Etude sur
la cyberdéfense et la cybersécurité
au sein des institutions européennes

DELEGATION AUX AFFAIRES STRATEGIQUES
MINISTERE DE LA DEFENSE

La Délégation aux Affaires Stratégiques soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la DAS a confié à **Esteral Consulting** cette étude sur la cyberdéfense et la cybersécurité au sein des institutions européennes, sous le numéro de marché 1501839960.

Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère de la défense et des anciens combattants
Délégation aux Affaires Stratégiques
Sous-direction Politique et Prospective de Défense
14 rue St Dominique 75700 PARIS SP 07

Etude sur la cyberdéfense et la cybersécurité au sein des institutions européennes

Esteral Consulting

Novembre 2011
Ministère de la défense et des anciens combattants
DAS - Marché n°1501839960

Table des matières

Introduction

Le premier objectif de cette étude est de présenter de manière aussi complète que possible l'ensemble des activités des Institutions européennes en cybersécurité et cyberdéfense, en en montrant la portée mais aussi les limitations, disparités, redondances, voire incohérences.

Sur cette base, il s'agit ensuite de tracer quelques pistes sur les améliorations possibles à apporter à ce dispositif dans le sens d'une meilleure complémentarité entre activités nationales et activités européennes en allant dans le sens d'une « plus grande intégration ».

Après quelques éléments de cadrage, l'étude retrace la manière dons les questions de cybersécurité se sont imposées au sein des grands axes politiques de l'Union (marché intérieur, Europe de la défense, affaires intérieures). Elle décrit ensuite la place actuelle de la cybersécurité et la cyberdéfense au sein des différentes Institutions européennes selon plusieurs plans : les acteurs, les outils de mise en œuvre interne, les thèmes d'activité. Elle s'achève avec une série de remarques et de propositions sur la manière dont pourrait évoluer la prise en compte de la cybersécurité et la cyberdéfense au sein des Institutions européennes.

Enfin, la variété des modes d'implication d'acteurs nationaux dans les activités de cybersécurité et cyberdéfense au sein des Institutions européennes est rappelée en annexe.

1 Cadrage

C'est au tournant de l'année 2000 qu'est apparu le besoin d'impliquer l'Union Européenne et ses Institutions dans la lutte contre les menaces cybernétiques, d'une part pour améliorer le fonctionnement de ses Institutions elles-mêmes, d'autre part pour rendre plus efficaces et complémentaires les politiques nationales des Etats-membres.

Ce besoin n'a fait que se renforcer, donnant lieu à de multiples programmes et structures spécifiques couvrant progressivement le champ thématique du cyberespace et de la cybersécurité. Il s'ensuit une difficulté croissante à acquérir et entretenir une vision claire, à défaut d'être exhaustive, de ces actions et de leur impact en matière de renforcement du niveau de cybersécurité à travers l'Europe.

Au second semestre 2009, un « mémento général sur les politiques et programmes européens en sécurité des systèmes d'information » a été rédigé à l'intention de l'ANSSI. Deux ans plus tard, beaucoup de choses ont évolué, notamment en ce qui concerne les questions de cyberdéfense et les politiques de défense et de sécurité. La présente étude ayant vocation à être aussi complète que possible (*stand-alone*), elle reprend, avec mise à jour en tant que de besoin, des éléments déjà abordés dans le mémento de 2009, tout en les complétant avec éléments apparus au cours des deux années écoulées.

Elle identifie aussi certains axes d'effort qui permettraient aujourd'hui de donner plus de cohérence aux actions de l'Union européenne et de fonder une stratégie globale de cybersécurité et de cyberdéfense au sein des Institutions européennes.

1.1 Limitations

Dans cette étude, le terme « Europe » et le qualificatif « européen » désignent, sauf exception dûment spécifiée, les instances européennes et des actions menées ou des politiques décidées et mises en œuvre dans le cadre des Institutions européennes (Commission, Agences, Conseil, Parlement …).

Elle n'aborde donc pas les actions et politiques menées dans un cadre national ou bilatéral.

1.2 Définitions

Dans le cadre de cette étude, les termes de cyberespace, cybersécurité, cyberdéfense, etc. seront utilisés en accord avec les définitions fournies dans le document du SGDSN sur la « Défense et la sécurité des systèmes d'information » et rappelés dans l'encadré ci-dessous.

Encadré : Définitions dans le domaine cyber (Défense et sécurité des systèmes d'information - Stratégie de la France – SGDSN/ANSSI 2011)

Cyberespace :

Espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques.

Cybersécurité :

Etat recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.

Cybercriminalité :

Actes contrevenants aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un délit ou d'un crime, ou les ayant pour cible.

Cyberdéfense :

Ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels.

Bien que le thème de l'étude soit limité à la cybersécurité et la cyberdéfense, les questions de cybercriminalité ont été incluses dans l'analyse par souci de cohérence et de complétude.

1.3 Positionnement des Institutions européennes dans l'architecture politique de l'Europe

1.3.1 Traité de l'Union européenne

L'Union Européenne est régie par le Traité de l'Union mis à jour en application du Traité de Lisbonne adopté le 1er décembre 2009.

Un élément important du Traité de Lisbonne tient à l'abandon de la distinction entre le 1er pilier (politiques communautaires), le deuxième pilier (politique étrangère et de sécurité commune) et le 3ième pilier (affaires intérieures dont police, justice, lutte contre la criminalité)[1]. En matière de cyberdéfense et de cybersécurité, cette évolution devrait conduire à des approches plus cohérentes et complémentaires au sein des institutions européennes.

Un autre élément important est la nomination d'un Haut Représentant pour les affaires étrangères et la politique de sécurité, qui s'appuie sur un organe spécifique, le Service européen pour l'action extérieure (SEAE)[2] récemment mis en place, ainsi que le passage d'une politique *européenne* de sécurité et de défense (ESDP à une politique de sécurité et de défense *commune* (CSDP).

1.3.2 Principes

Les actions européennes sont menées en complément ou par défaut des actions nationales, selon le principe de **subsidiarité** (plus petit niveau d'autorité publique compétente).

Les actions européennes sont élaborées en suivant le principe d'**indépendance**, c'est-à-dire hors intérêt national spécifique ou sectoriels (e.g. exclusivité de la Commission européenne pour les propositions de directive).

Les actions européennes respectent aussi le principe de **transparence** (droit d'accès aux documents de la Commission, du Conseil et de Parlement[3] ; consultations ouvertes sur les textes en préparation ou en révision).

1.3.3 Axes directeurs de la Commission

D'une manière générale, l'action de la Commission vise à développer les 4 libertés de mouvements à l'intérieur de l'Union, libertés qui constituent l'essence du marché

[1] http://europa.eu/scadplus/glossary/eu_pillars_fr.htm
[2] Voir article 27 du Traité : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0013:0046:FR:PDF
[3] Voir article 42 de la charte des droits fondamentaux http://www.europarl.europa.eu/charter/pdf/text_fr.pdf

intérieur: mouvements des biens, des personnes, des services et des capitaux. Le concept d'interopérabilité y tient une place majeure : l'objectif de la Commission est d'éliminer tous les obstacles ou « barrières » (réglementaires, techniques, organisationnels) propres à réduire la fluidité du marché intérieur. Cette réduction des obstacles à la fluidité du marché est entreprise sur la base d'une concertation entre les parties prenantes (secteur public, secteur privé, monde académique…).

Dans cette perspective, les actions de la Commission européenne sont menées principalement selon trois axes:

- Développement du cadre juridique européen (notamment les Directives à transposer dans le cadre national)
- Programmes de recherche et développement (notamment le programme cadre PCRD ou FP pour Framework Programme)
- Programmes d'application (notamment le programme des « Large Scale Pilots » ou LSP pour la mise en application de politiques européennes spécifiques)[4].

Pour un sujet donné (par exemple la signature électronique, ou la protection des données personnelles), ces trois champs sont mis à contribution de façon séquentielle et complémentaire.

La première étape consiste généralement en une communication rédigée à l'initiative de la Commission, suivie d'une consultation ouverte où citoyens et organismes sont invités à s'exprimer. Il peut aussi y avoir un « livre vert » (poser un problème) suivi d'un « livre blanc » (proposer des solutions). Lorsqu'une convergence suffisante est atteinte, la Commission rédige un projet de Directive qui est soumis à l'approbation du Parlement et du Conseil (principe de codécision). Après approbation, la Directive doit être transposée dans les cadres juridiques nationaux dans un délai de 3 à 5 ans. A noter aussi qu'un réexamen des Directives est entrepris au bout de 3 ans (en principe), conduisant fréquemment à une révision.

Pour faciliter la mise en application de ce nouveau cadre juridique, des actions de R&D sont inscrites dans les programmes prévus à cet effet. Des études spécifiques peuvent être aussi financées par la Direction Générale en charge du sujet.

