux Etats membres que lui a conféré le plan d'action de protection des infrastructures d'information critiques de 2009[194]. La Commission mène parallèlement un travail et un débat avec le Parlement concernant une réforme en profondeur de l'ENISA. Les débats et délais pouvant être longs, les débats pourraient encore être en cours alors que le mandat de l'ENISA toucherait à sa fin. C'est pourquoi, il est proposé de prolonger le mandat de l'Agence de dix-huit mois afin d'éviter cette situation.[195]. Ainsi en 2011, le Parlement européen et le Conseil adoptent un règlement modifiant la durée d'existence de l'agence et prolongeant celle-ci à une durée de neuf ans et six à partir de la date d'institution, le 14 mars 2004.[196] Concernant cette modification de l'ENISA, la Commission adopte en 2010 une proposition de règlement concernant l'ENISA.[197] Cette proposition une fois adoptée par le Parlement européen et le Conseil, remplacera le précédent règlement instituant l'Agence afin de créer une nouvelle mouture de cette Agence et

[189] Commission des Communautés européennes (2007), proposition de règlement du Parlement européen et du Conseil modifiant le règlement (CE) n°460/2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information en ce qui concerne sa durée, CIL(2007) 861 final, Bruxelles

[190] Commission des Communautés européennes (2007), Communication de la Commission au parlement européen et au Conseil sur l'évaluation de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), COM(2007) final, Bruxelles

[191] Commission des Communautés européennes (2007), *op.cit.*, p.3

[192] Journal officiel de l'Union européenne (2008), règlement (CE) N°1007/2008 du Parlement européen et du Conseil du 24 septembre 2008 modifiant le règlement (CE) N°460/2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information en ce qui concerne sa durée, Strasbourg, p.2

[193] Commission européenne (2010), Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (CE° n°460/2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information en ce qui concerne sa durée, COM(2010) 520 final, Bruxelles

[194] Commission des Communautés européennes (2009), *op.cit.*

[195] Commission européenne (2010), *op.cit.* ,p3

[196] Journal officiel de l'Union européenne (2011), Règlement (UE) n°(80/2011 du Parlement européen et du Conseil du 8 juin 2011 modifiant le règlement (CE) n°460/2004 instituant l'Agence européenne charge de la sécurité des réseaux et de l'information en ce qui concerne sa durée, Strasbourg, p1

[197] Commission européenne (2010b), proposition de règlement du Parlement européen et du Conseil concernant l'Agence européenne chargée de la sécurité des réseaux et de l'information – ENISA, COM(2010)521, Bruxelles

ce, pour une durée de cinq ans. Ce règlement est adopté en 2013 par le Parlement européen et le Conseil.[198]

Cette première partie consacrée à l'ENISA présentait les modifications institutionnelles apportées par les institutions européennes concernant le mandat de l'Agence. Les prochains paragraphes seront consacrés aux mesures prises par les institutions européennes dans les différents plans d'action afin de diriger le travail de l'ENISA.

Le premier plan présenté dans ce chapitre est l'EPCIP adopté par la Commission dans sa communication de 2006 concernant un programme européen de protection des infrastructures critiques[199]. Bien que l'ENISA soit créé depuis déjà deux ans, on ne retrouve dans cette communication aucune mesures prises concernant l'agence. Toujours en 2006, la Commission adopte une communication concernant une stratégie pour une société de l'information sûre.[200]

Si cette communication ne parle pas à proprement parler de la protection des infrastructures d'information critiques, elle revêt un intérêt certain dans cette recherche car elle présente une stratégie visant à atteindre un certain niveau de sécurité et ce par trois principes, le dialogue, le partenariat et la responsabilisation[201]. Ces trois principes induisent un système de fonctionnement du réseau des acteurs impliqués dans la sécurité des réseaux et de l'information. De plus, dans cette communication, la Commission émet une série de mesures à destination de l'ENISA.

Ainsi dans cette stratégie, en termes de partenariat, la Commission demande à l'ENISA de « *développer un partenariat de confiance avec les Etats membres et les parties prenantes en vue d'élaborer un cadre approprié pour la collecte de données »*[202]. Et ce, dans le but de parvenir à une politique de sécurité efficace et à une compréhension optimale et partagée de l'ampleur des défis à relever[203]

La Commission entend également demander à l'ENISA « *d'examiner la faisabilité d'un système européen de partage d'informations et d'alerte »*[204]. Et ce, en vue d'améliorer la réponse aux menaces pesant sur les réseaux.[205]

---

[198] Journal officiel de l'Union européenne (2013b), règlement (UE) n°526/2013 du Parlement européen et du Conseil du 21 mai 2013 concernant l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et abrogeant le règlement (CE) n°460/2004, Strasbourg

[199] Commission des Communautés européennes (2006a), *op.cit.*

[200] Commission des Communautés européennes (2006b), Communication de la Commission au Conseil, au Parlement européen, au Comité économique et social européen et au Comité des Régions sur une stratégie pour une société de l'information sûre –"Dialogue, partenariat et responsabilisation", COM(2006) 251 final, Bruxelles

[201] *ibidem*

[202] *idem*, p9

[203] *ibidem*

[204] *ibidem*

[205] *ibidem*

Suite à ces deux communications de la Commission, le Conseil adopte une résolution en 2007 relative à une stratégie pour une société de l'information sûre en Europe.[206] Dans cette résolution, le Conseil engage l'ENISA « *à continuer de travailler en étroite coopération avec les États membres, la Commission et les autres parties prenantes concernées afin d'atteindre les objectifs et d'accomplir les tâches définis dans le règlement (CE) no 460/2004 et à apporter son aide à la Commission et aux États membres dans les efforts qu'ils déploient en vue de satisfaire aux exigences en matière de sécurité des réseaux et de l'information, et contribuer ainsi à la mise en œuvre et au développement de la stratégie pour une société de l'information sûre en Europe, telle qu'elle est définie dans la présente résolution »;*[207]

Ensuite, en 2009, la Commission adopte une communication relative à la protection des IIC[208]. Ce plan d'action a déjà fait l'objet d'une présentation dans la section précédente, il sera fait état ici uniquement des mesures concernant l'ENISA. Le premier élément à mettre en lumière dans ce plan d'action est que l'Agence est sollicitée principalement pour venir en aide et soutenir les Etats membres dans chaque axe du plan et chaque volet. Ainsi, à titre d'exemple, la Commission invite l'ENISA à aider les Etats membres dans la définition d'un niveau minimum de capacités et de services pour les équipes d'intervention CERT[209] ; ou encore, l'ENISA est invitée à faire l'évaluation et l'inventaire des résultats des projets de partages d'information au niveau européen et national et i*n fine* d'aboutir à une feuille de route afin de promouvoir le déploiement du projet européen SEPIA[210]

Cette volonté de la Commission de faire de l'ENISA un appui et un soutien pour les Etats membres se retrouve également dans la résolution du Conseil[211] adoptée dans la foulée du plan d'action de 2009.

En 2011, la Commission adopte une nouvelle communication[212] concernant le plan de protection de IIC, dans laquelle elle dresse un inventaire des actions déjà entreprises ainsi que de nouvelles mesures à prendre pour améliorer l'efficacité de la protection.

---

[206] Journal officiel de l'Union européenne (2007), Résolution du Conseil du 22 mars 2007 relative à une stratégie pour une société de l'information sûre en Europe, (2007/C 68/01)

[207] *idem*, p4

[208] Commission des Communautés européennes (2009), Communication de la Commission au Parlement européen, au Conseil, au comité économique et social européen et au comité des régions relative à la protection des infrastructures d'information critiques : « protéger l'Europe des cyberattaques et des perturbations de grande envergure : améliorer l'Etat de préparation, la sécurité et la résilience », COM(2009)149 final, Bruxelles

[209] *idem*, p9

[210] *idem*, p10

[211] Journal officiel de l'Union européenne (2009), Résolution du Conseil du 18 décembre 2009 sur une approche européenne concerté en matière de sécurité des réseaux et de l'information, 2009/C 321/01

[212] Commission européenne (2011), *op.cit.*

Dans ces nouvelles recommandations à l'ENISA la Commission réitère sa volonté de voir l'Agence soutenir et appuyer les Etats membres dans leurs entreprises d'amélioration de la protection des ICC et de faciliter la coopération.[213] Ainsi, à titre d'exemple, la Commission invite l'ENISA à *« développer des services d'interopérabilités permettant l'intégration de tous les systèmes nationaux de partage d'information et d'alerte dans le SEPIA »*[214], ou encore, elle invite l'ENISA à continuer son soutien aux Etats membres dans l'élaboration de plan nationaux d'urgence et à organiser des exercices concernant les réactions en cas d'incidents de grande envergure[215].

Finalement, en 2013, la Commission adopte une communication concernant une stratégie de cyber-sécurité européenne[216]. De nouveau, la Commission réitère sa volonté de voir l'ENISA soutenir les Etats membres via l'élaboration de feuilles de route, de partage de bonnes pratiques en matière de prévention et de protection ainsi qu'un soutien opérationnel de l'Agence[217]. A titre d'exemple, la Commission invite l'ENISA à *« élaborer, en coopération avec les autorités nationales compétentes, les parties intéressées, les organismes européens et internationaux de normalisation et le Centre commun de recherche de la Commission européenne, des orientations et recommandations techniques pour l'adoption de normes et bonnes pratiques SRI dans les secteurs public et privé*[218], ou encore, à *« aider les Etats membres à développer de solides moyens de cyber-résilience au niveau national(…) »*[219]

La dernière partie de cette section consacrée à l'ENISA s'attardera sur les actions entreprises par l'ENISA concernant son aide et son soutien aux acteurs impliqués dans la protection des infrastructures d'information critiques.

Suivant les recommandations et directives des institutions européennes, l'ENISA a publié une série de documents concernant la reconnaissance des infrastructures critiques ou encore des bonnes pratiques à adopter en termes de protection et de prévention.

Ainsi, En 2009, l'ENISA publie un document intitulé *« Baseline capabilities for national/governmental CERTs »*[220] ainsi qu'une deuxième partie contenant les

[213] *idem*, pp11-18
[214] *idem*, p14
[215] *idem* p15
[216] Commission européenne (2013a), *op.cit.*
[217] *idem*, pp 7-15
[218] *idem*, p14
[219] *idem*, p8
[220] ENISA (2009a), Baseline capabilities for national/governmental CERTs, version 1.0 (initial draft)

recommandations[221]. Toujours en 2009, l'Agence publie un guide de bonnes pratiques sur les exercices nationaux[222]

En février 2010, l'ENISA prépare l'organisation du premier exercice paneuropéen sur la protection des ICC et ce, à la demande des Etats membres.[223] Afin de préparer au mieux cet exercice, divers ateliers furent organisés avec les Etats membres afin de les impliquer dans la préparation de l'exercice et ainsi s'assurer la participation d'un maximum d'entre eux[224] Au total, quatre ateliers se sont tenus afin de préparer au mieux cet exercice[225] dont la première phase s'est déroulée en Septembre 2010[226]. Le 4 novembre, l'exercice prend fin. 22 Etats-membres ont participé activement à l'exercice et 8 ont eu un rôle d'observateur. Le but final de cet exercice était d'établir un lien de confiance entre les Etats membres, d'accroitre les capacités de management de crise et de comprendre comment les interventions sont effectuées par les Etats membres, de tester les points de contacts et la communication, les procédures entre les Etats membres, de mettre en lumière les interdépendances entre ceux-ci et d'augmenter la capacité d'aide mutuelle des Etats membres en cas d'incident.[227]

Un nouvel exemple du support que fournit l'ENISA aux Etats membres et aux autorités nationales compétentes est à trouver dans la publication d'un guide sur les bonnes pratiques, des informations pratiques et des lignes directrices concernant la gestion d'incidents des réseaux par les CERTs[228]

Outre le support opérationnel fourni aux Etats membres, l'ENISA joue également un rôle de recherche et d'identification des nouvelles menaces dans une société où la technologie est en perpétuelle évolution. Ainsi à titre d'exemple, l'Agence, en 2012, publie un rapport[229]

---

[221] ENISA (2009b), Baseline capabilities of national/governmental CERTs part 2: Policy Recomandations, version 1.0 (initial draft)

[222] ENISA (2009c), Resilient e-Communications Networks – Good practice guide on national exercices enhancing the resilience of public communications networks

[223] ENISA (2010a), News item – first pan européan CIIP exercise, publié le 3 février 2010. URL : https://www.enisa.europa.eu/news/enisa-news/1st-pan-european-ciip-excercises, (consulté le 23 mai 2017)

[224] ENISA (2010b), News Item – towards the first pan européan CIIP exercise, publié le 15 mars 2010, URL : https://www.enisa.europa.eu/news/enisa-news/towards-the-1st-pan-european-ciip-exercise (consulté le 23 mai 2017)

[225] www.enisa.europa.eu/news

[226] ENISA (2010c), News item – "cyber europe 2010" the first pan européen CIIP exercise, publié le 4 octobre 2010, URL : https://www.enisa.europa.eu/news/enisa-news/2018cyber-europe-20102019-the-1st-pan-european-ciip-exercise-phase-one, (consulté le 23 mai 2017)