Pour les sujets d'une certaine ampleur (e.g. protection des infrastructures critiques), un programme spécifique d'application est mis en place sur plusieurs années (Critical Infrastructure Protection and Security, CIPS de 135 Millions d'euros sur 2007-2011). Enfin, des « Feuilles de routes » (Roadmap) peuvent être élaborées pour les sujets demandant une action dans la durée (e-Administration). Si la feuille de route inclut la mise en œuvre concrète d'une politique de la Commission, elle peut

[4] Antérieurement appelés eTEN (Trans-European Networks) et CIP (Competitiveness and Innovation Programmes)

donner lieu à des programmes pilotes impliquant un très grand nombre d'état et un financement de plusieurs dizaines de millions d'euros.

2 L'émergence de la cybersécurité, la cybercriminalité et la cyberdéfense au sein des politiques européennes

2.1 Vers une société de l'information et de la connaissance

Bien que la Directive sur la signature électronique date de décembre 1999[5], il est raisonnable de considérer l'adoption de la **Stratégie de Lisbonne**[6] au printemps 2000 comme l'étape fondatrice de la prise en compte par l'Union des enjeux de la sécurité des systèmes d'information au sein des politiques communautaire.

L'objectif de cette stratégie était de mettre en place une *« économie de la connaissance … capable d'une croissance économique durable accompagnée d'une amélioration quantitative et qualitative de l'emploi et d'une plus grande cohésion sociale* ».

Mais le déploiement des infrastructures de communication préparant cet objectif a constamment été confronté au besoin d'en assurer la sécurité, ne serait-ce que pour renforcer la confiance des utilisateurs: dès janvier 2001 la communication 2000/890 appelait à « *Créer une société de l'information plus sûre en renforçant la sécurité des infrastructures de l'information et en luttant contre la cybercriminalité* »[7].

Le plan d'action **eEurope 2002**[8] a principalement ciblé le renforcement des infrastructures de communication : accès à Internet « *moins chers, plus rapides et surs* », sécurisation des réseaux et des cartes à puces, mise en place d'un cadre juridique adapté au marché des télécommunications (voir 5.1.1 Paquet télécom), besoin d'une structure européenne pour aider au renforcement de la sécurité des systèmes d'information à travers l'Europe.

Tout en poursuivant le déploiement de réseaux sécurisés à large bande, le plan d'action **eEurope 2005**[9] a travaillé au développement de services en ligne (eGovernement, eBusiness, eHealth, eLearning, etc.). En Décembre 2003, le Conseil européen de Bruxelles décidait la création et l'implantation en Grèce d'une agence en charge de la sécurité des réseaux et de l'information (voir « 3.5.2 ENISA »).

---

[5] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:013:0012:0020:FR:PDF
[6] http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/fr/ec/00100-r1.f0.htm
[7] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0890:FIN:FR:PDF
[8] http://europa.eu/legislation_summaries/information_society/l24226a_fr.htm
[9] http://europa.eu/legislation_summaries/information_society/l24226_fr.htm

En 2005, l'« **Initiative i2010** »[10] établissait un cadre stratégique pour faire de l'Europe une société de l'information et de la connaissance. L'Initiative i2010 s'appuie sur trois axes :

- mettre en place un espace unique d'information (cadre juridique),
- renforcer l'innovation et l'investissement (programmes de R&D),
- ouvrir la société de l'information à tous (combler les fractures numériques).

Là encore, un axe d'effort important est de rendre Internet plus sûr vis-à-vis « *des fraudeurs, des contenus préjudiciables et des défaillances technologiques* ».

Une nouvelle étape en matière de cyberdéfense et de cybersécurité européennes est intervenue en 2007 avec l'approbation par le Conseil[11] de la « **Stratégie pour une société de l'information sûre** »[12] fondée sur trois lignes directrices : dialogue, partenariat et responsabilisation entre les acteurs publics, les entreprises et les utilisateurs individuels. Cette stratégie insiste sur la nécessité de :

- disposer de données fiables en matière de menaces, de vulnérabilités et d'incidents,
- mener des actions de sensibilisation valorisant la sécurité,
- mettre en place des mécanismes de partages d'information et d'alertes rapides,
- identifier et diffuser les bonnes pratiques.

Plus récemment, la Communication 2010-245 définissant un nouvel « **Agenda numérique pour l'Europe**[13] » prévoit un ensemble de 16 actions à mener d'ici à 2013. Beaucoup visent à supprimer les obstacles de tous ordres (technologies, réglementations, organisationnels) à l'encontre de la fluidité du marché des TIC entre Etats membres. Mais certaines actions visent aussi à renforcer la confiance et la sécurité : moderniser ENISA, développer la coopération entre les CERTs, créer un CERT des Institutions européennes, simuler des attaques internet à grandes échelles et apprendre à la contrer…

2.2 La construction de l'Europe de la Défense

La construction d'une politique de défense ne peut se développer sans une vision stratégique partagée des menaces, des enjeux et des actions à mener ainsi qu'un plan de développement de capacités et une protection rigoureuse des informations classifiées entre les entités impliquées. Aucune de ces conditions n'étaient pas en place en Europe avant les conclusions du Conseil européen de Cologne de juin 1999

[10] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0229:FIN:EN:PDF
[11] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:068:0001:0004:FR:PDF
[12] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0251:FIN:FR:PDF
[13] http://ec.europa.eu/information_society/digital-agenda/documents/digital-agenda-communication-en.pdf

sur le renforcement de la politique européenne commune de sécurité et de défense[14].

La première étape a logiquement porté sur la protection des informations classifiées et leurs conditions d'échange :

- Adoption en décembre 2001 d'un règlement de sécurité du Conseil européen (voir « 4.1 Règlement de sécurité » ci-après)
- Développement de réseaux sécurisés d'échange d'information entre le Secrétariat général du Conseil et les ministères nationaux concernés ainsi qu'entre l'Etat-major européen et les Etats-majors opérationnels (voir « 4.2 Les Réseaux et systèmes d'information européens » ci-après)
- Accord en 2003 entre l'Union et l'OTAN pour les échanges d'informations classifiées et les règles réciproques de leur protection[15], qui inclut en particulier un usage des mêmes standards et une reconnaissance réciproque de la qualification des outils de sécurité, y compris en matière de cryptographie.

Si la vision proposée en 2003 dans la « Stratégie européenne de sécurité »[16] n'évoquait pas les menaces et risques liés aux réseaux et à l'information, la vision à long terme[17] sur les besoins en capacités établie en 2006 par l'Agence européenne de défense[18] (AED ou EDA) évalue l'impact de la révolution technologique, notamment concernant les technologies de l'information pour les volets capacitaires « *informe* » (surveillance du cyberespace) et « *protège* » (protection des réseaux et zones d'actions contre les cyber-attaques).

Cette vision a conduit dès 2006 à placer la « capacité de mise en réseau » (ou NEC : Network Enabled Capability) parmi les principaux axes d'effort[19], avec pour objectif de mieux maîtriser les besoins d'échanges sécurisés d'information, en particulier pour ce qui concerne les engagements civilo-militaires, en combinant les trois composantes personnes/informations/technologies.

A l'heure actuelle, la cyberdéfense fait partie de la liste des 10 capacités prioritaires à développer[20]. Il s'agit surtout de protéger les réseaux militaires contre toutes formes de cyber-menaces tout en favorisant les échanges d'information indispensables aux

---

[14] http://www.europarl.europa.eu/summits/kol2_fr.htm#an3
[15] Cet accord spécifique fait partie de l'arrangement plus général dit « Berlin + »
[16] http://www.ladocumentationfrancaise.fr/dossiers/europe-defense/strategie-europeenne-securite.shtml
[17] http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/EN/reports/91135.pdf
[18] http://www.eda.europa.eu/
[19] http://www.eda.europa.eu/news/06-04-25/EDA_Hosts_Seminar_on_Network-Enabled_Capability
[20] http://eda.europa.eu/Capabilitiespriorities/Top10priorities/CyberDefence

actions en coopération et en coalition. L'idée d'un Nuage militaire (Military cloud) est avancée, par analogie avec l'information en nuage (Cloud computing) qui se développe actuellement dans le marché civil.

2.3 La lutte contre la criminalité et le terrorisme

La dimension numérique (cyberespace) s'est introduite dans le champ de la sécurité intérieure (ou affaires intérieures) en suivant deux chemins distincts mais convergents: d'une part dans le cadre de la lutte générale contre la criminalité, d'autre part dans le sillage de la politique anti-terroriste développée en réponse aux attaques du 11 novembre 2001.

Concernant la lutte générale contre la criminalité, l'instrument majeur qui a marqué la prise en compte de la dimension numérique a été la « **Convention Internationale contre la cybercriminalité** »[21] adoptée en 2001 par le Conseil de l'Europe. Mais, comme chacun sait, le Conseil de l'Europe n'est pas une Institution européenne[22] et se sont les Etats y siégeant qui doivent individuellement signer et ratifier cette convention. Seuls 32 Etats l'ont fait en date du 26 septembre 2011, 9 Etats membres de l'Union européenne ne l'ayant pas encore ratifiée[23].

Ceci n'a pas empêché les Institutions européennes de développer des actions allant dans le sens d'un renforcement de la lutte contre la cybercriminalité au sein de l'Union. C'est le cas de la Décision-cadre sur les **cyber-attaques** adoptée en 2005[24] par le Conseil européen et établissant des normes juridiques communes aux Etats membres dans ce domaine (incrimination, sanctions, échanges d'information, coopération intra-européenne). On peut aussi citer le programme Safer Internet (1999-2004) puis Safer Internet plus (2005-2008) et maintenant le Safer Internet Programme (2009-2013) ciblant notamment la lutte contre les contenus illégaux.

Concernant la lutte anti-terrorisme, les attentats de 2001 sur New-York et ceux de Madrid et Londres ont conduit à deux actions principales :

- la mise en place d'un Groupe de personnalités pour réfléchir sur le rôle de l'Europe en matière de sécurité[25] et dont les conclusions en mars 2004 ont conduit à la mise en œuvre d'un programme de recherche dédié aux questions de sécurité maintenant intégré dans le 7ième Programme Cadre

[21] http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm
[22] 47 Etats siègent au Conseil de l'Europe, 30 d'entre eux ne sont pas membres de l'Union européenne
[23] Autriche, Belgique, Grèce, Irlande, Luxembourg, Malte, Pologne, République Tchèque, Suède (en date du 26 septembre 2001)
[24] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:FR:PDF
[25] http://ec.europa.eu/enterprise/security/doc/gop_en.pdf

de R&D[26] (voir ci-après « 5.2 Programme Cadre de Recherche et Développement ») et à l'instauration d'une instante permanente, le « European Security Research Advisory Board » (ESRAB) mise en place pour conseiller la Commission en la matière[27].

- La prise en compte progressive des questions de protection des infrastructures critiques (voir ci-après « 5.3 Protection des Infrastructures critiques ») avec notamment :
  - une communication en 2004[28] proposant un programme européen pour la protection des infrastructures critiques (PEPIC),
  - la publication d'un « livre vert sur un programme européen de protection des infrastructures critiques »[29],
  - la proposition de procédure de recensement des infrastructures critiques européennes en décembre 2006[30],
  - la première mise en œuvre de cette procédure pour les infrastructures de transport et d'énergie en application de la Directive 2008/114 de décembre 2008[31],
  - le financement sur la période 2007-2013 d'un programme spécifique d'études pour « la prévention, préparation et gestion des conséquences en matière de terrorisme et autres risques liés à la sécurité »[32], visant à la protection et la sécurité des infrastructures critiques (CIPS).

Parallèlement, d'autres instruments juridiques européens sont venus compléter certaines questions concernant aussi bien la lutte contre la criminalité que la lutte anti-terroriste, telles que la Directive 2006/24 sur les données de connexion[33], la Résolution du Conseil de 1995 sur les interceptions légales[34].

3 Les acteurs

Les échanges d'information et les réseaux informatiques ayant un rôle croissant dans les activités économiques et les politiques qui les soutiennent, la question de leur sécurité des systèmes d'information se répartit largement à travers l'ensemble des Institutions européennes

---

[26] http://cordis.europa.eu/fp7/security/about-security_en.html
[27] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:191:0070:0072:EN:PDF
[28] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:FR:PDF
[29] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0576:FIN:FR:PDF
[30] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0787:FIN:FR:PDF
[31] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:FR:PDF
[32] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:058:0001:0006:FR:PDF
[33] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:FR:PDF
[34] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996G1104:EN:HTML

3.1 Commission européenne

Six Directions générales sont principalement impliquées dans les questions de sécurité des systèmes d'information

3.1.1 DG INFSO[35] (Société de l'information et des médias)

Au sein de la Direction A (Audiovisuel, Media, Internet), l'Unité A3 (Internet, Sécurité de l'information et des réseaux) pilote les travaux sur les enjeux de sécurité (e.g. étude ARECI sur la résilience des infrastructures de communication publiques[36]), prépare des communications (COM2006/251 : stratégie pour une société de l'information sûre, COM 2009/149 : protection des infrastructures d'information critiques …), assure le suivi de certains thèmes (signature électronique et sa directive 1999/93) et suit particulièrement les activités de l'agence ENISA.

La direction B (Politiques de communication électronique, notamment l'Unité B1 : Développement des politiques) est en charge du cadre légal du marché des communications électroniques (Unités B2 & B3 : mise en œuvre des cadres réglementaires ; voir ci-après « 5.1.1 Paquet télécom ») et de la politique de gestion du spectre de fréquence (Unité B4).

La direction F (Technologies et infrastructures émergentes) comprend l'Unité F5 (Confiance et sécurité) qui supervise la composante sécurité du volet « technologies de la société de l'information » du Programme Cadre de R&D (voir ci-après « 5.2 Programme Cadre de Rechercher et développement »). Elle inclut aussi les Unités F1 & F2 qui traitent des technologies émergentes et futures et l'Unité F4 en charge des nouvelles infrastructures (par exemple le réseau mondial GEANT entre universités et centres de recherche), tous thèmes porteurs de nouveaux défis en matière de sécurité.

Enfin la direction H (Enjeux sociétaux liés aux technologies de l'information et de la communication) inclut notamment l'Unité H2 (Technologies de l'information pour le gouvernement et les services publics) en charge des questions d'administration électronique (voir ci-après « 5.8 Administration électronique »).

Bien sur, des questions de sécurité interviennent aussi dans de nombreux sujets traités par d'autres Unités de la DG INFSO, telles que D4 (Entreprises en réseaux et RFID), G3 (Systèmes enfouis et contrôles), G4 (TIC pour les transports), H1 (Télémédecine), etc.

[35] Voir organigramme http://ec.europa.eu/dgs/information_society/directory/pdf/organi_en.pdf
[36] http://www.epractice.eu/en/library/281377

3.1.2 DG Justice[37]

La direction C (Droits fondamentaux et citoyenneté) est en charge des questions liées à la protection des données personnelles, par l'intermédiaire de l'Unité C3 qui gère les contrats d'étude sur les technologies d'amélioration de la vie privée (voir ci-après « 5.7 Protection de la vie privée »).

Cette DG partage aussi avec la DG Home (Affaire intérieures) le service commun des moyens d'audit interne, y compris pour la gestion des documents et des systèmes d'information (voir 4.4 « Moyens d'audit interne »).

3.1.3 DG Home (Affaires intérieures)[38]

La Direction A (Sécurité intérieure), plus précisément son Unité A2 (Lutte contre le crime organisé) est l'entité en charge des questions de cybercriminalité (voir 5.6 ci-après). Parallèlement, l'Unité A1 (gestion de crises et lutte contre le terrorisme), est responsable du programme européen de protection des infrastructures critiques (PEPIC ou EPCIP) et du programme d'études CIPS (voir 5.9 ci-après).

La Direction C (Migration et frontières), à travers les Unités C2 (Projets informatiques : infrastructures et aspects juridiques) et C3 (Systèmes informatique à grande échelle et biométrie), est en charge des réseaux, bases de données et applications sécurisés dédiés (voir « 4.2 Réseaux et systèmes d'information européens)

3.1.4 DG ENTR (Entreprise et Industries)[39]

La direction C (Politique Réglementaire) gère à travers l'Unité C5 les relations de la Commission avec les organismes européens de standardisation CEN, ETSI, CENELEC, y compris pour les questions de cyberdéfense (voir ci-après « 5.4 Standardisation et certification »).

La direction D (Innovations industrielles et industries de la mobilité) est concernée par la cyberdéfense en raison du développement des TIC pour la compétitivité et l'innovation industrielle (Unité D3) et du caractère sensible ou classifié de données relevant des industries de « défense, aérospatiales et maritimes » (Unité D4).

Enfin, dans la mesure où les moyens spatiaux participent aussi de la problématique des systèmes d'information dont la sécurité doit être assurée, il faut noter l'entité GP/3 (Programmes de navigation par satellites européens : Applications, sécurités, aspects internationaux) impliquée dans la politique de sécurité du système Galileo et

---

[37] http://ec.europa.eu/justice/about/files/organisation_chart_en.pdf
[38] http://ec.europa.eu/dgs/home-affairs/chart/docs/organigramme_fr.pdf
[39] http://ec.europa.eu/enterprise/dg/files/org_chart_fr.pdf

de ses signaux, ainsi que la Direction H (Espace, sécurité et GMES), notamment l'Unité H3 responsable des programmes de R&D en sécurité et l'Unité H4 responsable du programme GMES.

3.1.5 DG HR (Ressources Humaines et Sécurité)[40]

La direction DS (Sécurité) assure la politique de sécurité pour l'ensemble de la Commission. En particulier, l'Unité DS.5 est en charge de la « sécurité informatique » (voir ci-après« 4.1 Règlements de sécurité » et « 4.2 Réseaux et systèmes d'information »).

3.1.6 DG JRC (Centre commun de recherche)[41]

Deux instituts du CCR (ou JRC) traitent des questions de cybersécurité et cyberdéfense au sein de divers programmes de recherche, soit financés par la Commission (voir ci-après « 5.1.1 Programme Cadre de Recherche et développement »), soit sur contrats extérieurs :

- L'institut de protection et de sécurité du citoyen (IPSC) d'ISPRA abrite le laboratoire « Evaluation des technologies de sécurité » (Unité G6) qui mène des travaux techniques (ex : senseurs biométriques)
- L'institut d'études de prospectives technologique (IPTS) de Séville où se trouve le laboratoire « société de l'information » (Unité J4) qui mène des travaux plus orientés vers les impacts sociaux (acceptabilité, confiance) des technologies de l'information.