[227] ENISA (2010d), Press release – First EU cyber security exercise "cyber Europe 2010" with >320 "incidents" successfully concluded, publié le 5 novembre 2010, URL : https://www.enisa.europa.eu/news/enisa-news/cyber-europe-20102019-cyber-security-exercise-with-320-2018incidents2019-successfully-concluded, (consulté le 23 mai 2017)

[228] ENISA (2011b), Press release – New guide on cyber security incident management to support the fight against cyber attacks, publié le 20 janvier 2011, URL : https://www.enisa.europa.eu/news/enisa-news/new-guide-on-cyber-security-incident-management-to-support-the-fight-against-cyber-attacks, (consulté le 23 mai 2017)

[229] ENISA (2012), Critical cloud computing – A CIIP perspective on cloud computing services, Version 1.0

concernant l'importance que revêt la sécurité du *cloud* tant ces dernières années de nombreux infrastructures et organisations sont devenues dépendantes de l'internet en nuage.[230]

Une dernière action de l'ENISA pouvant être mise en lumière est la création d'un partenariat public-privé (*European Public Private Partnership for Resilience, EP3R)* dans la foulée du plan d'action de protection des infrastructures critiques adopté par la Commission en 2009[231]. Ce partenariat est créé pour accroitre la coopération entre les diverses parties et suis quatre objectifs : Encourager le partage d'information et les bonnes pratiques politiques et industrielles afin d'améliorer une compréhension commune ; être une plateforme de débat concernant les priorités, les objectifs et les mesures des politiques ; arriver à des critères minimum pour la sécurité et la résilience en Europe ; et finalement L'indentification et la promotion de bonnes pratiques minimales en terme de sécurité et de résilience[232]

Cette section consacrée à l'Agence européenne chargée de la sécurité des réseaux et de l'information revêt un double intérêt dans cette recherche. En effet, d'une part elle présente la gestion de l'ENISA par les institutions européennes et de l'autre elle présente les actions de l'ENISA en tant que méta-gouvernant. Cette double casquette de l'ENISA se révèlera d'une importance capitale lors de l'analyse de la régulation du réseau qui fera l'objet du chapitre suivant.

2.2.6 Autres

Cette section s'attardera sur une série de mesures ne rentrant pas dans un des plans mais relevant d'un intérêt dans cette recherche car ils modifient des cadres légaux ou des objectifs généraux venant impacter les acteurs impliqués dans la protection des infrastructures d'information critiques

La première mesure présentée est une décision-cadre de 2005, adoptée par le Conseil, relative aux attaques visant les systèmes d'information[233]. Cette décision-cadre est à destination des

[230] ENISA (2013), Press release – New Enisa report : the double-edged sword of cloud computing in Critical Information Infrastructure Protection, publié le 14 février 2013, URL : https://www.enisa.europa.eu/news/enisa-news/new-enisa-report--the-double-edged-sword-of-cloud-computing-in-critical-information-infrastructure-protection, (consulté le 23 mai 2017)

[231] Commission des Communautés européennes (2009), *op.cit.*

[232] ENISA, European Public Private Partnership for Resilience (EP3R), URL : https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ppps/public-private-partnership/european-public-private-partnership-for-resilience-ep3r, (consulté le 23 mai 2017)

[233] Journal officiel de l'Union européenne (2005), Décision-cadre 2005/222/JAI du Conseil du 24 février 2005 relative aux attaques visant les systèmes d'infromation, Bruxelles

Etats membres, ces dernier devant adopter dans leurs cadres législatifs nationaux respectifs les dispositions dans un laps de temps défini, comme le stipule son article 12[234]
Cette décision cadre vise à harmoniser les cadres légaux nationaux en matière de reconnaissance, d'identification et de sanction des attaques visant les systèmes d'informations, ainsi qu'à faciliter et encadrer la coopération en matière de partage d'informations entre les Etats membres. [235] Cette décision sera modifié en 2013 par le Parlement et le Conseil.[236] Cette décision-cadre a été sélectionnée dans la matériau empirique de ce mémoire car elle institue un cadre légal européen amenant les Etats membres à évoluer dans une direction commune. Ce qui est, un des aspects du « travail » du méta-gouvernant.

Le deuxième élément présenté dans cette section est une communication de la Commission adoptée en 2006 concernant une stratégie pour une société de l'information sûre.[237] Dans cette communication, la Commission relève que malgré les efforts effectués par les secteurs privé et public et ce, au niveau mondial, européen ou national, la sécurité pose encore et toujours de sérieux problèmes.[238] Et les évolutions technologiques ne cessant de s'accélérer, de nouveaux logiciels malveillants ne cessent d'inonder les réseaux[239]. C'est pourquoi la Commission entend via cette stratégie, amener les parties prenantes vers un système de gouvernance caractérisé par le dialogue, le partenariat et la responsabilisation. Ainsi, la Commission invite, les Etats membres, et les autres parties prenantes à collaborer dans le partage des bonnes pratiques en matière de sécurité de l'information (SRI), en participant à des exercices de cyber-incidents et à créer des partenariats afin d'assurer la disponibilité et le partage des informations.[240]
Ce document trouve son intérêt dans cette recherche car il tente d'influencer les acteurs du réseaux en agissant sur le type de relation qui caractérise ce réseau d'acteur.

Le dernier document présenté dans cette section découle directement de la précédente communication. Dans la foulée de cette dernière, le Conseil adopte une résolution relative à

[234] *idem*, p71
[235] *idem*, pp 68-70
[236] Journal officiel de l'Union européenne (2013a), *op.cit.*
[237] Commission des communautés européennes (2006b), Communication de la Commission au Conseil, au Parlement européen, au Comité économique et social européen et au Comité des Régions – Une stratégie pour une société de l'information sûre – « dialogue, partenariat et responsabilisation », COM(2006) 251 final, Bruxelles
[238] *idem*, pp3-6
[239] *ibidem*
[240] *idem*, pp 8-10

une stratégie pour une société de l'information sûre en Europe.[241] Cette Résolution a déjà été citée précédemment dans ce mémoire. Par cette mesure, le Conseil engage les acteurs à intensifier leurs efforts en matière d'attitude à adopter concernant la sécurité, à intensifier la coopération entre toutes les parties prenantes ainsi qu'à mettre en œuvre des bonnes pratiques afin d'atteindre un niveau optimal de sécurité des TIC.[242] Ce document s'avèrera pertinent dans l'analyse car il consacre à la fois les mesures prises dans la stratégie de 2006 pour une société de l'information sûre mais également une série de mesures prises dans le cadre de l'EPCIP précédemment présenté.

L'Union européenne est consciente depuis plusieurs décennies que les technologies de l'information et de la communication prennent une place de plus en plus importante dans notre société. Cela va de pair avec de nouvelles formes de menaces liées à l'évolution de ces technologies. Si au début des années 80 jusqu'à l'aube du troisième millénaire l'Union européenne ne s'est pas impliqué de manière importante en la matière (faute aussi au niveau technologique de l'époque). Les années 2000 et les évolutions technologiques toujours plus importantes ont vu l'Union européenne intensifier son travail en vue de protéger les réseaux au maximum et ainsi assurer le bon fonctionnement de notre société. Si atteindre ce niveau de sécurité nécessite des efforts de toutes les parties concernées, allant de l'UE à l'utilisateur final, certains aspects de sécurité relèvent du bon vouloir des Etats membres et des exploitant de certaines infrastructures dites critiques. Ainsi à partir de 2005 la Commission intensifie son travail en matière de protection d'infrastructures critiques et plus tard, plus particulièrement en matière de protection d'infrastructures d'informations critiques. L'UE ne disposant pas des ressources nécessaires à la gestion de la protection de ces infrastructures elle se voit contrainte, dans les limites de ses compétences, de tenter d'influencer les acteurs impliqués et de les faire avancer dans une direction commune afin de combiner les efforts et de maximiser l'efficacité de la sécurité. C'est pourquoi, entre 2005 et 2013 l'UE, a produit une série de programme, plan d'action et stratégie afin d'instaurer un système de gouvernance au sein duquel les relations entre acteurs sont facilitées, et la coopération entre ces derniers est accrue. Afin d'institutionnaliser certains aspects de ces plans, le Parlement et le Conseil ont adopté une série de directives et de résolutions à destination des Etats-membres et des parties prenantes à la protection des IIC. L'ENISA, l'agence européenne chargée de la sécurité des réseaux et de

[241] Journal officiel de l'Union européenne (2007), Résolution du Conseil du 22 mars 2007 relative à une stratégie pour une société de l'information sûre en Europe, (2007/C 68/01)
[242] *idem*, p4

l'information joue également un rôle important dans l'efficacité de ce réseau. Cette agence sert de bras opérationnel aux institutions européennes en étant en contact direct avec les différents acteurs. Le chapitre suivant sera consacré à l'analyse des modes opératoires utilisés par l'UE en vue de gérer ce système de gouvernance constitué d'acteurs autonomes et interdépendants issus des secteurs publics et privés.

Chapitre 3 : Analyse et réponse aux hypothèses

3.1 Analyse

Cette partie sera consacrée à l'analyse des élément précédemment exposés. Ceux-ci concernant la gestion et la régulation du réseau d'acteurs impliqués dans la cyber-sécurité européenne et en particulier dans la protection des infrastructures d'information critiques. L'objectif de cette analyse est de mettre en lumière les différents modes d'exercice de la méta-gouvernance par l'Union européenne en vue de comprendre comment cette dernière parvient à exercer sa fonction de méta-gouvernant. A cette fin, et comme mentionné précédemment, la typologie d'Eva Sorensen servira de grille de lecture lors de cette analyse. Préalablement à l'analyse à proprement parler, il est intéressant d'effectuer un bref rappel de cette typologie et des éléments principaux caractérisant chacun des quatre modes opératoires identifiés.

La première, le *hands-off framing of the self governance* qui consiste en un façonnage du contexte politique, économique, financier au sein du quel évolue le réseau. Deuxièmement le *hands-off storytelling,* qui consiste en la construction de buts communs et la construction d'un imaginaire collectif notamment. La troisième, le *hands-on support and facilitation to self-governing actors,* qui consiste en une intervention directe du méta-gouvernant afin de supporter et de promouvoir les activités des acteurs du réseau. Et finalement, la quatrième forme est celle du *hands-on participation.* Dans cette forme, le méta-gouvernant agit comme un acteur à part entière du réseau afin de l'influencer.

L'analyse sera divisée en cinq parties, à l'instar de la partie précédente consacrée à la protection des IIC, à savoir, 1) l'EPCIP ; 2) le plan d'action PIIC ; 3) Stratégie de cyber-sécurité européenne de 2013 ; 4) l'ENISA, cette partie sera elle-même analysée en deux temps. Premièrement la gestion de l'ENISA par les Institutions européennes et deuxièmement, les actions de l'ENISA en sa qualité de méta-gouvernant ; et finalement 5) Autres

3.1.1 L'EPCIP

Les premiers éléments faisant l'objet de cette analyse sont les actions et mesures prises et entreprises dans la cadre du programme européen de protection des infrastructures critiques.

Ainsi le livret vert de la Commission concernant un programme européen de protection des infrastructures critiques adopté en 2005[243] est le point de départ de ce programme et de notre analyse. Ce document proposant une série de scénarios concernant la future mise en place d'un programme européen de protection des IC est à destination d'un maximum d'acteurs impliqué dans la protection de ces infrastructures, à savoir, les Etats membres, les propriétaires et exploitants d'infrastructures, les organes de réglementation, les organisations professionnelles, les associations sectorielles et les administrations publiques à tous les niveaux[244]. Par ce livret vert, la Commission répond à une demande du Conseil[245] concernant un programme Européen de protection d'infrastructures critiques, et surtout effectue un pas en avant dans le processus de gestion de la sécurité des IC. L'objectif de la Commission en publiant ce livret est une réaction et une mobilisation maximale des acteurs[246] en vue de l'élaboration d'un programme de protection étant au plus près des préoccupations des parties prenantes et de la sorte atteindre une adhésion importante et une participation importantes à ce programme

Au regard de la typologie de Sorensen, cette démarche de la Commission s'inscrit dans le mode opératoire dit du *storytelling.* En effet, malgré les interactions directes entre la Commission et les autres acteurs, celles-ci restent d'ordre purement consultatif. Le but de ce livret est d'amener les acteurs constituant le réseau vers un objectifs commun, les amener à collaborer dans un futur programme et ce en leur proposant divers scénarios d'élaboration de ce dernier. En mettant en avant les relations qui existent entre les acteurs, en les amenant à identifier les types de risques face auxquels le programme devra faire face par exemple. Cette pratique s'inscrit pleinement dans le *storytelling* dans le sens ou la Commission tente de construire une image d'un futur commun et engendre des attentes des acteurs de ce futur.