3.2 Secrétariat général du Conseil

Contrairement à la Commission, le Secrétariat général du Conseil est confronté à la gestion de beaucoup d'informations classifiées, que ce soit pour les échanges avec les ministères nationaux, ceux avec l'OTAN ou autres.

L'organisation a sensiblement changé sur ce plan. L'ancien Bureau Infosec n'est plus rattaché au Secrétaire général adjoint et l'ensemble des activités de sécurité ont été regroupées dans la Direction 3SIC[42] (Sécurité, Sureté et Systèmes d'Information et de Communication), qui fait partie de la Direction Générale A-Personnel et Administration[43] du Secrétariat général du Conseil.

La Direction 3SIC est elle-même subdivisée en 5 entités :

1. Le « Bureau de sécurité » qui traite de la sécurité physique

[40] http://ec.europa.eu/dgs/human-resources/documents/hr_chart_fr.pdf
[41] http://ec.europa.eu/dgs/jrc/downloads/jrc_orga_fr.pdf
[42] http://europa.eu/whoiswho/public/index.cfm?fuseaction=idea.hierarchy&nodeID=254596&lang=FR
[43] http://europa.eu/whoiswho/public/index.cfm?fuseaction=idea.hierarchy&nodeID=4597&lang=FR

2. La Direction 5 « Systèmes d'information et de communication » (environ 120 personnes, beaucoup plus grosse que les autres)
3. L'Unité « Service de prévention »
4. L'Unité « Assurance de l'information » (ex-Bureau Infosec)
5. L'Unité « Planification de la continuité d'activité et autorité d'homologation de sécurité »

Les 2ième, 4ième et 5ième sont principalement celles qui sont impliquées dans les questions de sécurité des systèmes d'information. La Direction 5 abrite une Unité « Sécurité des SIC sensibles » qui comprend trois équipes (Etudes, Gestion des incidents, Inspections) dont la seconde (Gestion des incidents ou Network Defence Capability) travaille en relation avec le CERT-EU en gestation (voir 4.3 « CERT-EU »).

3.3 SEAE (Service Européen des Actions Extérieures)[44]

Créer par le Traité de Lisbonne, le Service Européen des Actions Extérieures est une nouvelle Institution européenne résultant principalement du regroupement d'équipes précédemment placées au sein du Conseil (Comité Militaire – EUMC ; Centre de situation - SITCEN)) ou de la Commission (DG RELEX) ou leur étant rattachées (Etat-major européen – EUMS ; Direction de la planification de crise – CMPD ; Capacité civile de planification et de conduite d'actions – CPCC ; Centre satellitaire européen, Agence européenne de défense, Institut européen d'études de sécurité).

Le SEAE est responsable de la conduite de la Politique Etrangère et de Sécurité Commune.

Fin 2011, le SEAE regroupe quelques 600 personnes. Au sein de la Direction administrative et financière, se trouve un bureau de sécurité qui comprend une équipe en charge de la sécurité des communications.

3.4 Parlement

C'est la Commission parlementaire ITRE (industrie, recherche et énergie) qui suit les questions relatives au développement de la société de l'information et aux enjeux de sécurité associés[45].

Le Parlement européen porte une attention particulière à la protection de la vie privée et des données personnelles.

3.5 Autres organismes européens

[44] http://www.libertysecurity.org/IMG/pdf/EU_Commission_-_Organizational_Chart_DG_External_Relations.pdf
[45] http://www.europarl.europa.eu/activities/committees/homeCom.do?language=FR&body=ITRE

3.5.1 EDPS

Le Contrôleur européen des données personnelles est l'autorité indépendante en matière de protection des données, dont la responsabilité s'étend sur l'ensemble des Institutions européennes. Créé par la directive 2001/45[46], il est l'équivalent de la CNIL au niveau national français.

Il a pouvoir de contrôle sur les réseaux européens (voir ci-après « 4.2 Réseaux et systèmes d'information »). Il conseille la Commission en matière juridique, notamment pour la révision des directives traitant de données personnelles (voir ci-après « 5.7 Protection de la vie privée »).

3.5.2 ENISA

ENISA est une agence de régulation de la Commission[47] créée en mars 2004 dans le but de développer à travers l'Europe la culture en sécurité des systèmes d'information[48].

C'est l'instance européenne la plus spécifiquement dédiée à la sécurité des systèmes d'information. Elle conseille la Commission et les Etats membres dans tous les domaines relevant de la sécurité de l'information et des réseaux, elle mène des études et des actions de concertations sur les thèmes retenus dans son programme annuel d'activité validé par le Conseil d'Administration où siègent les représentants des Etats membres et de la Commission. Elle est étroitement impliquée dans la mise en œuvre des politiques communautaires décidées en matière de cybersécurité et de cyberdéfense.

Créée initialement pour une période de 5 ans, elle a été prolongée jusqu'en septembre 2013 avec un mandat identique par décision du Parlement et du Conseil[49]. Un nouveau mandat, incluant probablement une extension de ses responsabilités et moyens, est en préparation.

3.5.3 EDA

Créée en juillet 2004[50], l'Agence européenne de défense est une agence du Service Européen des Actions Extérieures chargée de concrétiser la politique européenne de défense aux plans du développement de capacités opérationnelles, de sa base

[46] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/DataProt/Legislation/Reg_45-2001_FR.pdf

[47] Pour la distinction entre agences de régulation et agences exécutives, voir http://eur-lex.europa.eu/LexUriServ/site/fr/com/2001/com2001_0428fr01.pdf , page 36

[48] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:077:0001:0011:FR:PDF

[49] http://www.enisa.europa.eu/media/news-items/extension-of-enisa2019s-mandate-published-1

[50] http://eur-lex.europa.eu/LexUriServ/site/fr/oj/2004/l_245/l_24520040717fr00170028.pdf

industrielle et technologique, des programmes de R&D et des coopérations dans le domaine de l'armement[51].

Son plan de développement de capacités (CDP) inclut, parmi ses dix priorités, une capacité de cyberdéfense afin de protéger les réseaux nécessaires à la préparation, la gestion et l'action des forces. Le développement de cette capacité est sous la responsabilité de la Direction des Capacités.

3.5.4 EUROPOL

Europol est initialement un bureau (« office ») créé en 1992 par le Traité de l'Union pour traiter les renseignements relatifs aux activités criminelles en Europe[52]. Il devient une agence européenne par décision du Conseil européen Justice et Affaires intérieures en avril 2009.

Une part importante de ses activités consiste à assurer la gestion et l'échange d'informations très sensibles relatives à toutes sortes de fraudes. Le département des capacités (Capabilities Department) assure la disponibilité des moyens nécessaires en termes de communications sécurisées[53].

Depuis 2002, Europol est le principal pôle européen de lutte contre la cybercriminalité et dispose d'un centre dédié dont les compétences ont été étendues en novembre 2009 pour inclure des fonctions opérationnelles telles que le signalement en ligne des délits observés sur Internet[54].

3.5.5 Entreprises Communes (Joint Undertaking)

Une entreprise commune (ou JU, Joint Undertaking) est un organe de l'Union créé pour améliorer la mise en œuvre de ses politiques (article 187 du Traité de l'Union en cours). Elle correspond à un partage de responsabilités entre les secteurs public et privé, généralement associé à un investissement important de l'industrie en vue d'un marché très prometteur à plus ou moins long terme[55].
Les deux entreprises communes qui touchent le plus aux questions de sécurité des systèmes d'information sont :

[51] http://www.eda.eu.int/Aboutus/Howweareorganised/Organisation
[52] http://www.europol.europa.eu/
[53] https://www.europol.europa.eu/content/page/organisational-chart-157
[54] http://www.publications.parliament.uk/pa/ld200910/ldselect/ldeucom/68/68we05.htm
[55] On peut citer des entreprises communes telles qu'ITER (physique atomique), ENIAC (nanotechnologies), SESAR (ciel unique européen), etc.

- La JU GALILEO[56] mise en place en 2002 pour gérer le financement de la phase de déploiement de la constellation de navigation par satellites. Faute de l'apport privé escompté et des responsabilités confiées à l'Agence Spatiale Européenne (ESA), l'entité se concentre sur les aspects de sécurité, notamment pour la gestion du signal public réglementé (PRS)
- La JU ARTEMIS[57] créée en 2008 pour le développement des calculateurs enfouis (applications attendues en télémédecine, transport intelligent, armement, aérospatiale…)

A noter que la Commission a renoncé jusqu'à présent à créer une JU sur les outils et services pour la sécurité des systèmes d'information, faute sans doute d'une perspective de marché suffisamment prometteuse et de partenaires industriels suffisamment motivés (les deux aspects étant évidemment liés).