Le second élément à faire l'objet de cette analyse est une communication adoptée par la Commission en 2006 concernant un programme de protection des infrastructures critiques.[247] Ce document fait suite au livret vert de 2005. Le plan présenté est à destination, comme pour le livret vert de 2005, de toutes les parties prenantes et intéressées dans le domaine de la protection des infrastructures critiques. Cette communication *« expose les principes, les*

[243] Commission des Communautés européennes (2005), *op.cit.*
[244] *idem*, p3
[245] *idem*, p2
[246] *ibidem*
[247] Commission des Communautés européennes (2006a), *op.cit.*

procédures et les instruments proposés pour mettre en œuvre l'EPCIP[…] »[248]. Ce document présente un cadre communautaire pour la protection des IC[249]

De cette démarche de la Commission, il est possible d'identifier deux modes opératoires relevant de la méta-gouvernance. Dans un premier temps, il est possible de mettre en lumière des pratiques d'ordre *storytelling.* En effet, la Commission, identifie les menaces auxquelles doivent faire face les IC, elle se dresse également comme allié des Etats membres on se disant disponible en cas de sollicitation des Etats notamment en matière de recensement des IC et met l'accent sur les interdépendances existant entre les acteurs[250]. De la sorte, la Commission induit, dans le chef des parties prenantes, des images d'un « ennemi » commun et d'allié commun. Cette construction d'un imaginaire collectif et de relation est une des caractéristiques du *storytelling.*

Dans un second temps, la Commission établit un plan d'action comprenant plusieurs volets eux même divisés en plusieurs phases. Chaque action de ce programme cible un acteur, avec un délai d'action plus ou moins précis. (Voir annexe 3). La création d'un cadre d'action, précis, et d'objectif généraux tout en laissant la mise en œuvre aux acteurs relève selon la typologie de Sorensen du *Hands-off framing*. Celui-ci étant exercé de manière douce, le design institutionnel n'étant pas modifié.

Le troisième et dernier élément analysé dans le cadre de l'EPCIP est la directive 2008/114/CE du Conseil se rapportant au recensement et à l'identification des infrastructures européennes.[251] Cette directive est à destination des Etats membres.[252] Elle vient institutionnaliser une série de mesures concernant l'identification et le recensement des ICE proposées dans la Communication de la Commission.[253] L'adoption de cette directive s'inscrit dans une démarche dite de *framing.* En effet, cette dernière institutionnalise une méthodologie d'indentification et de recensement des infrastructures critiques ainsi qu'un plan de sécurité des opérateurs qu'elle détaille ensuite dans son annexe.[254] (ANNEXE 4) Cette directive contraint les Etats membres à adopter les mesures nécessaires à la mise en œuvre des objectifs décrit dans celle-ci, et ce, endéans un laps de temps imparti comme le stipule son article 12 consacré à la mise en œuvre : « les Etats membres adoptent les dispositions nécessaire pour se conformer à la présente

[248] *idem,* p2
[249] *ibidem*
[250] *idem,* pp 2-7
[251] Journal officiel de l'Union européenne (2008a), *op.cit.*
[252] *idem,* p80
[253] Commission des Communautés européennes (2006a), *op.cit.*
[254] Journal officiel de l'Union européenne (2008a), *op.cit.,* pp 81-82

directive au plus tard le 12 janvier 2011 ».[255] La modification du cadre institutionnel et des règles du jeu régissant le système de gouvernance au sein duquel évoluent les acteurs relèvent du *framing* exercé de manière forte.
Si la création d'un centre d'alerte et de partage d'information européen a été abordé dans le chapitre précédent, celui ne fera pas l'objet d'une analyse étant donné qu'il n'a pas vu le jour et que la proposition fut retirée plusieurs années plus tard.

De cette première partie il est possible de retirer les éléments suivants. Premièrement, la Commission adopte des comportements relevant du *Hands-off framing* et du *Hands-off storytelling.* Ses recommandations et mesures visent tous les acteurs impliqués dans la protection des infrastructures critiques.
Le Conseil, agit suite à la proposition de la Commission. Il exerce la méta-gouvernance suivant un mode opératoire relevant du *hands-off framing* et le fait en direction des Etats membres.

3.1.2 Plan d'action PIIC

La deuxième section de cette analyse sera consacrée au plan d'action de protection des infrastructures d'information critiques présenté et adopté en 2009 par la Commission. Le premier élément à être analysé est la communication concernant le plan PIIC adopté par la Commission en 2009.[256] Ce document et le plan qu'il consacre prennent place dans une nouvelle démarche de l'UE concernant la protection des IIC et émanant du constat que, malgré les efforts déjà entrepris et les mesures déjà prises, les acteurs du réseau ne s'impliquent pas encore assez et mettent ainsi en danger la sécurité de ces infrastructures[257]
Une nouvelle fois, lors de l'analyse de cette action entreprise par la Commission il est possible d'identifier deux comportements de méta-gouvernance se combinant. Premièrement, dans sa première partie, la Commission narre les risques encourus et les menaces pesant sur les infrastructures d'information critiques. Elle identifie également les enjeu d'une meilleure sécurité, d'une meilleure préparation et la nécessité d'une meilleure coopération entre tous les acteurs afin d'arriver à une efficacité maximale en matière de protection de ces infrastructures. De ce point de vue-là, cette pratique peut être considérée comme du *hands-off storytelling* au regard de la typologie de Sorensen. En effet, de nouveau, la Commission identifie l'ennemi,

[255] *idem*, p80
[256] Commission des Communautés européennes (2009), *op.cit.*
[257] *idem*, p3

ainsi que les enjeux que revêt une meilleure protection pour amener les acteurs à se mobiliser dans la même direction, à savoir, une coopération accrue en vue d'améliorer la protection des infrastructures critiques.

Dans un second temps, la Commission propose un plan afin de parvenir à un meilleur niveau de protection des infrastructures d'information critiques. Les mesures constituant ce plan sont à destination de l'ENISA, des Etats membres ainsi qu'à toute autre partie prenante et invite ceux-ci à diverses entreprises afin d'atteindre les objectifs précédemment définis par la Commission et correspondant aux différents axes du plan d'action. Par cette démarche, la Commission modifie le contexte politique au sein duquel évoluent les acteurs et ce, via la définition d'objectifs généraux tout en laissant la liberté d'action aux acteurs. Cette pratique relève, selon la typologie d'Eva Sorensen, du *Hands-off framing*, exercé de manière douce. En effet, le cadre institutionnel n'est pas modifié. Seuls des objectifs et une manière de les atteindre sont présentés aux acteurs.

Le deuxième élément prenant place dans l'élaboration du plan d'action PIIC à être analysé est une résolution[258] adoptée par le Conseil et adoptée en 2009 dans la foulée de l'adoption du plan d'action PIIC par la Commission. Cette résolution consacre une série de mesures présentées dans la communication de la Commission. Elle est destinée à toutes les parties prenantes à la sécurité et la protection des infrastructures d'information critiques. Avant de poursuivre l'analyse il est important de préciser qu'un nombre conséquent de mesures sont prises à destination de l'ENISA dans le plan précédemment présenté, dans cette résolution et dans les futurs éléments analysés. Ces mesures à destination de l'ENISA seront analysées dans une partie ultérieure et entièrement dévolue à l'Agence. Ainsi donc, cette résolution invite les parties visées par cette dernière à continuer les efforts entrepris, ou à prendre de nouvelles dispositions, mesures ou actions afin d'améliorer cette protection. Par cette résolution le Conseil reprend les objectifs du plan d'action et invite les acteurs à les atteindre via une meilleure collaboration, en améliorant et en intensifiant le partage d'informations notamment. Cette démarche du Conseil s'inscrit, selon les critères identifiés par Sorensen, dans le *hands-off framing* étant donné que le Conseil définit des objectifs généraux et des principes régissant les interactions entre acteurs afin d'atteindre ceux-ci. Et modifie de la sorte le contexte politique.

Le troisième élément à être analysé dans le cadre du plan d'action PIIC est à mettre à l'actif de la Commission qui, en 2011, adopte une nouvelle communication concernant son plan de

[258] Journal officiel de l'Union européenne (2009), *op.cit.*

protection des infrastructures d'information critiques[259] Celle-ci fait l'état des lieux des actions déjà effectuées dans le cadre du plan de 2009[260]. Elle présente également les prochaines étapes du plan d'action afin de poursuivre et d'améliorer sa mise en œuvre et de la sorte, atteindre un niveau de protection optimal. Cette communication amène ainsi des évolutions dans la mise en œuvre en fonction des actions déjà menées et en s'adaptant aux évolutions technologiques. Elle fait également office de réactivation des acteurs impliqués dans la mise en œuvre du plan.
Cette communication revêt un caractère plutôt informatif. Néanmoins, elle réaffirme le cadre d'action au sein duquel doivent évoluer les acteurs et le réajuste en fonction des besoins de la mise en œuvre du plan. Cette démarche peut donc est identifiée comme un comportement relevant du *Hands-off framing.*

L'élément suivant est de nouveau à mettre à l'actif de la Commission. Cette dernière, en vue d'améliorer la mise en œuvre du plan d'action, a établi en 2009 un forum européen des Etats membres.[261] Ce forum est créé en vue d'offrir aux Etats membres une arène favorisant les débats et l'échange concernant notamment les bonnes pratiques[262]. Ainsi, la création d'une telle structure peut s'apparenter au mode opératoire se rapportant au *hands-off framing*. En effet, la Commission crée un espace d'échange et par la modifie une partie du cadre institutionnel, via l'ajout d'une nouvelle arène, au sein de laquelle s'opèrent les processus d'interaction entre un certain type d'acteurs, en l'occurrence l'autorité publique. La création de cette plateforme de débat peut être vue comme une modification du contexte politique dans lequel évoluent les acteurs et ainsi amener ce réseau autorégulé vers une meilleure coopération en matière d'échange de bonnes pratiques notamment.
Le dernier élément analysé dans le cadre du plan PIIC est une nouvelle fois à mettre à l'actif de la Commission. Cette dernière, dans le cadre du développement d'un système européen de partage d'information, a soutenu financièrement deux projets prototypes de système de partage et ce, dans le cadre du projet européen « prévention, préparation et gestion des conséquences en matière de terrorisme et autres risques liés à la sécurité »[263]

De cette analyse du plan PIIC il ressort plusieurs éléments. Premièrement, la Commission exerce principalement la méta-gouvernance de manière *Hands-off,* à la fois *framing* et

[259] Commission européenne (2011), *op.cit.*
[260] Commission des Communautés européennes (2009), *op.cit.*
[261] Commission européenne (2011),*op.cit.,* p13
[262] *ibidem*
[263] Journal officiel de l'Union européenne (2007b), *op.cit.*

storytelling et ce à destination de toutes les parties prenantes. Il ressort également qu'elle a agi de manière *Hands-on* via le support en termes de ressources financière à un projet particulier. Deuxièmement, de nouveau le Conseil agit dans la foulée de la Commission et exerce la méta-gouvernance selon un mode d'action relevant du *Hands-off framing.*

3.1.3 Stratégie de cyber-sécurité européenne 2013

Cette partie se concentrera sur les actions entreprises par les Institutions européennes dans le cadre de la stratégie de cyber-sécurité de 2013 adoptée par la Commission.[264]Ce document est à destinations en particuliers des Institutions européennes, des organismes européens et aux Etats membres, mais consacre également certaines mesures à destination du secteur privé et du monde académique. Cette communication ne vise pas directement la protection des infrastructures d'information critiques mais présente un nouveau cadre de gouvernance de la cyber-sécurité en général. Ce qui, *de facto,* impacte le cadre de gouvernance de la sécurité et de la protection des infrastructures d'information critiques.

De nouveau, ce document peut être analysé en deux temps et deux modes opératoires relevant de la méta-gouvernance peuvent y être identifiés. Ainsi dans un premier temps, la Commission identifie les nouvelles menaces ainsi que les potentielles solutions à amener en vue de parvenir à un niveau de sécurité optimal. Elle met en avant les relations d'interdépendances qui existent entre les acteurs et le besoin pour tous d'avoir un niveau de sécurité optimal afin de ne pas représenter un point faible dans la sécurité. Cette pratique peut être considérée comme du *Hands-off storytelling.* En effet, le fait d'identifier une menace commune, de faire prendre conscience des relations qui unissent les acteurs afin de les amener à travailler de concert en vue d'atteindre un niveau de sécurité optimal rejoint pleinement les critères énoncés par Sorensen concernant la pratique du *storytelling.*

Dans un second temps, la Commission présente une série de mesures et d'actions à entreprendre afin de mettre en œuvre la stratégie de cyber-sécurité. La Commission invite les différents acteurs à collaborer en matière notamment de recherche et de développement ou de lutte contre la cybercriminalité. Par cette stratégie, la Commission introduit un nouveau cadre de gouvernance en établissant des partenariats, des responsabilités et en fixant des objectifs généraux à atteindre. Cette pratique se rapporte à du *hands-of framing.* En effet, la Commission

[264] Commission européenne (2013a), *op.cit.*

modifie les règles du jeu, identifie des objectifs généraux, mais laisse les acteurs agir de manière autonome dans la réalisation de ces objectifs.
Afin d'institutionnaliser cette stratégie, une proposition de directive est jointe à cette communication.[265] Cependant, à l'heure actuelle, le travail législatif est toujours en cours et cette directive n'a toujours pas été adoptée. Elle ne fera donc pas l'objet d'une analyse mais reste pertinente comme élément à prendre en compte lors de la réponse à la question centrale de cette recherche.

Le second et dernier élément à être analysé dans le cadre de cette stratégie européenne de cyber-sécurité est à mettre à l'actif du Parlement européen et du Conseil. Ceux-ci ont adoptés en 2013 une directive[266] venant remplacer une décision cadre de 2005[267] (2005/222/JAI) concernant l'identification et la sanction des attaques contre les systèmes d'information. Cette directive est à destination des Etats membres et vise à harmoniser et rapprocher le droit pénal de ces derniers en matière d'attaque contre les systèmes d'information ainsi qu'à instaurer un nouveau système de coopération entre les Etats membres. Cette directive, venant modifier le cadre institutionnel et visant à modifier le cadre légal des Etats membres peut être considérée comme une pratique du *hands-off framing* et ce de manière forte car le design institutionnel est modifié.

De l'analyse de cette stratégie de cyber-sécurité il est possible de ressortir les éléments suivants. Premièrement, la Commission agit selon des procédés relevant du *Hands-off framing* et du *storytelling.* Elle exerce cette méta-gouvernance à destination de toutes les parties impliquées dans la cyber-sécurité.
Deuxièmement, le Parlement européen et le Conseil exercent la méta-gouvernance via le *hands-off framing* et ce, en modifiant un cadre légal particulier entrainant la modification du contexte politique.

3.1.4 ENISA

Cette avant dernière partie de l'analyse sera consacrée à l'ENISA, l'agence européenne chargée de la sécurité des réseaux et de l'information. L'analyse s'effectuera en deux temps. Premièrement, elle se concentrera sur la gestion et la régulation de l'ENISA et de ses objectifs

[265] Commission européenne (2013b), *op.cit.*
[266] Journal officiel de l'Union européenne (2013), *op.cit.*
[267] Journal officiel de l'Union européenne (2005), *op.cit.*

par les Institutions européennes. Dans un second temps, l'analyse portera sur les comportements de l'Agence en sa qualité de méta-gouvernant.

Le premier aspect analysé se rapporte à la modification du mandat de l'ENISA, et plus précisément concernant la durée de vie de l'Agence, via la modification du règlement l'instituant.[268] Ainsi, par deux fois, en 2008 et 2011, le mandat de l'ENISA fut prolongé via le même mode opératoire. La Commission adopte une proposition de règlement qu'elle transmet ensuite au Conseil et au Parlement européen qui l'adoptent et modifient de la sorte le règlement de base instituant l'Agence. Ce mode opératoire des Institution européennes relève du *Hands-off framing.* En effet, en prolongeant la durée du mandat de l'ENISA et en lui allongeant de la sorte sa durée d'existence, l'UE modifie le design institutionnel au sein duquel évoluent les acteurs et ce en prolongeant la présence d'un acteur clef de ce réseau, lui-même impliqué dans la méta-gouvernance comme il sera fait état plus tard. En 2013, l'ENISA subit une modification complète du règlement l'instituant.[269] Cette modification respecte encore une fois le *modus operandi* précédemment mis en lumière. Ce règlement est adopté par le Parlement européen et le Conseil suite à une proposition de la Commission.

Le second aspect analysé se rapporte à la production d'objectifs, et de recommandations à destination de l'ENISA. Ceux-ci sont pris par la Commission, le Parlement européen et le Conseil dans leurs différents documents adoptés. L'analyse ne s'effectuera pas mesures par mesures cela ne revêtant pour la suite de ce mémoire aucun intérêt. Les recommandations et mesures prises étant sensiblement semblables, seuls les modes opératoires seront identifiés et analysés. Ainsi, comme précédemment présenté, la Commission dans ses différents plans d'action adoptés émet une série de recommandations à l'intention de l'ENISA et notamment, oriente son travail vers le soutien aux Etats membres ainsi que vers une amélioration de la coopération entre les Etats concernant la préparation et la réponse aux incidents, via par exemple l'établissement de normes minimales de sécurité ou de feuilles de route. Ces mesures se retrouvent ensuite consacrées dans les résolutions du Parlement européen et du Conseil. De ces pratiques il est possible de mettre en lumière un type comportement se rapportant à la méta-gouvernance. Ainsi, la Commission via l'établissement d'objectifs généraux à destination de l'ENISA, à savoir, accroitre la sécurité et la protection des infrastructures d'information critiques via l'accroissement du soutien aux Etats membres par exemple s'inscrit dans une démarche dite de *Hands-off framing* exercé de manière « douce ». En effet, la contexte politique

[268] Journal officiel de l'Union européenne (2004), *op.cit*
[269] Journal officiel de l'Union européenne (2013b), *op.cit.*

au sein duquel évolue l'Agence n'est pas modifié via le design institutionnel mais via l'élaboration d'objectifs tout en laissant une liberté d'action dans l'accomplissement de ces derniers.
Deuxièmement, le Conseil et le Parlement européen consacrent les objectifs énoncés par la Commission via l'adoption de résolutions. L'ENISA se voit de la sorte invitée à collaborer et à coopérer avec les acteurs impliqués dans la PIIC et ce de manière légale. Ce mode opératoire peut être considéré également comme du *hands-off framing* au regard de la typologie d'Eva Sorensen dans le sens où il modifie également le contexte politique

Après s'être intéressée, dans sa première partie, à la méta-gouvernance exercée sur l'ENISA, la deuxième partie de l'analyse se concentrera sur la méta-gouvernance exercée cette fois par l'ENISA en vue d'améliorer l'efficacité du réseau et ainsi atteindre un niveau optimal en matière de protection des infrastructures d'information critiques. Ainsi, en réponse aux recommandations faites par les Institutions européennes et en réponse aux sollicitations des Etats membres, l'ENISA exerce son rôle de méta-gouvernant via divers *modus operandi.* Il est possible d'identifier les différents comportements recensés dans la typologie de Sorensen. Cependant, ces comportements se combinent au sein de mêmes entreprises de l'Agence. Aux fins de cette analyse, les comportements seront isolés mais il est important de garder en tête qu'en pratique ceux-ci sont combinés afin d'arriver à exercer le rôle de méta-gouvernant de la manière la plus efficace possible et ainsi arriver à une sécurité des IIC optimale.
Premièrement, nous pouvons mettre en lumière des comportements relevant du *storytelling.* En effet, comme consacré dans le règlement instituant l'agence[270] un des objectifs de celle-ci est de développer une culture de la cyber-sécurité. A cette fin, l'ENISA a publié une série de rapport concernant les menaces. L'agence émet également régulièrement des documents concernant les stratégies nationales afin d'informer tous les Etats membres des différentes avancées[271]. Les différentes publications cernant les bonnes pratiques à adopter, les critères minimums à adopter en matière de sécurité ou encore concernant la reconnaissance des IIC peuvent être comprises comme des actions de l'ENISA visant à induire dans le chef des Etats membres et des autres acteurs impliqués une certaine culture de la cyber-sécurité et plus particulièrement de la sécurité et de la protection des infrastructures critiques. Une dernière action entreprise par l'ENISA est l'élaboration d'un exercice paneuropéen de réaction à divers cyber-incidents. Cet exercice avait entre autre objectif d'amener les Etats membres à prendre

[270] Journal officiel de l'Union européenne (2004), *op.cit.*
[271] www.Enisa.europa.eu/publications

conscience du nombre de menaces pesant sur les systèmes, des lacunes en matière de sécurité dans ces systèmes, mais également de mettre en lumière les relations d'interdépendance existant entre les Etats-membres et le besoin d'aide mutuelle afin de parvenir à un niveau élevé de sécurité.
Ces pratiques, au regard des caractéristiques relevées par Sorensen dans la pratique du *storytelling*, s'inscrivent pleinement dans ce mode opératoire. En effet, la construction d'image commune, la construction de relations et la mise en lumière de celles-ci sont des caractéristiques appartenant à la pratique du s*torytelling* et qui se retrouvent dans les actions de l'ENISA.

Comme précisé ci-dessus, les différents modes opératoires seront isolés et ce, au sein des mêmes actions entreprises par l'Agence. Ainsi, il est possible de mettre en lumière, après les pratiques relevant du *storytelling,* des pratiques relevant du *framing.* Si l'on reprend les caractéristiques données par Sorensen concernant ce mode opératoire, on retrouve la modification des règles du jeu, ou encore la définition d'objectif généraux.
Ainsi via ses publications, notamment les feuilles de routes, la méthodologie de reconnaissance des infrastructures d'information critiques, le guide des bonnes pratiques concernant les exercices nationaux, l'Agence instaure un cadre d'action, de nouvelles règles et de nouvelles directions à prendre par les Etats membres afin d'atteindre les objectifs finaux du réseau, la résilience et la protection des ICC. L'Agence a également mis en place un partenariat public-privé, l'EP3R. cette plateforme modifie également les règles du « jeu » en offrant une arène de débat entre le secteur public et privé afin de parvenir à des solutions de sécurité répondant aux besoins de tous les acteurs impliqués.

Troisièmement, si les premiers comportements étaient d'ordre *Hands-off* en raison du caractère indirect des interactions avec les acteurs, l'ENISA agit également de manière *Hands-on.*
Premièrement, et selon les recommandations des institutions européennes, l'ENISA doit soutenir les Etats membres, ceux-ci peuvent solliciter l'aide de l'Agence dans leurs diverses entreprises concernant la sécurité des ICC. L'ENISA a donc soutenu les Etats-membres, quand ceux-ci en faisaient la demande, dans l'élaboration de leurs stratégies de cyber-sécurité. L'Agence fournit un soutien de type expertise, en effet, en mettant à disposition des Etats membres et des autres parties prenantes à la protection des IIC ses recherches, ses analyses, l'ENISA met à disposition son expertise, une de ses principales ressources, afin de soutenir les Etats dans l'établissement de plan de protection nationaux efficaces.

Le dernier comportement identifié est celui de la participation. L'exemple le plus probant dans cette recherche est celui de l'exercice paneuropéen de protection des infrastructures d'information critiques. Si, effectivement, l'ENISA répond à une demande des Etats membres dans l'aide à la préparation de cet exercice.[272], et vient soutenir cette initiative. Elle fait, en fait, plus que soutenir l'initiative. En effet, elle participe activement à l'élaboration de cet exercice et s'y implique avec les Etats membres notamment dans l'organisation des différents *workshops* et la participation active lors de l'exercice et ensuite des conclusions à tirer de ce dernier.

Plusieurs éléments ressortent de cette analyse consacrée à l'ENISA. Premièrement, l'Agence fait l'objet d'acte de méta-gouvernance de la part des Institutions européennes et ce via des procédés relevant du *hands-off storytelling,* notamment via la modification du règlement instituant l'agence ou en lui fixant des objectifs généraux.
Deuxièmement, l'ENISA se révèle être un acteur clef dans la méta-gouvernance exercée par l'UE. En effet, si l'on peut identifier des comportements d'ordre *hands-off,* ce sont ceux relevant de modes opératoires *hands-on* qui confèrent à l'ENISA ce rôle d'acteur clef. L'Agence régule le réseau en étant en interaction directe avec les acteurs, en facilitant et supportant leurs entreprises ou en participant directement comme acteur à part entière de ce réseau.

3.1.5 Autres

Cette dernière partie de l'analyse s'intéressera aux trois derniers éléments relevant de la méta-gouvernance identifiés dans le chapitre précédent.
Le premier à faire l'objet de l'analyse est la décision-cadre de 2005[273] adoptée par le Conseil et relative à l'identification et aux sanctions en matière d'attaque des systèmes d'information. Par cette directive le Conseil vise l'harmonisation des cadre légaux nationaux en matière d'attaque contre les systèmes d'information ainsi qu'à accroitre la coopération des Etats membres. Cette directive, à l'instar des directives précédemment analysées et à destination des Etats membres. Cette démarche du Conseil peut être considérée comme un comportement relevant du *hands-on framing* exercé de manière forte car elle opère un design institutionnel et modifie de la sorte le contexte politique au sein duquel évoluent les acteurs impliqués dans la sécurité des systèmes d'information.

[272] ENISA (2010a), *op.cit.*
[273] Journal officiel de l'Union européenne (2005), *op.cit.*

Le deuxième élément à être analysé est une communication de la Commission adoptée en 2006[274]. Par cette dernière, la Commission veut introduire un nouveau système de gouvernance basé sur le dialogue, le partenariat et la responsabilisation. Pour ce faire, la Commission identifie dans un premier temps les lacunes en sécurité existant au niveau européen et national et tente de démontrer les interdépendances existant entre les différents acteurs impliqués dans ce système de gouvernance. Ensuite elle propose un cadre d'action en invitant les différents acteurs à collaborer ensemble dans divers domaines comme le partage d'information par exemple. Ce document est à destination des toutes les parties prenantes. Par l'adoption de ce dernier, la Commission exerce son rôle de méta-gouvernant de deux manières. Premièrement il est possible de mettre en lumière un comportement relevant du *hands-off storytelling.* En effet, en vue d'amener les acteurs à avancer dans une direction commune, la Commission identifie les menaces potentielles ainsi que les relations entre acteurs pouvant mener à une meilleure préparation à y faire face. De la sorte, la Commission construit des relations « amis-ennemis » et induit dans le chef des acteurs une possibilité de faire face à ces risques en collaborant. Cette pratique, réponds aux éléments relevant du *storytelling* identifiés par Sorensen. Dans un second temps, la Commission place un cadre d'action et ce, en invitant les acteurs à suivre ses recommandations. Par cette pratique, la Commission tente de modifier le contexte politique au sein duquel évoluent les acteurs impliqués dans la sécurité des systèmes d'information en leur fixant des objectifs généraux tout en laissant la liberté d'action en vue de rejoindre ces derniers. Cette pratique est assimilée à du *hands-off framing* exercé de manière douce au regard de la typologie de Sorensen.