4 Les outils de mise en œuvre interne

Jusqu'à la fin des années 90, les institutions européennes n'avaient pas eu à traiter beaucoup d'informations très sensibles, encore moins classifiées (voir ci-dessus chapitre 2). A partir de l'an 2000, les outils nécessaires à la protection des informations et des réseaux ont peu à peu été mis en place, même s'il reste encore de larges marges de progression.

4.1 Règlements de sécurité

Il a fallu attendre 2001 pour que soient adoptés des règlements de sécurité au sein des Institutions européennes, incluant la protection d'informations classifiées aux niveaux RESTREINT UE, CONFIDENTIEL UE, SECRET UE et TRES SECRET UE/EU TOP SECRET.

De tels règlements ont été adoptés pour le Conseil (décision du 19 mars 2001)[58], le Parlement (décision du 13 novembre[59]) et la Commission (décision du 29 novembre[60]). Le 27 mai 2011, le Conseil a adopté un nouveau règlement portant sur

[56] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:138:0001:0008:FR:PDF et http://europa.eu/legislation_summaries/internal_market/single_market_for_goods/motor_vehicles/l24098_en.htm#AMENDINGACT
[57] https://www.artemis-ju.eu/
[58] http://admi.net/eur/loi/leg_euro/fr_301D0264.html
[59] Voir l'annexe VII du règlement intérieur du Parlement pour un état actuel de la protection des informations confidentielles http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+RULES-EP+20090309+ANN-07+DOC+XML+V0//FR#def1
[60] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001D0844:FR:HTML

la protection des informations classifiées y compris pour dans le cas de contrats et sous-contrats industriels[61].

Les autres organes de l'Union (ex : agences) sont généralement soumis à un règlement de transparence et confidentialité (ex : ENISA) qui reprend ces règles de protection de l'information.

La question des échanges d'information classifiée entre les Etats membres et le Institutions Européennes reste délicate, faute d'un texte juridique commun définissant les niveaux de classification et les règles de protection entre les Institutions européennes et les Etat membres. Ce texte devant avoir valeur de traité, la lourdeur des procédures d'adoption à mettre en jeu a conduit à se contenter d'une série d'accords bilatéraux entre Etats, complété d'un échange de lettres avec l'UE et d'un engagement des Etats à appliquer aux informations classifiées EU des règles de protection au moins égales à celles du Conseil.

4.2 Réseaux et systèmes d'information européens

En plus des très nombreux réseaux donnant un accès public aux informations de l'Union, un certain nombre de réseaux ont été mis en place par les Institutions européennes pour assurer des échanges protégés d'information en interne ou avec des partenaires extérieurs.

Réseaux concernant les échanges entre administrations et entités travaillant sur les projets financés par l'UE :

- sTESTA, réseau transeuropéen sécurisé pour les échanges télématiques entre administrations. C'est la version sécurisée du réseau TESTA jusqu'au niveau UE restreint
- CIRCA, devenu CIRCABC, Centre de ressources d'information et de communication[62], utilisant un droit d'accès (besoin den connaître) pour les personnes impliquées dans des actions ou groupes de travail de l'Union
- réseau Extranet interne à la Commission, validé pour la protection des informations UE restreint.

Réseaux concernant les échanges d'information à contenu diplomatique et militaire :

- réseau CORTESY pour les échanges d'information diplomatiques en liaison avec la politique européenne commune des affaires étrangères et de sécurité jusqu'au niveau CONFIDENTIEL UE

[61] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:141:0017:0065:EN:PDF
[62] http://circa.europa.eu/Public/irc/infso/Home/main

- réseau ESDP.net (ex WEU.net) pour les échanges d'information à caractère militaire entre le SGCEU et les ministères de la défense des Etats membres jusqu'au niveau SECRET UE
- réseau SESAME devant à terme (2012) remplacer les deux réseaux précédents
- réseau EU OPS WAN pour les échanges d'information entre l'Etat-major européen et les Etats-majors opérationnels

Ces réseaux sont gérés par la Direction 3SIC du Secrétariat Général du Conseil et ses équipes en matière d'homologation, inspection, gestion des incidents, etc. (voir « 3.2 Secrétariat général du Conseil » ci-dessus).

Réseaux concernant d'autres questions de sécurité :

- système FADO d'archivage d'images pour lutter contre l'immigration clandestine et la criminalité organisée
- réseau BDL pour la transmission d'informations classifiées entre EUROPOL et les officiers de liaison nationaux
- Base de données EURODAC (base de données et réseaux) contenant les empreintes digitales des demandeurs d'asile
- SCEPYLT[63], système d'information centralisé visant à sécuriser la commercialisation des explosifs en Europe
- Systèmes d'Information Schengen[64] (SIS et SIS II) sur le signalement des personnes et des objets dans le cadre de la politique Schengen, ainsi que le système d'information VIS (Visa Information System) opérationnel depuis fin 2010 pour la lutte contre les fraudes ou les demandes multiples à l'attribution de visas.

4.3 CERT-UE

C'est en juin 2011 qu'a été constituée une équipe en charge de coordonner à l'échelle des Institutions européennes la réponse aux incidents ou attaques à l'encontre des systèmes d'information[65].

Ce *Computer Emergency Response Team* est pour l'instant composé d'un expert d'ENISA, 2 du Conseil européen, 1 du Parlement, 1 du Comité Economique et Social, 5 de la Commission, soit 10 personnes au total. Il a été établi à titre probatoire, un bilan des résultats devant être effectué au bout d'un an et une décision prise en mai 2012 sur la suite à donner.

[63] Système de contrôle et de protection des explosifs, pour la prévention et la lutte contre le terrorisme
[64] http://www.europarl.europa.eu/comparl/libe/elsj/zoom_in/25_fr.htm
[65] On peut compter 20.000 postes de travail à la Commission, 2000 au Secrétariat du Conseil, de l'ordre de 6.000 à 7.000 dans la vingtaine d'agences, soit au total 30.000 à 35.000.

Le CERT-UE a une fonction de support vis-à-vis des équipes existantes au sein des entités européennes pour la protection des systèmes d'information. Il remplit un rôle de diffuseur d'informations générales sur les menaces, de conseil à la demande et d'assistance en cas d'incident, de coordination en cas d'attaques de grande ampleur et de situation critique.

Le CERT-UE entretien un site ouvert sur les vulnérabilités, les menaces et les acteurs menaçants[66]. Il a recensé 60 organismes européens susceptibles d'être ses « clients » et qui présentent une maturité très variée en termes d'expertise et de moyens de cyberdéfense. Il a visité l'ensemble des CERTs établis dans les pays européens et se présente d'ores et déjà comme un point focal de circulation d'informations grâce à son site dédié. Il a vocation à s'intégrer progressivement dans les exercices paneuropéens sur les attaques contre les systèmes d'information (voir « 5.9 Protection des infrastructures critiques »).

Logiquement, le CERT-UE devrait être pérennisé en mai 2012. Il est possible qu'il acquière le statut de « bureau » (office) au sein des Institutions européennes.

4.4 Moyens d'audit interne

La Commission dispose d'un service commun d'audit interne en SSI réparti entre la DG Home[67] et la DG Justice[68], sous forme d'équipes directement rattachées chaque fois au Directeur général.

Pour le Secrétariat du Conseil, des capacités d'audit (ou inspections) existent à la Direction 5-CIS au sein de la Direction 3SIC[69], d'une part pour les réseaux sensibles avec l'équipe « défense des réseaux » de l'unité «sécurité des SIC sensibles » (Direction 5-CIS), d'autre part pour les réseaux classifiés avec l'Unité « Planification de la continuité d'activité et autorité d'homologation de sécurité » (Direction 3SIC).

5 Les thèmes d'activité

5.1 Réglementation du marché des communications électroniques publiques

Le cadre juridique européen réglementant le marché des communications publiques consiste essentiellement en une série de directives adoptées en 2002 (dit « paquet télécom ») et de quelques autres sur la signature électronique, le commerce

[66] http://cert.europa.eu/cert/plainedition/en/cert_about.html
[67] http://ec.europa.eu/dgs/home-affairs/chart/docs/organigramme_fr.pdf
[68] http://ec.europa.eu/justice/about/files/organisation_chart_en.pdf
[69] http://europa.eu/whoiswho/public/index.cfm?fuseaction=idea.hierarchy&nodeID=254596&lang=FR

électronique et le marché des services. Ces Directives abordent bien entendu la question de la sécurité des systèmes et services publics de communication.

5.1.1 Paquet télécom

- directive 2002/19[70], dite « accès », donnant aux autorités réglementaires nationales pouvoir de « fixer les conditions techniques et opérationnelles pour assurer le fonctionnement normal des réseaux ».
- directive 2002/20[71], dite « autorisation », prévoyant qu'une autorisation de mise en exploitation d'un réseau peut être conditionnée au « maintien de l'intégrité du réseau public » et de la « sécurité des réseaux publics face au accès non autorisés »
- directive 2002/21[72], dite « cadre », créant les autorités nationales de régulation devant contribuer à « assurer un haut niveau de protection des données personnelles » et « garantir l'intégrité et la sécurité des réseaux de communication publics »
- directive 2002/22[73], dite « service universel », spécifiant que « les Etats membres prennent toutes les mesures nécessaires pour assurer l'intégrité du réseau téléphonique public… et garantir un accès ininterrompu aux services d'urgence »
- directive 2002/58[74], dite ePrivacy, spécifiant les conditions d'application de la directive 1995/46[75] de protection des données personnelles dans le cas particulier de la mise en œuvre de systèmes de communication électroniques.