Le troisième et dernier élément à faire l'objet de cette analyse est une résolution adoptée en 2007 par le Conseil[275]. Celle-ci fait suite à la Communication précédemment analysée et en consacre une série de mesures. De la sorte, le Conseil entend enjoindre les acteurs visés par les différentes mesures à les mettre en œuvre en vue d'arriver à une efficacité maximale du réseau d'acteurs et, de la sorte, élever le niveau de sécurité des systèmes d'information. En agissant de cette manière, le Conseil modifie le contexte politique au sein duquel évoluent les acteurs. Cette pratique relève du *hands-off framing* au regard de la typologie d'Eva Sorensen.

[274] Commission des communautés européennes (2006b), *op.cit.*
[275] Journal officiel de l'Union européenne (2007), *op.cit.*

De cette dernière partie d'analyse il est possible de ressortir les éléments suivants. Comme pour les parties précédentes, la Commission agit de manière *hands-off* et ce, via les procédés relevant du *framing* et du *storytelling*
Le conseil exerce sa méta-gouvernance de nouveau à la suite d'une proposition de la Commission selon un mode opératoire relevant du *hands-off framing.*
Outre la directive du Conseil étant à destination des Etats-membres, les deux autres mesures le sont à destination de toutes les parties prenantes.

Cette analyse touche à sa fin, en guise de conclusion de cette dernière un tableau récapitulatif des différents éléments analysés est dressé. Les différents comportements relevant de la méta-gouvernance mis en lumière dans cette partie serviront d'éléments fondamentaux à la poursuite de l'objet de ce mémoire, à savoir, comprendre comment l'Union européenne parvient à exercer son rôle de méta-gouvernant sur les acteurs impliqués dans la protection des infrastructures d'information critiques.

Pour conclure cette partie consacrée à l'analyse, un récapitulatifs des principaux éléments mis en lumière sera effectué. Ainsi plusieurs comportements ont pu être observé.
Premièrement, il ressort de cette analyse que la Commission agit principalement de manière *hands-off* via des modes opératoires relevant du *storytelling et du framing*, en adoptant des plans d'actions, des stratégies ou encore des programmes en matière de protection des IC.
Deuxièmement, le Parlement européen et le Conseil agissent dans la foulée de la Commission et consacrent les mesures que celle-ci présente, par l'adoption de résolution ou de directives. En agissant de la sorte, les deux institutions exercent la méta-gouvernance selon le mode opératoire dit du *hands-off framing.*
Troisièmement, l'ENISA, en tant que méta-gouvernant, agit à la fois de manière *hands-on* et *hands-off.* Ses actions menées en interaction directe avec les acteurs lui confèrent une importance capitale dans la régulation du réseau d'acteurs impliqués dans la PIIC. En effet, l'ENISA participe à ce réseau activement et soutien les entreprises des Etats membres en vue d'améliorer la sécurité et la protection des infrastructures.

3.2 Réponse aux Hypothèses

Cette dernière section du chapitre sera consacrée à la réponse aux hypothèses précédemment énoncées. Celles-ci sont au nombre de trois et sont les suivantes : 1) L'Union européenne (sous-entendu ici la Commission, le Parlement européen et le Conseil) assure, seule, la régulation du réseau d'acteurs impliqués dans la protection des infrastructures d'information critiques ; 2) Chaque Institution exerce une fonction propre en tant que méta-gouvernant du réseau d'acteurs impliqués dans la protection des infrastructures d'information critiques ; 3) L'Union européenne (sous-entendu ici, les Institutions (Conseil, Parlement et Commission ainsi que l'Agence en charge de la sécurité des réseaux et de l'information – ENISA) exerce son rôle de méta-gouvernant de manière hands-on, en interaction directe avec les acteurs impliqués dans la protection des infrastructures d'information critiques.

Avant de poursuivre cette partie il est important de préciser que les éléments employés afin de répondre aux différentes hypothèses émanent des mesures et actions entreprises officiellement par l'Union européenne en sa qualité de méta-gouvernant. Les actions et mesures émanant d'interactions informelles ne seront pas prises en compte dans ce mémoire. En effet, en raison du caractère sensible du sujet abordé dans ce mémoire, toutes nos demandes d'entrevue, de manière formelle ou informelle se sont vues refusées. La réponse reflètera donc uniquement le actions publiquement présentées et entreprises par l'Union européenne, ce qui constitue, comme précédemment mentionné, une des principales limites de ce mémoire. Cette précision effectuée, les réponses aux différentes hypothèses peuvent à présent être formulées.

3.2.1 Hypothèse 1 : L'Union européenne (sous-entendu ici la Commission, le Parlement européen et le Conseil) assure, seule, la régulation du réseau d'acteurs impliqués dans la protection des infrastructures d'information critiques.

Cette hypothèse concerne la capacité de méta-gouvernance des institutions européennes. Par celle-ci, il sera tenté de juger la capacité de la Commission, du Parlement et du Conseil à exercer seul ce rôle de méta-gouvernant.

Ainsi, comme il au regard des éléments ressortis de l'analyse, il est clair que les Institutions européennes sont les seuls acteurs à exercer ce rôle de régulateur du réseau de protection des

infrastructures d'information critiques et ce, via divers modes opératoires. Premièrement la Commission a régulièrement présenté des communications adoptant de plans et une série de mesures. Ces dernières visant à introduire un cadre d'action propice à la bonne mise en œuvre des mesures et entreprises dans le but d'accroitre le niveau de protection des infrastructures critiques. Preuve en est, le programme européen de protection des infrastructures critiques (2006)[276], le Plan de protection des infrastructures d'information critiques (2009)[277] ou encore la Stratégie européenne de cyber-sécurité (2013)[278]. La Commission a également tenté de réguler ce réseau via une certaine construction d'objectifs communs en amenant les différentes parties prenantes à prendre conscience du gain potentiel en efficacité qui pouvait être atteint en améliorant la coopération et le partage d'information notamment, ou encore en identifiant les menaces pesant sur chacun des acteurs et le danger que présentait ne fut-ce qu'une défaillance d'un de ceux-ci tant les interdépendances sont fortes à l'heure d'un monde interconnecté.

Le Conseil et le Parlement ne sont pas en reste et viennent appuyer le travail de la Commission en institutionnalisant les mesures prises par celle-ci. Preuve en est la décision-cadre de 2005[279] et sa modification en 2013[280]. Ou encore les différentes résolutions et directives à la suite des communications de la Commission comme par exemple la résolution du conseil de 2009 concernant une approche européenne concertée en matière de sécurité des réseaux de l'information[281]

Cependant, ces modes opératoires s'effectuent de manière *hands-off*, sans interactions directes avec les acteurs impliqués dans la protection des infrastructures d'information critiques. De plus, les mesures contraignantes ne le sont qu'à destination des Etats-membres, or comme il a été mentionné dans les différents plan de la Commission, le secteur privé joue un rôle essentiel dans la sécurité des infrastructures critique.

Il en résulte qu'un acteur clef, au niveau européen, s'érige comme un élément indispensable à l'exercice de la méta-gouvernance par l'Union européenne. Cet acteur, l'ENISA, fut créé en 2004 et endosse depuis un rôle de bras opérationnel de l'Union européenne concernant la régulation de la gouvernance de la protection des infrastructures critiques. En effet, comme il l'a été démontré dans ce mémoire, nombre de mesures prises par les Institutions européennes, le sont en direction de l'Agence. Cette dernière, suivant ces recommandations, opère en

[276] Commission des Communautés européennes (2006a), *op.cit.*
[277] Commission des Communautés européennes (2009), *op.cit.*
[278] Commission européenne (2013a), *op.cit.*
[279] Journal officiel de l'Union européenne (2005), *op.cit.*
[280] Journal officiel de l'Union européenne (2013), *op.cit.*
[281] Journal officiel de l'Union européenne (2009), *op.cit.*

interaction directe avec les acteurs impliqués dans ce système de gouvernance. Ainsi, elle offre un support en matière d'expertise au Etats-membres dans l'élaboration de stratégies nationales par exemple. Mais l'Agence participe également comme acteur à part entière du réseau notamment via l'élaboration d'exercices paneuropéens et la participation à ces derniers.
Dès lors, il est opportun d'apporter une réponse nuancée à cette hypothèse. En effet, au regard des éléments susmentionnés, l'UE peut exercer seule son rôle de méta-gouvernant, dans le cas où l'agence est comprise dans ce qui est entendu par l'UE. Si seuls le Conseil, la Commission et le Parlement européen sont pris en compte, l'UE ne peut exercer seule cette régulation car elle ne peut agir, ou en moindre mesure, de manière directe sur les interactions entre les parties prenantes.

3.2.2 Hypothèse 2 : Chaque Institution exerce une fonction propre en tant que méta-gouvernant du réseau d'acteurs impliqués dans la protection des infrastructures d'information critiques.

Cette seconde hypothèse s'intéresse au rôle exercé par chacun des acteurs européens dans l'exercice de la méta-gouvernance. Ces acteurs sont la Commission, le Conseil, le Parlement européen et finalement l'ENISA.
De l'analyse, il ressort clairement des rôles distincts pour chaque méta-gouvernant. Premièrement, la Commission établit des stratégies et des plans d'action au sein desquels elle identifie les menaces auxquelles doivent faire face les infrastructures critiques ainsi que les possibles solutions en vue d'y faire face de manière optimale. Pour ce faire, la Commission introduit un cadre d'action au sein duquel elle identifie les acteurs devant coopérer et les matières dans lesquelles ces derniers doivent collaborer. Elle adopte ensuite des plans d'action, programmes ou stratégies au sein desquels elle présente une série de mesures à prendre en vue d'une mise en œuvre optimale et *in fine* atteindre un niveau de sécurité élevé. En agissant de la sorte, la Commission adopte principalement des comportements de méta-gouvernance relevant du *hands-off framing* exercé de manière douce et de *hands-off storytelling.*
Le Parlement européen et le Conseil agissent, eux, dans les différents plans exposés, à la suite des communications de la Commission. Ainsi, ces derniers adoptent dans leurs directives, les

mesures à destination des Etats membres et dans leurs résolutions les mesures à destination de toutes les parties prenantes. Ces deux Institutions viennent appuyer la Commission dans l'élaboration de ses plans d'action en institutionnalisant les différentes mesures et en leur donnant un caractère contraignant, notamment dans le chef de celle à destination des Etats membres. De la sorte, le Parlement européen et le Conseil adoptent un mode opératoire de la méta-gouvernance d'ordre *hands-off framing* exercé de manière forte.

Un mode de fonctionnement similaire a pu être mis en lumière concernant la gestion de l'ENISA. Notamment dans la prolongation de ses mandats pour laquelle le Parlement européen et le Conseil agissaient à la suite de l'adoption par la Commission de communications proposant un texte législatif, en l'occurrence un règlement. Ce dernier étant *in fine* adopté par le Conseil et le Parlement européen.

Concernant l'Agence européenne en charge de la sécurité des réseaux et de l'information, comme il a déjà été fait état dans la section précédente, cette dernière joue un rôle capital dans l'exercice de la méta-gouvernance. En effet, comme il a été démontré dans l'analyse, l'ENISA endosse le rôle de bras opérationnel de l'UE dans le cadre de l'exercice de la méta-gouvernance. A ce titre, elle combine les quatre modes opératoires identifiés par Sorensen. Le principal rôle de l'ENISA est d'interagir directement avec les acteurs impliqués dans la protection des infrastructures d'information critiques. Ainsi elle leur offre un soutien en mettant à disposition des Etats membres ses ressources en termes d'expertise.

La réponse à cette hypothèse concernant les rôles des acteurs européens dans la méta-gouvernance semble claire. Pris isolément, chacun des acteurs joue un rôle bien précis, ces rôles étant complémentaires et indissociables en vue de l'exercice optimal de la régulation du système de gouvernance de la protection des infrastructures d'information critiques

3.2.3 Hypothèse 3 : L'Union européenne (sous-entendu ici, les Institutions (Conseil, Parlement et Commission ainsi que l'Agence en charge de la sécurité des réseaux et de l'information – ENISA) exerce son rôle de méta-gouvernant de manière hands-on, en interaction directe avec les acteurs impliqués dans la protection des infrastructures d'information critiques.

Cette troisième et dernière hypothèse s'intéresse à l'exercice de la méta-gouvernance via les modes opératoires dits *hands-on.* C'est-à-dire, des modes opératoires au sein desquels le

méta-gouvernant interagit directement avec les acteurs du réseau. Comme cela a été précédemment mentionné, les éléments de réponses sont issus de documents et mesures officielles adoptées par les Institutions européennes et l'ENISA, la réponse à cette hypothèse ne tiendra compte ici que de ces actions et en aucun cas de relations informelles pouvant être entretenues entre les méta-gouvernant et les autres parties prenantes au réseau. Des éléments de réponse ont déjà été apporté dans les deux hypothèses précédentes. Ainsi, comme il a été démontré, outre la Commission qui a financé des projets prototypes en matière de partage d'information, un seul acteur exerce la méta-gouvernance en étant en interaction directe avec les acteurs composant le réseau et y prenant également part. Cet acteur étant l'Agence européenne chargée de la sécurité des réseaux et de l'information, l'ENISA.

En effet, il ressort de l'analyse que l'ENISA est sollicitée par les Etats-membres afin d'apporter un soutien dans l'élaboration de stratégies nationales de sécurité des réseaux ou encore en matière de reconnaissance et d'indentification des infrastructures critiques. Ainsi, l'ENISA a mis à disposition des Etats ses ressources et en particulier celles relevant de l'expertise. De plus, outre la production de documents visant à aider les Etats membres dans leurs entreprises, l'ENISA a également pris part au réseau et ce, comme un acteur à part entière. L'exemple de l'exercice paneuropéen de protection des infrastructures d'information critiques en est l'élément le plus probant. En effet, l'Agence collabore directement avec les Etats membres lors de la préparation de cet exercice, les accompagne dans la mise en œuvre de celui-ci ainsi que dans les conclusions à en tirer.

De nouveau, la réponse à cette hypothèse doit être nuancée. En effet, s'il parait clair que l'Union européenne exerce également la méta-gouvernance via des procédés d'ordre *hands-on*, ceux-ci sont effectués par l'Agence européenne en charge de la sécurité des réseaux et de l'information. Le Conseil, le Parlement européen et la Commission, exerçant eux cette méta-gouvernance presque uniquement de manière *hands-off*, l'exception étant le soutien financier de la Commission à certains projets.

En guise de conclusion, un constat général concernant les acteurs visés par cette méta-gouvernance sera effectué. Ainsi, qu'importe la manière dont la méta-gouvernance est exercée, les actions et les mesures prises dans le cadre de celle-ci le sent principalement à destination des autorités publiques et d'organismes nationaux ou européens relevant du secteur public. Le constat est donc fait que via les mesures officielles, l'UE a champ d'action restreint concernant

le secteur privé. Or celui-ci, comme la Commission l'a notamment rappelé, et ce, à plusieurs reprises dans ses communications, est d'une importance capitale dans la protection des infrastructures d'informations critiques.

Conclusion

Ce mémoire touche à présent à sa fin. Un récapitulatif des éléments présentés sera effectué préalablement à la réponse à la question de départ de ce mémoire.

Ainsi l'objet de ce mémoire était la régulation, par l'Union européenne, du réseau d'acteurs impliqués dans la protection des infrastructures d'information critiques. La sécurité de ces infrastructures est d'une importance capitale pour nos sociétés. En effet, une défaillance ou la destruction d'une de ces infrastructures entrainerait de graves conséquences sur le fonctionnement des Etats ainsi que sur le bien-être des citoyens. Afin d'atteindre un niveau de protection optimal de ces infrastructures, il est nécessaire d'avoir une politique européenne coordonnée ainsi que des stratégies nationales harmonisées. A ces fins, les Institutions européennes ont élaboré une série de plan d'action, de programme et de stratégie concernant la protection des infrastructures critiques et la cyber-sécurité en général. Ces mesures sont prises dans le but d'amener les acteurs impliqués dans le domaine à agir dans une direction commune et non plus seulement en fonction de leurs intérêts individuels. Le propos de ce mémoire est justement de comprendre comment l'Union européenne parvient à effectuer cette régulation. Afin d'y parvenir, ce mémoire a présenté trois faits importants en matière de gestion du réseau : Le programme de protection des infrastructures critiques, le plan d'action de protection des infrastructures d'information critiques, la stratégie européenne de sécurité de 2013. A ces trois faits importants à mettre à l'actif de l'UE s'ajoutent une partie consacrée à l'ENISA, sa régulation ainsi que ses actions en tant que méta-gouvernant. Finalement une dernière partie concernant une série de mesures ayant un intérêt en termes de méta-gouvernance a été présentée.

Afin d'analyser ces différents éléments et ainsi comprendre comment l'UE parvient à effectuer cette régulation, ce mémoire s'est basé sur les théories de la méta-gouvernance et en particulier sur la typologie des modes d'action donnée par Eva Sorensen. Elle identifie quatre *modus operandi*. Le *hands-off framing,* le *Hands-off storytelling,* le *Hands-on support and facilitation* et finalement le *hands-on participation.*

L'analyse fut orientée en fonction des trois hypothèses de ce mémoire, à savoir, 1) L'Union européenne (sous-entendu ici la Commission, le Parlement européen et le Conseil) assure, seule, la régulation du réseau d'acteurs impliqués dans la protection des infrastructures d'information critiques ; 2) Chaque Institution exerce une fonction propre en tant que méta-gouvernant du réseau d'acteurs impliqués dans la protection des infrastructures d'information critiques ; 3) L'Union européenne (sous-entendu ici, les Institutions (Conseil, Parlement et

Commission ainsi que l'Agence en charge de la sécurité des réseaux et de l'information – ENISA) exerce son rôle de méta-gouvernant de manière hands-on, en interaction directe avec les acteurs impliqués dans la protection des infrastructures d'information critiques.

Il ressort de cette analyse plusieurs éléments. Premièrement, Les trois institutions européennes, seules, ne peuvent mener à bien la régulation du réseau d'acteur. C'est pourquoi l'Agence européenne chargée de la sécurité des réseaux de l'information a été instituée. Deuxièmement, il ressort que dans l'exercice de la méta-gouvernance, chaque acteur (Commission, Parlement européen, Conseil et ENISA) joue un rôle bien précis. En effet, la Commission présente et adopte les différents programmes et stratégies ainsi que différentes recommandations en vue de la mise en œuvre de ceux-ci. A la suite du travail de la Commission, le Parlement européen et le Conseil adoptent des directives et des résolutions donnant un caractère contraignant à une série de mesures présentées par la Commission. Les directives sont destinées exclusivement aux Etats membres. Les résolutions sont, elles, destinées à l'ensemble des parties prenantes. L'ENISA, elle, agit au sein du réseau, suivant les recommandations des institutions européennes, afin de soutenir et de faciliter le travail des Etats membres et des autorités compétentes en matière de protection des infrastructures d'information critiques. L'agence peut être considérée comme le bras opérationnel de l'UE, dans l'exercice de la méta-gouvernance. En effet, c'est le seul acteur à agir au plus près des acteurs en interaction directe avec ceux-ci. Cependant, il ressort également de l'analyse qu'un acteur est peu visé par la méta-gouvernance. En effet, les mesures sont principalement prises à destination des acteurs du secteur public. Or, le secteur privé détient et exploite majoritairement les IIC et est donc un acteur clef dans la protection de ces dernières.

Ces éléments permettent de répondre à la question principale de ce mémoire qui est : « Comment l'Union européenne régule-t-elle le réseau d'acteurs impliqués dans la mise en œuvre des politiques de protection des infrastructures d'information critiques ? »

Il est important de rappeler que ces éléments de réponse ne tiennent compte que des mesures prises officiellement par l'UE et ne tiennent en aucun cas compte des interactions informelles pouvant survenir entre les différents acteurs et le méta-gouvernant.

Ce mémoire de recherche offre une analyse de l'exercice de la méta-gouvernance par l'Union européenne sur un réseau composé de multiples acteurs issus des secteurs public et privé. Ont été mis en lumière divers mode opératoires se répétant successivement durant le laps de huit ans analysé. Ce mémoire a également mis en lumière une autre question qui n'a pas fait l'objet d'une recherche dans ce mémoire. Ainsi, il est pertinent de se demander pourquoi, alors que l'importance de la sécurité de ces infrastructures est capitale pour le bon fonctionnement de

notre société, les acteurs impliqués dans la protection des infrastructures d'information critiques ne fournissent pas plus d'efforts afin d'améliorer le niveau de protection et ce, sans l'intervention de l'Union européenne.

Les technologies de l'information prenant de plus en plus de place dans notre société, les interdépendances s'accroissant dû à l'inter-connectivité de plus en plus importante et les menaces pesant sur celles-ci se diversifiant au gré des évolutions technologiques[282], l'importance du travail de méta-gouvernant exercé par l'Union européen sera de plus en plus important afin de garantir la sécurité des citoyens et leurs bien-être.

[282] Commission européenne (2013a), *op.cit.*

Bibliographie

Ouvrages

- CHHOTRAY V. and STOKER G. (2009), *governance theory and practice : a cross-disciplinary approach*, Palgrave Macmillan, New York,
- CHRISTOU G. (2016), *Cybersecurity in the European Union – Resilience and Adaptability in Governance Policy*, Palgrave Macmillan, London
- HERMET G., BADIE B., BIRNBAUM P., BRAUD P. (2005), Dictionnaire de la science politique et des institutions politiques, 6e édition, ARMAND COLIN, Paris
- HOOD C. and MARGETTS H. (2007), *The Tools of Government in the Digital Age*, Palgrave Macmillan, London,
- JON P. (2000), *Debating governance: Authority, Steering, and Democracy*, Oxford University Press, New-York
- KOOIMAN J. (1994), *Modern governance : new government society interactions*, SAGE, London
- KOOIMAN J. (2003), *Governing as governance*, SAGE, London
- LEVI-FAUR D. (2012), *The oxford Handbook of governance*, Oxford University Press, Oxford
- R.A.W. RHODES (1997), *Understanding Governance, Policy networks, Governance, Reflexivity and Acountability*, Open University Press, Buckingham
- ROSENAU J. and CZEMPIED E.-O. (1992), *Governance without government: order and change in world politics*, University Press, Cambridge
- TORFING J. and SORENSEN E. (2008), *Theories of democratic network governance*, Palgrave MacMilllan, Basingstoke (Version papier + version Kindle)

Articles scientifiques

- AGRANOFF R. And MCGUIRE M. (2001), *Big questions in public management research, in, Journal of public administration research and theory* : J-Part, Vol 11, N°3 pp 295-326
- BAKER K and STOKER G (2012), *Metagovernance and nuclear power in Europe*, *in* Journal of European Policy, 19:7, pp 1026-1051

- BLANCO I. LOWNDES V. PRATCHETT L. (2009), *Policy networks and governance Networks : Towards a greater conceptual clarity,* in Political Studies Review, vol 11, pp 297-308
- BORZEL A.T. (2012), *The European union – a unique governance mix? , in*, *LEVI-FAUR D.* (2012),, *the oxford Handbook of governance,* Oxford University Press, OXFORD, ch 43
- KLIJN E.-H., STEIJN B. and EDELENBOS J. (2010), *The impact of network management on outcomes in governance networks*, in Public administration, vol 88, No.4, Blackwell, OXFORD, pp 1063-1082
- GUY PETERS B. (2012*), Governance as Political theory, in LEVI-FAUR D.* (2012),, *the oxford Handbook of governance,* Oxford University Press, OXFORD, chapitre 25
- KLIJN E.-H. (2008), *governance and governance networks in Europe : an assessment of ten years of research on the theme, in* Public Management Review Vol 10 issue 4 pp 505-525
- KLIJN E.-H. (2008), *Governance and Governance Networks in Europe, an assessment of ten years of research on the theme, in ,* Public Management Review, Vol 10 : 4 : 2008, pp 505-525
- KLIJN E.-H. and EDELENBOS J. (2008), *Meta-governance as network management, in,* TORFING J. and SORENSEN E. (2008), *Theories of democratic network governance*, Palgrave MacMilllan, Basingstoke, ch 11
- KOOIMAN J. And JENTOFT S.(2009), *Meta-governance : values, norms and principles, and the making of hard choices", in* Public administration, Vol 87, No 4 pp. 818-836
- MCGUIRE M. (2002), *Managing networks : Propositions on what managers do and why they do it, in,* Public Administration Review Vol 62 n°5 pp 599-609

- MCGUIRE M. (2002), *Managing networks : Propositions on what managers do and why they do it, in,* Public Administration Review Vol 62 n°5 pp 599-609

- RHODES R.A.W. (2000), *Governance in public administration, in,* Jon Pierre (2000), *Debating governance: Authority, Steering, and Democracy,* Oxford University Press, New-York, chapitre 4
- RHODES R.A.W. (2012), *Waves of governance, in,* LEVY FAUR D (2012), *the oxford Handbook of governance,* Oxford University Press, OXFORD., ch 3

- ROSENAU J. (1992),*Governance, order and change in world politics*, *in*, ROSENAU J. and CZEMPIED E.-O. (1992), *Governance without government: order and change in world politics*, UNIVERSITY PRESS, 1992, CAMBRIDGE Ch 16
- SORENSEN E. (2006), *'Metagovernance: the changing role of politicians in processes of democratic choice'*, *in,* The American Review of Public Administration, 36(1):98–114
- SORENSEN E. and TORFING J. (2008) *Theoretical approches to metagovernance in* TORFING J. and SORENSEN E. (2008), *Theories of democratic network governance*, Palgrave MacMilllan, Basingstoke