[70] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0019:FR:HTML
[71] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0020:FR:HTML
[72] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0033:0033:FR:PDF
[73] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0051:0077:FR:PDF
[74] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:FR:PDF
[75] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:FR:HTML

Ce cadre réglementaire a introduit des avancées dans le domaine de la sécurité des réseaux :

- la mise en œuvre par les opérateurs[76] de communications publiques de **mesures de sécurité appropriées** pour garantir la sécurité et l'intégrité des réseaux de télécommunication d'une part (art. 13 bis de la directive cadre) et la sécurité du traitement des données à caractère personnel d'autre part (art. 4 de la directive vie privée et communications électroniques) ;
- le **contrôle** par les autorités nationales des mesures mises en œuvre (art.13ter de la directive cadre et art. 4 de la directive vie privée et communications électroniques).

Une révision de ces Directives est intervenue en 2009, conduisant aux Directives 2009/136[77] (dite *Droits des citoyens*) et 2009/140[78] (*Vers une meilleure réglementation*), sans incidence majeure en matière de cyberdéfense et de cybersécurité, sauf pour ce qui concerne la protection des données personnelles (voir ci-après « 5.7 Protection de la vie privée »).

Une décision de la Commission a créé en juillet 2002 un groupe européen de régulateurs (ERG)[79] pour veiller à la bonne application de ces directives et préparer leur révision. Il a été remplacé en 2009 par le BEREC (Body of European Regulators in Electronic Communications) dont le règlement[80] a été approuvé par le Conseil et le Parlement.

5.1.2 Autres directives

- directive 1999/93[81], définissant les conditions de mise en œuvre d'une **signature électronique**
- directive 2000/31[82], définissant les conditions de mise en œuvre de services électronique, en particulier le **commerce électronique**
- directive 2002/77[83], définissant les conditions de la **concurrence** au sein du marché des communications électroniques
- directive 2006/24[84], définissant les conditions de rétention des **données de connexion**

---

[76] Définies comme les entreprises fournissant des réseaux de communications publics (directive cadre) ou des services de communications électroniques (directives cadre et vie privée).
[77] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:Fr:PDF
[78] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:FR:PDF
[79] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:200:0038:0040:FR:PDF
[80] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0001:0010:EN:PDF
[81] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:013:0012:0020:FR:PDF
[82] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0016:FR:PDF
[83] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:249:0021:0021:FR:PDF

5.2 Programme Cadre de Recherche et Développement

Depuis les années 80, le **programme cadre de R&D** (PCRD ou FP) est organisé en tranches de 5 ans, le septième s'étendant maintenant sur 7ans pour suivre le cycle budgétaire de l'Union (2007-2013). Les télécommunications puis les communications électroniques ont toujours été un thème « privilégié » des PCRD, représentant près de 20% des financements (le PCRD est issu du programme ESPRIT du début des années 80 déjà consacré aux technologies de télécommunications). Le PCRD ne représente au total que 4 à 5% du financement public total de R&D en Europe, mais joue un rôle important en tant que promoteur des coopérations entre acteurs scientifiques et techniques européens.

Le 7ième PCRD 2007-2013 comprend 4 volets : Coopération, Idées, Personnes, Capacités (hors CCR et Euratom). Le volet Coopération se répartit en 10 thèmes[85]. Les questions de cyberdéfense et de cybersécurité apparaissent dans les thèmes TIC (anciennement IST, Technologies de la Société de l'Information) et Sécurité (après intégration dans le 7ième PCRD de l'Action Préparatoire de Recherches en Sécurité 2004-2007). Le budget Coopération est de 32 365 millions d'euros, dont 1350 pour la sécurité et 9110 pour les TIC.

Les projets et leur financement relèvent principalement de cinq catégories : les programmes intégrés (IP), les réseaux d'excellence (NoE), les projets de recherche ciblée (STREP) les actions de coordination (CA) et les actions de soutien spécifique (SA). Des financements sont attribués 2 ou trois fois par an par le biais d'appels à proposition (call) regroupant des questions spécifiques relatives à certains volets et certains thèmes.

A titre d'exemple, l'appel de juillet 2009 comprend dans le volet TIC (call 5) un montant de 90 millions d'euros sur le thème de la confiance[86], et dans le volet Sécurité (call 3) un seul projet (action de coordination) sur la continuité d'activités et la restauration en cas de crise affectant des infrastructures vitales, notamment les réseaux publics de communication (référence 2010.4.4.1, page 29).

Par contre, le programme 2011-12 en Coopération[87] ne comporte par de thème de cyberdéfense ou de cybersécurité. Le programme Sécurité 2012 comprend néanmoins dans son volet « Cybercrime » un appel sur la convergence entre sécurités physique et numérique et un autre sur la résilience numérique (informatique en nuage sécurisée pour des infrastructures critiques).

---

[84] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:FR:PDF
[85] http://cordis.europa.eu/fp7/home_fr.html
[86] ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/ict-wp-2009-10_en.pdf , pages 21-22
[87] http://cordis.europa.eu/fp7/ict/docs/3_2012_wp_cooperation_update_2011_wp_ict_en.pdf

5.3 Programme Compétitivité et Innovation

Sur la période 2007-2013, le Programme Compétitivité et Innovation (CIP) complète le PCRD en finançant des déploiements pilotes de solutions d'interopérabilité à l'échelle de plusieurs pays, ce qui amène à prendre en compte les questions de sécurité associées[88]. Le CIP comprend trois volets :

- Innovation et esprit d'entreprise
- Appui stratégique en matière de TIC[89]
- Energies intelligentes pour l'Europe.

Le programme d'appui stratégique en matière de TIC aussi appelé « ICT Policy Support Programme » consiste à mobiliser un grand nombre d'Etats membres (6 ou 8 minimum) pour mettre en pratique la réalisation d'un objectif européen dans un domaine donné de façon à ce que l'activité puisse se poursuivre à la fin du soutien financier européen et que les autres pays dans cette activité y soient progressivement entrainés.

De tels projets durent 3 à 4 ans et requièrent des financements de l'ordre de plusieurs dizaines de millions d'euros chacun.

Entre 2007 et 2011, 5 projets pilotes à grande échelle (Lagre Scale Pilot ou LSP) ont ainsi été engagés sur des thèmes rattachés à l'administration électronique qui ont pour point commun un besoin de sécurisation du transport de messages électroniques et la validation d'outils d'authentification et de signature électroniques (voir ci-après « 5.8 Administration électronique »).

5.4 Standardisation et certification

Les trois entités européennes de standardisation CEN[90], ETSI[91] et CENELEC[92] sont regroupées au sein de l'ICTSB (Bureau de standardisation des TIC[93]) où un groupe spécifique, le **NISSG** (Network and Information Security Steering Group[94]) traite les questions de cyberdéfense. Les relations avec le Commission (expression de besoins, suivi, contrats de support) sont assurées par les services de la DG ENTR (voir ci-dessus « 3.1.4 DG ENTR »).

Depuis 2002, la Commission ne cherche plus à intervenir sur les questions de certification de produits et services en matière de cyberdéfense, après une tentative

[88] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:310:0015:0040:FR:PDF
[89] http://ec.europa.eu/information_society/activities/ict_psp/about/index_en.htm
[90] http://www.cen.eu/cenorm/homepage.htm
[91] http://www.etsi.org/WebSite/homepage.aspx
[92] http://www.cenelec.eu/
[93] http://www.ictsb.org/
[94] http://www.ictsb.org/Working_Groups/NISSG/Index.htm

avortée de Directive relative à l'usage des Critères Communs et de communautarisation de l'accord intergouvernemental de reconnaissance mutuelle.

5.5 Développement de capacités militaires de cyberdéfense

Les Institutions européennes, l'EDA dans le cas présent, ne peuvent agir que sur la base d'une vision et d'une volonté partagée entre les Etats-membres. Bien que la cyberdéfense soit une des 10 capacités prioritaires adoptée en mars 2011 pour l'EDA, la réalisation de cet objectif reste entravée par des incertitudes et divergences quant au concept même de cyberdéfense militaire, son enjeu, ses limites, et l'effort que les Etats membres sont prêts à y consacrer.

Tout le monde est bien sûr d'accord sur la nécessité de protéger les moyens de communications et les informations de défense à un niveau cohérent avec leur degré de classification. Mais l'émergence de cyber-capacités offensives développés plus ou moins ouvertement par des Etats ou avec leur soutien pose de nouveaux problèmes.