Documents officiels

- Centre de documentation sommet G7-G8 (1998), Déclaration sur les drogues et la criminalité du 16 mai 1998, Document en ligne, URL : http://g7.sciencespo-lyon.fr/spip.php?article71
- Commission des Communautés européenne (2003), Proposition de règlement du Parlement européen et du Conseil instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information, COM(2003)63 final, Bruxelles
- Commission des Communautés européennes (2005), Livret vert sur un programme européen de protection des infrastructures critiques, COM(2005)576 final, Bruxelles
- Commission des Communautés européennes (2006a), Communication de la Commission sur un programme européen de protection des infrastructures critiques, COM(2006)786 final
- Commission des Communautés européennes (2006b), Communication de la Commission au Conseil, au Parlement européen, au Comité économique et social européen et au Comité des Régions sur une stratégie pour une société de l'information sûre –"Dialogue, partenariat et responsabilisation", COM(2006) 251 final, Bruxelles
- Commission des Communautés européennes (2007), Communication de la Commission au parlement européen et au Conseil sur l'évaluation de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), COM(2007) final, Bruxelles
- Commission des communautés européennes (2008), proposition de décision du Conseil relative au réseau d'alerte concernant les infrastructures critiques (CIWIN), COM(2008) 676 final, Bruxelles

- Commission des Communautés européennes (2009), Communication de la Commission au Parlement européen, au Conseil, au comité économique et social européen et au comité des régions relative à la protection des infrastructures d'information critiques : « protéger l'Europe des cyberattaques et des perturbations de grande envergure : améliorer l'Etat de préparation, la sécurité et la résilience », COM(2009)149 final, Bruxelles
- Commission européenne (2010), Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (CE° n°460/2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information en ce qui concerne sa durée, COM(2010) 520 final, Bruxelles
- Commission européenne (2010b), proposition de règlement du Parlement européen et du Conseil concernant l'Agence européenne chargée de la sécurité des réseaux et de l'information – ENISA, COM(2010)521, Bruxelles
- Commission européenne (2011), communication de la commission au parlement européen, au conseil, au comité économique et social européen et au conseil des régions relative à la protection des infrastructures d'information critiques "réalisation et prochaines étapes : vers une cybersécurité mondiale", COM(2011) 163 final, Bruxelles
- Commission européenne (2013a), 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, JOIN(2013) Final
- Commission européenne (2013b), 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)48 final, Bruxelles
- Conseil de l'Europe (1981), Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, STE n°108, Strasbourg
- Conseil de l'Europe (2001), Convention sur la cybercriminalité, STE n°185, Budapest
- ENISA (2009a), Baseline capabilities for national/governmental CERTs, version 1.0 (initial draft)
- ENISA (2009b), Baseline capabilities of national/governmental CERTs part 2: Policy Recomandations, version 1.0 (initial draft)
- ENISA (2009c), Resilient e-Communications Networks – Good practice guide on national exercices enhancing the resilience of public communications networks

- ENISA (2011a), EISAS- European information sharing and alert system for citizens and SMEs – a roadmap for further development and deployment
- ENISA (2012), Critical cloud computing – A CIIP perspective on cloud computing services, Version 1.0
- ENISA (2014), Methodologies for the identification of Critical Information Infrastructure assets and services – Guidelines for charting electronic data communication networks
- Journal officiel de l'Union européenne (2004), règlement (CE) n°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, Strasbourg
- Journal officiel de l'Union européenne (2005), Décision-cadre 2005/222/JAI du Conseil du 24 février 2005 relative aux attaques visant les systèmes d'information, Bruxelles
- Journal officiel de l'Union européenne (2007a), Résolution du Conseil du 22 mars 2007 relative à une stratégie pour une société de l'information sûre en Europe, (2007/C 68/01)
- Journal officiel de l'Union européenne (2007b), Décision du Conseil du 12 février 2007 établissant pour la période 2007-2013, dans le cadre du programme général « sécurité et protection des libertés » le programme spécifique « prévention, préparation et gestion des conséquences en matière de terrorisme et autres risques liés à la sécurité », Bruxelles
- Journal officiel de l'Union Européenne (2008a), Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection, Bruxelles
- Journal officiel de l'Union européenne (2008b), règlement (CE) N°1007/2008 du Parlement européen et du Conseil du 24 septembre 2008 modifiant le règlement (CE) N°460/2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information en ce qui concerne sa durée, Strasbourg
- Journal officiel de l'Union européenne (2009), Résolution du Conseil du 18 décembre 2009 sur une approche européenne concerté en matière de sécurité des réseaux et de l'information, 2009/C 321/01
- Journal officiel de l'Union européenne (2011), Règlement (UE) n°(80/2011 du Parlement européen et du Conseil du 8 juin 2011 modifiant le règlement (CE) n°460/2004 instituant l'Agence européenne charge de la sécurité des réseaux et de l'information en ce qui concerne sa durée, Strasbourg

- Journal officiel de l'Union européenne (2012), retrait de propositions de la Commission qui ne revêtent plus d'un caractère d'actualité, (2012/C J56/06)
- Journal officiel de l'Union européenne (2013a), Directive 2013/40/UE du Parlement européen et du Conseil du 12 aout 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil.
- Journal officiel de l'Union européenne (2013b), règlement (UE) n°526/2013 du Parlement européen et du Conseil du 21 mai 2013 concernant l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et abrogeant le règlement (CE) n°460/2004, Strasbourg
- Journal officiel des Communautés européennes (2002), directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive « cadre »)

Communiqués de presse

- ENISA (2010a), News item – first pan européan CIIP exercise, publié le 3 février 2010. URL : https://www.enisa.europa.eu/news/enisa-news/1st-pan-european-ciip-excercises, (consulté le 23 mai 2017)
- ENISA (2010b), News Item – towards the first pan européan CIIP exercise, publié le 15 mars 2010, URL : https://www.enisa.europa.eu/news/enisa-news/towards-the-1st-pan-european-ciip-exercise (consulté le 23 mai 2017)
- ENISA (2010c), News item – "cyber europe 2010" the first pan européen CIIP exercise, publié le 4 octobre 2010, URL : https://www.enisa.europa.eu/news/enisa-news/2018cyber-europe-20102019-the-1st-pan-european-ciip-exercise-phase-one, (consulté le 23 mai 2017)
- ENISA (2010d), Press release – First EU cyber security exercise "cyber Europe 2010" with >320 "incidents" successfully concluded, publié le 5 novembre 2010, URL : https://www.enisa.europa.eu/news/enisa-news/cyber-europe-20102019-cyber-security-exercise-with-320-2018incidents2019-successfully-concluded, (consulté le 23 mai 2017)
- ENISA (2011b), Press release – New guide on cyber security incident management to support the fight against cyber attacks, publié le 20 janvier 2011, URL :

https://www.enisa.europa.eu/news/enisa-news/new-guide-on-cyber-security-incident-management-to-support-the-fight-against-cyber-attacks, (consulté le 23 mai 2017)

- ENISA (2013), Press release – New Enisa report : the double-edged sword of cloud computing in Critical Information Infrastructure Protection, publié le 14 février 2013, URL : https://www.enisa.europa.eu/news/enisa-news/new-enisa-report--the-double-edged-sword-of-cloud-computing-in-critical-information-infrastructure-protection, (consulté le 23 mai 2017)

Sitographie

- www.consilium.europa.eu
- www.ec.europa.eu
- www.enisa.europa.eu
- www.eur-lex.europa.eu

Annexes

Annexe 1 – Plan d'action PIIC dans Communication COM(2009)149 final

5. LE PLAN D'ACTION

5.1. Préparation et prévention

Base commune de capacités et de services en vue d'une coopération paneuropéenne. La Commission invite les États membres et les parties concernées à:

- définir, avec l'appui de l'ENISA, un niveau minimum de capacités et de services pour les équipes d'intervention en cas d'urgence informatique (CERT) nationales ou gouvernementales et les opérations de réaction en cas d'incident, pour soutenir la coopération paneuropéenne;

- veiller à ce que les CERT nationales ou gouvernementales constituent un élément clé de la capacité nationale en matière de préparation, de partage d'information de coordination et de réaction.

Objectif: fin 2010 pour la définition commune de normes minimales, fin 2011 pour la mise en place de CERT nationales ou gouvernementales qui fonctionnent bien dans tous les États membres.

Partenariat public privé européen pour la résilience (EP3R). La Commission

- encouragera la coopération entre le secteur public et le secteur privé sur des objectifs liés à la sécurité et à la résilience, sur les exigences de base et sur l'adoption de bonnes mesures et pratiques politiques. Ce partenariat sera axé, en priorité, sur la dimension européenne envisagée sous les angles stratégique (bonnes pratiques politiques, par exemple) et tactique ou opérationnel (déploiement industriel). Il sera fondé sur des initiatives nationales existantes et sur les activités opérationnelles de l'ENISA et il les complétera.

Objectif: fin 2009 pour une feuille de route et un plan concernant le partenariat EP3R, mi-2010 pour l'établissement du partenariat, fin 2010 pour les premiers résultats.

Forum européen pour le partage d'information entre États membres. La Commission

- établira un forum européen permettant aux États membres d'échanger des informations et de bonnes pratiques politiques sur la sécurité et la résilience des infrastructures d'information critiques. Ce forum tirera parti des résultats des activités des autres organismes et en particulier de l'ENISA.

Objectif: fin 2009 pour le lancement du forum; fin 2010 pour les premiers résultats

5.2. Détection et réaction

Système européen de partage d'information et d'alerte (SEPIA) La Commission soutient:

le développement et le déploiement d'un système européen de partage d'information et d'alerte destiné aux citoyens et aux PME et fondé sur des systèmes nationaux et privés de partage d'information et d'alerte. La Commission soutient financièrement deux projets de prototypes complémentaires[27]. L'ENISA est invitée à faire l'inventaire des résultats de ces projets et d'autres initiatives nationales et à établir une feuille de route afin de promouvoir le développement et le déploiement du SEPIA.

Objectif: fin 2010 pour mener à bien les projets de prototypes, fin 2010 pour la feuille de route relative à un système européen.

5.3. Atténuation et récupération

Planification en cas d'urgence et exercices à l'échelon national. La Commission invite les États Membres à:

- élaborer des plans nationaux en cas d'urgence et organiser régulièrement des exercices portant sur la réaction en cas d'incident de grande envergure affectant la sécurité des réseaux et sur la récupération après défaillance grave, afin de renforcer la coordination paneuropéenne. Les CERT/CSIRT nationales ou gouvernementales pourraient être chargées d'organiser des exercices de planification d'urgence et de test à l'échelon national, avec la participation de parties intéressées des secteurs public et privé. L'ENISA est invitée à participer pour soutenir l'échange de bonnes pratiques entre États membres.

Objectif: fin 2010 pour l'organisation d'au moins un exercice à l'échelon national dans chaque État membre.

Exercices paneuropéens portant sur des incidents de grande envergure affectant la sécurité des réseaux. La Commission:

- soutiendra financièrement le développement d'exercices paneuropéens portant sur des incidents affectant la sécurité d'internet[28], qui pourront également constituer la base opérationnelle d'une participation paneuropéenne à des exercices internationaux sur des incidents affectant la sécurité des réseaux, tels que le «Cyber Storm» aux Etats-Unis.

Objectif: fin 2010 pour la conception et le lancement du premier exercice paneuropéen, fin 2010 pour une participation paneuropéenne à des exercices internationaux.

Renforcement de la coopération entre les CERT nationales/gouvernementales. La Commission invite les États Membres à:

- renforcer la coopération entre les CERT nationales/gouvernementales, le cas échéant en mettant à contribution et en développant des mécanismes de coopération existants tels que l'EGC (Groupe des CERT gouvernementales européennes)[29]. L'ENISA est invitée à s'employer activement à stimuler et à soutenir la coopération paneuropéenne entre CERT nationales/gouvernementales, qui devrait déboucher sur une meilleure préparation, sur une capacité européenne de réaction en cas d'incident renforcée et sur des exercices paneuropéens (et/ou régionaux).

Objectif: fin 2010 pour le doublement du nombre d'organismes nationaux participant à l'ECG; fin 2010 pour le développement par l'ENISA de matériel de référence destiné à soutenir la coopération paneuropéenne.

5.5. Critères pour les infrastructures critiques européennes dans le secteur des TIC

Critères spécifiques au secteur des TIC En se fondant sur la première activité déjà menée à bien en 2008, la Commission:

- continuera à élaborer, en coopération avec les États membres et toutes les parties concernées, les critères relatifs à l'identification des infrastructures critiques européennes dans le secteur des TIC. À cet effet, des informations pertinentes seront tirées d'une étude spécifique en cours de lancement[32].

Objectif: première moitié de 2010: définition par la Commission des critères pour les infrastructures critiques européennes dans le secteur des TIC.