D'une part, si un pays est soumis à un cyber-attaques stratégique, rien de dit que les systèmes de communication militaires seront les premiers visés : étant en principe parmi les mieux protégé, les attaquants pourront préférer s'en prendre à des infrastructures critiques (énergie, transports, finances, santé…) dont la sécurité est plus difficile à assurer (responsabilités croisées public/privé, manque d'expériences concrètes) alors que leur la paralysie entraverait gravement la vie du pays. Les capacités militaires devraient-elles être sollicitées pour y remédier ? Sous quelle forme, avec quelle responsabilité et quels moyens ?

D'autre part, à partir du moment où des Etats développent des capacités offensives, est-il raisonnable de se priver de moyens équivalents ? Mais qu'elle légitimité peut-il y avoir à l'emploi de telles armes ? Comment peut-on définir un acte de guerre dans le cyberespace ?

Pour que puisse être développée au niveau européen une capacité de cyberdéfense, la première étape consiste à bien connaître la position et les capacités nationales des Etats-membres. C'est ce qu'a entrepris l'EDA dans un appel d'offre à l'été 2011. Il est aussi prévu qu'une équipe de projet (« Project Team ») soit mise en place en novembre 2011.

Il n'est reste pas moins que le volet offensif reste classifié à un niveau élevé dans les pays impliqués et relève plutôt d'une logique de renseignement (on ne peut partager qu'entre égaux). L'approche envisageable pour l'EDA à moyen terme devrait rester limitée à la protection de systèmes d'information militaires, en liaison avec le

développement d'autres capacités prioritaires (« CSDP information exchange » et la « Network Enabled Capability »).

Il est regrettable que le travail conceptuel sur ces questions reste peu développé au niveau européen. L'UEO a mené une étude sur la Guerre Informatique en 2008[95] et le Collège Européen de Sécurité et de Défense a organisé en mai 2011 un cours pilote sur les enjeux européens de la cybersécurité, mais l'Institut européen d'études de sécurité (ISS[96]) ne semble pas très intéressé par ces questions. Tout au plus peut-on noter dans le livre publié en juillet 2009 sur les « ambitions européennes en matière de défense à l'horizon 2020 »[97] (p. 56) que « *des dommages catastrophiques pourront être infligés aux cyber-infrastructures des sociétés postindustrielles … En 2020, la capacité à gérer une cyber-guerre sera vitale pour notre sécurité. Cependant, cette tâche ne sera probablement pas confiée aux militaires et à la PESD* ».

5.6 Lutte contre la cybercriminalité

Dans le cadre du programme « Prévention et Lutte contre la Cybercriminalité » doté de 600 millions d'euros de 2007 à 2013, la DG Home a entrepris une série d'appels d'offre pour financer des actions visant à renforcer la coordination entre les forces de l'ordre (law enforcement)[98].

La cybercriminalité est un des 16 thèmes retenus pour ce programme, suite aux conclusions du « European Cybercrime Training and Education Group » (ECTEG)[99] d'Europol sur la nécessité d'associer les forces de l'ordre, les entreprises, et le monde académique pour mieux assurer une capacité d'anticipation et de réponse rapide à ces menaces.

C'est ainsi qu'a été créé en 2009 un Centre d'excellence en cybercriminalité (2Centre) afin de développer les actions de recherche, d'éducation et de formation. Il rassemble des équipes académiques, industrielles et universitaires en France (Universités de Troyes et de Montpellier 1, Gendarmerie Nationale, Police Nationale, Thalès, Microsoft-France) et en Irlande (University College Dublin, Police nationale, Microsoft-Irland, eBay, Irish Bankink Federation). Il a vocation à être le point de départ d'un réseau européen de centres d'excellence de formation et de recherche dédié à la lutte contre la criminalité informatique, notamment sur le réseau Internet.

[95] http://www.assembly-weu.org/fr/documents/sessions_ordinaires/rpt/2008/2022.pdf
[96] http://www.iss.europa.eu/
[97] http://www.iss.europa.eu/uploads/media/What_ambitions_for_European_defence_in_2020.pdf
[98] http://ec.europa.eu/home-affairs/funding/isec/funding_isec_en.htm
[99] http://www.ecteg.eu/

Mais le principal pôle européen de cybercriminalité reste Europol et son Centre de criminalité en haute technologie (High Tech Crime Centre – HTCC) créé pour mener des actions de coordination, de soutien opérationnel, d'analyse stratégique et de formation. Europol a aussi mis en place une Plateforme européenne de la cybercriminalité (European Cyber Crime Platform – ECCP) qui travaille sur :

- Le système de signalement en ligne des délits observés (I-CROS)
- L'analyse des fichiers (Cyborg)
- Les sujets d'expertise sur Internet et d'expertise médico-légale (I-Forex)

Enfin Europol a adopté en juillet 2011 une série de recommandations sur le futur de la lutte contre le crime organisé en Europe[100] avec en particulier un nouveau modèle fondé sur une coopération entre Europol, Frontex (agence européenne de contrôle aux frontières), le SITCEN et ENISA.

5.7 Protection de la vie privée

Le cadre juridique européen pour la protection des données personnelles est fondé sur la Charte des droits fondamentaux (article 8) et les directives 1995/46[101], 2002/58[102] et 2009/136[103]. Les acteurs principaux sont le Contrôleur européen (EDPS), la DG Justice (voir ci-dessus 3.5.1 et 3.1.2) et le groupe Article 29 (groupe de représentants des autorités nationales défini par l'article 29 de la Directive 1995/46).

L'absence de critères technologiques et opérationnels précis mentionnés dans ces textes entraîne un certain flou quant à leur mise en œuvre, conduisant le groupe 29 à publier régulièrement des « avis »[104] interprétatifs.

Au plan technique, plusieurs voies ont été suivies :

- des travaux de R&D ont été menés sur des technologies améliorant la protection de la vie privée (Privacy Enhancing Technologies – PET[105]) telles qu'anonymisation, pseudonymisation, etc. L'impact commercial reste incertain et la DG JLS (antécédent de la DG Justice) a lancé début 2009 une étude sur un modèle économique des PETS

[100] https://www.europol.europa.eu/sites/default/files/publications/epcc-organisedcrimeconclusions.pdf
[101] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:FR:HTML
[102] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:FR:PDF
[103] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:Fr:PDF
[104] http://ec.europa.eu/justice/data-protection/article-29/documentation/index_en.htm
[105] http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf

- Les services du Contrôleur européen envisagent un système de « Meilleure Technologie Disponible »[106] inspirée d'une approche semblable pour l'environnement

- La Commission a financé de juin 2007 à février 2009 une action pilote pour la mise en place d'un schéma de certification de produits et services favorisant la protection des données personnelles « European Privacy Seal » ou EUROPRISE[107] ; la certification EUROPRISE est maintenant une entité autonome qui accrédite des experts évaluateurs et délivre des certificats (22 délivrés de fin 2008 à septembre 2011)[108]

Mais un pas important a été franchi avec les trois principes retenus dans le cadre de la Directive 2009/136 et portant révision de la Directive 2002/58 : l'utilisation du principe de « Privacy by design » (prendre en compte la questions de protection des données personnelles dès le démarrage des projets) ; certification (utilisation recommandée de produits et service certifiés en matière de protection des données personnelles) ; notification (obligation de notifier les compromission de données personnelles auprès des personnes concernées et de l'autorité national indépendante). Il faudra un certain temps pour que la transposition de cette Directive puis l'application des lois nationales produisent leurs effets.

Au plan juridique, la révision de la directive 1995/46 a été engagée en mi-2009, une proposition de la Commission est attendue fin 2011.

5.8 Administration électronique

Le développement l'administration électronique est considéré comme un enjeu majeur au sein de l'Union[109]. Outre une feuille de route de recherche et développement englobant les 6ième, 7ième et 8ième PCRD[110], la Commission s'est appuyée sur le programme CIP (voir 5.3) pour mettre en place un série de pilotes à grande échelle (LSP) visant à doter l'Europe d'outils interopérables et surs pour une série d'applications de l'administration électronique.

Ces applications portent sur :

[106] Ou Best Available Technologie - BAT
[107] European Privacy Seal, dans le cadre du programme eTEN prédécesseur de CIP, voir https://www.european-privacy-seal.eu/results/deliverables/Final%20Report
[108] https://www.european-privacy-seal.eu/awarded-seals
[109] Voir par exemple les déclarations ministérielles de Manchester (2005) et Malmö (2009)
[110] http://ec.europa.eu/information_society/activities/egovernment/docs/project_synopsis/2005_projects/press_releases/egovrtd2020_press_release.pdf

- l'identification électronique des citoyens (STROK[111], 32 entités de13 pays européens),
- la gestion des marchés publics en ligne (PEPPOL[112], 17 entités de 11 pays européens)
- enregistrement unique en ligne de prestataires de service (SPOCS[113], 33 entités de 16 pays européens),
- échange de données médicales de patients (epSOS[114], 47 entités appartenant à 121 pays européens, plus la Suisse et la Turquie)
- échange de documents juridiques et réglementaires (eCODEX[115] ; 18 partenaires de 13 pays européens, plus la Turquie)

Ces pilotes ont démarré entre 2007 (STORK) et 2011 (eCODEX) et leur état d'avancement respectif a conduit à rechercher une meilleure convergence entre des outils correspondant à un même besoin (transport sécurisé de messages, validation de signatures). C'est aussi le sens du programme ISA[116] (Interoperability Solutions for European public Administration), qui de 2010 à 2015 doit favoriser cette convergence tout en préparant les adaptations règlementaires nécessaires et le développent de standards.