Annexe 2 : Résolution du Conseil du 18 décembre 2009 sur une approche européenne concertée en matière de sécurité des réseaux et de l'information

des réseaux et des systèmes d'information;

11. qu'il est important d'étudier les effets, les risques et les perspectives stratégiques de la création d'équipes d'intervention en cas d'urgence informatique pour les institutions de l'UE et de réfléchir au futur rôle éventuel de l'ENISA dans ce domaine;

12. des travaux réalisés jusqu'à présent par l'ENISA dans le domaine de la sécurité des réseaux et de l'information et de la nécessité de continuer à développer cette agence pour en faire un organisme efficace apportant des avantages clairs dans le domaine de la sécurité des réseaux et de l'information;

V. SOULIGNE:

1. qu'une stratégie européenne renforcée et globale en matière de sécurité des réseaux et de l'information, avec des rôles clairement définis pour la Commission européenne, les États membres et l'ENISA, revêt une importance fondamentale pour relever les défis actuels et futurs;

2. qu'après une consultation et une analyse appropriées, il convient d'envisager, dans le cadre du processus législatif, la modernisation et le renforcement de l'ENISA en lui donnant un mandat qui autorise une certaine souplesse et permette aux États membres et à la Commission d'exercer une surveillance et aux représentants des parties prenantes du secteur privé de jouer un rôle efficace. Ce mandat devrait tenir compte du cadre réglementaire pour les réseaux et services de communications électroniques, être conforme aux ambitions définies dans le programme de Lisbonne et comprendre des objectifs liés à la recherche, à l'innovation, à la compétitivité, à la croissance économique et à l'instauration de la confiance;

VI. INVITE LES ÉTATS MEMBRES À:

1. poursuivre les travaux visant à renforcer la confiance des utilisateurs finaux dans les TIC par des campagnes de sensibilisation;

2. organiser des exercices nationaux et/ou participer à des exercices européens périodiques dans le domaine de la sécurité des réseaux et de l'information, en tenant compte de la nécessité d'une planification détaillée liée à la complexité du domaine et à la participation du secteur privé. L'ENISA pourrait, à leur demande, aider les États membres à cette fin. L'ampleur et la dimension géographique des exercices devraient évoluer naturellement dans le temps et reposer sur les risques reconnus;

3. créer des équipes d'intervention en cas d'urgence informatique dans les États membres qui n'ont pas encore mis en place une telle capacité et renforcer la coopération entre ces équipes à un niveau européen. L'ENISA pourrait aider les États membres à cette fin;

4. intensifier les efforts consacrés aux programmes d'éducation, de formation et de recherche en matière de sécurité des réseaux et de l'information afin de garantir la disponibilité au sein de l'UE des compétences techniques et des experts nécessaires et d'accroître le professionnalisme de ces derniers dans ce domaine;

5. réagir de concert en cas d'incident transfrontière et renforcer leur capacité à le faire de manière appropriée, ce qui requiert un renforcement du dialogue entre les décideurs concernés, en particulier sur les questions de confidentialité;

VII. INVITE LA COMMISSION À:

1. apporter, le cas échéant, un soutien aux États membres dans la mise en œuvre de la présente résolution;

2. informer régulièrement le Parlement européen et le Conseil des initiatives prises au niveau de l'UE dans le domaine de la sécurité des réseaux et de l'information;

3. en collaboration avec l'ENISA, lancer une campagne visant à sensibiliser le public européen et les acteurs privés à l'importance d'une gestion du risque appropriée dans le domaine de la sécurité des réseaux et de l'information;

4. continuer, en collaboration avec les États membres, à recenser les mesures susceptibles d'inciter les fournisseurs d'infrastructures de communications électroniques à offrir des infrastructures solides et résilientes aux utilisateurs finaux, aux entreprises et aux pouvoirs publics;

5. en collaboration avec les États membres, mettre au point des méthodes permettant une évaluation comparative au niveau de l'UE de l'impact socio-économique des incidents et de l'efficacité des mesures préventives;

6. encourager et améliorer les modèles multipartites, qui doivent apporter une valeur ajoutée manifeste pour les utilisateurs finaux et les entreprises;

7. présenter une stratégie globale en matière de sécurité des réseaux et de l'information (1), comprenant des propositions relatives à un mandat renforcé et souple pour l'ENISA et prévoyant une surveillance accrue des États membres et de la Commission;

8. réaliser une analyse, en collaboration avec les États membres, sur les équipes d'intervention en cas d'urgence informatique, afin de recenser les domaines dans lesquels une plus ample coopération est nécessaire;

9. poursuivre l'examen concernant la mise au point d'une approche commune ou interopérable pour les institutions de l'UE en ce qui concerne l'achat de systèmes et de services TIC sécurisés;

VIII. ENGAGE L'ENISA À:

1. continuer d'apporter un soutien actif aux États membres, à la Commission européenne et aux autres parties prenantes concernées dans la mise en œuvre des politiques européennes en matière de sécurité des réseaux et de l'information et du plan d'action pour la protection des infrastructures d'information critiques;

2. travailler en collaboration avec les États membres, la Commission et les organismes statistiques en vue de la mise au point d'un cadre de données statistiques sur l'état de la sécurité des réseaux et de l'information en Europe;

IX. INVITE LES PARTIES PRENANTES À:

1. intensifier leurs efforts pour renforcer le niveau de sécurité des réseaux et de l'information, notamment en ce qui concerne l'offre de produits et services fiables, dignes de confiance et faciles à utiliser;

2. informer les utilisateurs de manière adéquate des risques en matière de sécurité liés aux produits et services et des moyens de s'en protéger;

3. prendre toutes les mesures techniques et organisationnelles appropriées pour garantir la continuité, l'intégrité et la confidentialité des réseaux et services de communications électroniques;

4. poursuivre les travaux de normalisation dans le domaine de la sécurité des réseaux et de l'information afin d'essayer de trouver des solutions harmonisées et interopérables;

5. participer avec les États membres à des exercices afin de pouvoir réagir de manière appropriée aux urgences.

Annexe 3 : Plan d'action pour l'EPCIP dans Communication COM(2006)786 final

Le plan d'action pour l'EPCIP

Volet n° 1 – Stratégies consécutives de l'EPCIP

Le volet n° 1 servira de plate-forme stratégique pour la coordination et la coopération globales dans le cadre de l'EPCIP, qui seront assurées par le groupe de contact PIC de l'UE.

Phase 1

Action	Acteur	Calendrier
Recensement des secteurs prioritaires pour lesquels une action s'impose (Les secteurs des transports et de l'énergie figureront parmi les premières priorités)	Commission	dès que possible et ensuite sur une base annuelle
Élaboration de définitions de travail et d'une terminologie pour chaque secteur d'infrastructures critiques	Commission, États membres et autres acteurs concernés le cas échéant	au plus tard un an après l'entrée en vigueur de la directive sur les ICE
Définition de critères généraux à utiliser pour recenser les ICE	Commission, États membres et autres acteurs concernés le cas échéant	au plus tard un an après l'entrée en vigueur de la directive sur les ICE
Élaboration d'un inventaire des programmes nationaux, bilatéraux et communautaires de protection des infrastructures critiques	Commission et États membres	en cours
Élaboration et adoption de lignes directrices pour la collecte et l'utilisation de données sensibles par les acteurs concernés	Commission, États membres et autres acteurs concernés le cas échéant	en cours
Recensement des meilleures pratiques liées à la PIC, des outils et méthodes d'évaluation des risques	Commission, États membres et autres acteurs concernés le cas échéant	en cours
Commande d'études concernant les liens de dépendance	Commission, États membres et autres acteurs concernés le cas échéant	en cours

Phase 2

Action	Acteur	Calendrier
Détermination des failles pour lesquelles une initiative communautaire apporterait une valeur ajoutée	Commission, États membres et autres acteurs concernés le cas échéant	en cours
Le cas échéant, constitution de groupes d'experts sectoriels en matière de PIC au niveau de l'Union	Commission, États membres et autres acteurs concernés le cas échéant	en cours
Recensement des propositions d'actions en matière de PIC susceptibles d'être financées au niveau de l'Union	Commission et États membres	en cours
Premiers financements communautaires d'actions dans le domaine de la PIC	Commission	en cours

Phase 3

Action	Acteur	Calendrier
Lancement de la coopération avec des pays tiers et des organisations internationales	Commission et États membres	en cours

Volet n° 2 – Protection des infrastructures critiques européennes (ICE)

Le volet n° 2 tendra à réduire la vulnérabilité des ICE.

Phase 1

Action	Acteur	Calendrier
Définition de critères sectoriels à utiliser pour recenser les ICE	Commission, États membres et autres acteurs concernés le cas échéant	au plus tard un an après l'entrée en vigueur de la directive sur les ICE

Phase 2

Action	Acteur	Calendrier
Recensement et vérification secteur par secteur des infrastructures critiques susceptibles d'être classées comme ICE	Commission et États membres	au plus tard un an après l'adoption des critères pertinents, et ensuite à intervalles réguliers

Classement comme ICE	Commission et États membres	en cours
Recensement des points vulnérables, des menaces et des risques à l'égard de certaines ICE, et établissement de plans de sûreté pour les exploitants (PSE)	Commission, États membres, propriétaires/exploitants d'ICE (rapport général à la Commission)	au plus tard un an après le classement comme ICE
Évaluation de la nécessité de prendre des mesures de protection et des mesures au niveau de l'UE	Commission, États membres et autres acteurs concernés le cas échéant	au plus tard 18 mois après le classement comme ICE
Évaluation de l'approche adoptée par chaque État membre en ce qui concerne les niveaux d'alerte applicables aux infrastructures classées comme ICE. Lancement d'une étude de faisabilité relative à l'étalonnage ou à l'harmonisation de ces niveaux d'alerte.	Commission et États membres	en cours

Phase 3

Action	Acteur	Calendrier
Élaboration et adoption de propositions relatives à des mesures de protection minimales pour les ICE	Commission, États membres, propriétaires/exploitants d'ICE	après avoir apprécié la nécessité de prendre des mesures de protection et des mesures au niveau de l'UE
Mise en œuvre des mesures de protection minimales	États membres et propriétaires/exploitants d'ICE	en cours

Volet n° 3 – Soutien relatif aux ICN

Le volet n° 3 s'inscrit dans un cadre national et vise à aider les États membres à protéger leurs infrastructures critiques nationales.

Phase 1

Action	Acteur	Calendrier
Échange d'informations concernant les critères utilisés pour recenser les ICN	États membres (avec l'aide de la Commission, sur demande)	en cours

Phase 2

Action	Acteur	Calendrier
Recensement et vérification secteur par secteur des infrastructures critiques susceptibles d'être classées comme ICN	États membres et autres acteurs concernés le cas échéant	en cours
Classement de certaines infrastructures critiques comme ICN	États membres	en cours
Analyse par secteur des failles existantes en matière de sûreté des ICN	États membres et autres acteurs concernés le cas échéant (avec l'aide de la Commission, sur demande)	en cours

Phase 3

Action	Acteur	Calendrier
Conception et établissement de programmes nationaux de protection des infrastructures critiques	États membres (avec l'aide de la Commission, sur demande)	en cours
Conception de mesures de protection spécifiques pour chaque ICN	États membres, propriétaires/exploitants d'ICN (avec l'aide de la Commission, sur demande)	en cours
Suivi afin de vérifier que les propriétaires/exploitants mettent en œuvre les mesures d'application nécessaires	États membres	en cours

Annexe 4 : Procédure de recensement des ICE – Annexe directive 2008/114/CE

ANNEXE III

Procédure applicable en ce qui concerne le recensement par les États membres des infrastructures critiques pouvant être désignées parmi les ICE au titre de l'article 3

L'article 3 exige que chaque État membre recense les infrastructures critiques pouvant être désignées comme ICE. Cette procédure est mise en œuvre par chaque État membre en respectant la série d'étapes consécutives reprises ci-après.

L'ICE potentielle qui ne satisfait pas aux exigences de l'une des étapes successives ci-après est considérée comme «non ICE» et est exclue de la procédure. L'ICE potentielle qui répond aux définitions est soumise aux étapes suivantes de la présente procédure.

Étape 1

Chaque État membre applique les critères sectoriels afin d'opérer une première sélection parmi les infrastructures critiques existant au sein d'un secteur.

Étape 2

Chaque État membre applique la définition des infrastructures critiques visée à l'article 2, point a), à l'ICE potentielle recensée lors de l'étape 1.

La gravité de l'impact sera déterminée par application des méthodes nationales de recensement des infrastructures critiques ou sur la base des critères intersectoriels, à l'échelon national approprié. En ce qui concerne les infrastructures qui offrent un service essentiel, il sera tenu compte de l'existence de solutions de remplacement ainsi que de la durée de l'arrêt/de la reprise d'activité.

Étape 3

Chaque État membre applique l'élément transfrontalier de la définition d'ICE visée à l'article 2, point b), à l'ICE potentielle qui a franchi les deux premières étapes de la procédure. Si l'ICE potentielle répond à la définition, elle est soumise à l'étape suivante de la procédure. En ce qui concerne les infrastructures qui offrent un service essentiel, il sera tenu compte de l'existence de solutions de remplacement ainsi que de la durée de l'arrêt/de la reprise d'activité.

Étape 4

Chaque État membre applique les critères intersectoriels aux ICE potentielles restantes. Les critères intersectoriels tiennent compte des éléments suivants: la gravité de l'impact et, pour les infrastructures qui offrent un service essentiel, l'existence de solutions de remplacement, ainsi que la durée de l'arrêt/de la reprise d'activité. Les ICE potentielles qui ne répondent pas aux critères intersectoriels ne seront pas considérées comme étant des ICE.

L'identification des ICE potentielles qui franchissent toutes les étapes de cette procédure n'est communiquée qu'aux États membres susceptibles d'être affectés considérablement par lesdites infrastructures.