L'Unité H2 de la DG INFSO, en charge du thème administration électronique, supervise aussi des études spécifiques allant dans le sens de la feuille de route : mise en ligne des procédures et documents douaniers (ITAIDE[117]), modélisation des services en ligne pour les administrations locales (PICTURE[118]), programmes coordonnés de R&D pour l'administration électronique (e-Goverment[119]), etc.

5.9 Protection des infrastructures critiques et résilience des infrastructures d'information

Dans le sillage des attaques terroristes utilisant les moyens de transport et des conclusions du Groupe de personnalité chargées de réfléchir sur le rôle de l'Europe en matière de sécurité (voir 2.3 ci-dessus), le Conseil a demandé en juin 2004 l'élaboration d'une stratégie globale pour la protection des infrastructures critiques. Sur la base du *Livre Vert sur un programme européen de protection des*

[111] http://www.eid-stork.eu/
[112] http://www.peppol.eu/News/news/ict-psp-draft-program-additional-peppol-budget/ et http://www.peppol.eu/about_peppol/project_partners/france
[113] http://www.eu-spocs.eu/index.php
[114] http://www.epsos.eu/
[115] http://www.ecodex.eu/
[116] http://ec.europa.eu/isa/actions/index_en.htm
[117] http://www.itaide.org/
[118] http://www.picture-eu.org/project/index.shtml
[119] http://www.egovernet.org/

infrastructures critiques édité par la Commission en novembre 2005, le Conseil « Justice et Affaires intérieures » a décidé en décembre 2005 la mise en place de ce programme placé sous la responsabilité de la DG JLS puis, à partir de 2010, de la DG Affaires intérieures (voir 3.1.3).

Ce programme européen de protection des infrastructures critiques (PEPIC ou EPCIP) comporte un volet stratégique (quelles infrastructures sont critiques ?) et un volet pratique (quels outils et procédures pour les protéger ?).

Au plan législatif et organisationnel, la communication 2006/787 propose un tableau des différents types d'infrastructures critiques, validé par la directive 2008/114[120]. Celle-ci définit la notion *d'infrastructures critiques européennes* (celles … *dont l'arrêt ou la destruction aurait un impact considérable sur deux États membres au moins*…) et les répartit par secteurs : le secteur des TIC comprend 11 sous-secteurs parmi lesquels les réseaux publics de communication et les réseaux dédiés aux actions spécifiques de production et de distribution (Supervisory Control and Data Acquisition Systems – SCADA).

Le recensement des infrastructures à caractère européen a été engagé pour les infrastructures de transport et d'énergie par la directive 2008/114. Il est prévu de l'étendre aux infrastructures de communication au cours de la révision de cette même directive (2011-2012).

Au plan pratique, le programme CIPS (Critical Insfrastructure Protection and Security) s'étend de 2007 à 2013 et dispose de 135 millions d'euros pour la mise au point d'outils, procédures et moyens de protection des infrastructures critiques. D'ores et déjà, une part importante de ces études CIPS est consacrée à la protection des infrastructures d'information, notamment des exercices paneuropéens pour tester les plans d'urgence Internet, l'identification en temps réel des codes malicieux, la modélisation d'interdépendances dans le secteur des ICT, l'étude des partenariats public-privé pour améliorer la résilience des réseaux de communication fixe et mobile.

De son côté, l'Unité A3 de la DG INFSO a engagé un effort important pour améliorer la résilience des infrastructures critiques d'informations, notamment en finançant de 2006 à 2007 l'étude ARECI (Résilience et robustesse des infrastructures de communication) qui a fourni une série de 10 recommandations[121] reprises depuis lors dans le cadre d'études spécifiques de la DG INFSO et dans le programme d'études CIPS.

[120] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:FR:PDF
[121] http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/areci_study/index_en.htm

Elaboré par la DG INFSO, la communication 2009/149 analyse les enjeux et difficultés relatifs à la résilience des réseaux de communication en Europe, et la communication 2011/163[122] préconise un renforcement des coopérations intra-européennes et la mise en place de partenariats stratégiques de dimension internationale.

Cinq volets d'action sont mis en avant[123] :

- Préparation et prévention,
- Détection et réponse,
- Compensation et rétablissement,
- Coopération internationale,
- Critères de qualification des infrastructures dans le secteur des TIC,

L'Unité A3 de la DG INFSO anime aussi deux instances de coordination, le Partenariat public-privé européen pour la résilience (EP3R) et le Forum Européen des Etats membres.

Un effort particulier est fait en faveur d'actions communes coordonnées entre les pays membres, avec la réalisation d'exercices paneuropéens sur des incidents de grande envergure affectant la sécurité des réseaux (Cyber Europe 2010). En 2011 un exercice du même type est mis en œuvre dans le cadre du programme CIPS (Eurocybex, le 27 septembre), ainsi que le premier exercice coordonné entre l'Europe et les Etats-Unis (Cyber Atlantic 2011, le 3 novembre).

On peut aussi noter qu'ENISA est largement mise à contribution pour la mise en œuvre de l'ensemble de ces activités.

[122] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF
[123] http://ec.europa.eu/information_society/policy/nis/docs/comm_ciip/comm_pdf_2009_0149_f_en.pdf

6 Bilan et perspectives

Même si le rôle de certaines personnalités brillantes placées au sein de ces Institutions peut avoir un effet marquant sur les évolutions, d'une manière générale les Institutions européennes ne peuvent agir que sur la base d'une vision cohérente et une volonté commune d'un ensemble suffisamment large de gouvernements des Etats membres (majorité qualifiée ou unanimité).

Lorsque cette vision et cette volonté font défaut, les mandats des organes communautaires restent limités, de même que la portée de leurs actions. Pour ceux qui souhaite faire évoluer les choses, il importante alors de bien identifier les barrières politiques à l'origine de ces limitations. Il ne faut pas non plus sous estimer le poids de la complexité des structures européennes (inépuisable thème de la « comitologie ») et les entraves qui peuvent en résulter.

En matière de cyberdéfense, comme dans bien d'autres domaines, les actions communautaires visent à établir une meilleure cohérence politique et une plus grande interopérabilité des systèmes et applications, tout en renforçant la sécurité générale au sein de l'Union. Les questions de cyberdéfense et de cybersécurité étant abordées dans des domaines très variés, les décisions touchant à la cyberdéfense sont prises au sein de Conseils européens distincts (niveau ministériel). Un bilan des actions communautaires en cyberdéfense est présenté ci-dessous.

Deux remarques préalables.

Les estimations disponibles sur la croissance de l'usage des TIC (pénétration d'Internet au sein des ménages, des entreprises et des administrations par exemple), la fréquence des incidents ou attaques et enfin le coût des dommages subis, indiquent une forte corrélation entre tous ces différents paramètres. Cela montre que les politiques de cyberdéfense et cybersécurité mises en œuvre ne réduisent pas les attaques et leur impact, tout au plus les limitent-elles.

Mais cela montre aussi que le coût croissant de cette insécurité n'entrave pas la généralisation de l'usage de ces technologies : les bénéfices qu'elles procurent aux citoyens, entreprises et administrations (souplesses d'emploi, confort, productivité…) sont en règle générale considérés comme supérieurs aux dommages subis. Avec en corolaire une difficulté permanente à faire valoir des politiques de SSI souvent perçues comme trop complexes et coûteuses.

Le deuxième point tient en un paradoxe. Au départ, la sécurité de l'information associée aux techniques de cryptographie touchait aux activités de renseignement. Et dans ce domaine, on ne collabore et on n'échange qu'entre égaux.

Le développement d'Internet ouvrant l'usage des outils cryptographiques à tous, l'élargissement des enjeux de sécurité (réseaux, intégrité et disponibilité de l'information) et l'ubiquité des menaces ont rendu nécessaire une large collaboration entre les organismes en charge de la cyberdéfense. Ceci reste vrai pour les menaces d'origine ludique, criminelle voire terroriste.

Mais à partir du moment où se développent des menaces « stratégiques », c'est-à-dire d'origine plus ou moins directement étatique, la problématique a tendance à revenir à la logique du renseignement. Ainsi l'ouverture à des réseaux toujours plus interconnectés et des applications plus diversifiées pourraient conduire à un resserrement des coopérations étatiques en matière de cyberdéfense.

Il suffit de voir le faible niveau des coopérations européennes en matière de renseignement pour comprendre qu'il y a là un problème particulier quant au rôle que les Institutions européennes pourront jouer en matière de cyberdéfense, au moins dans l'horizon prévisible.

6.1 Bilan

Un certain nombre d'activités de cyberdéfense au sein des Institutions européennes peuvent se prévaloir d'un bilan positif.

Le **Programme de Recherche et Développement** a su intégrer pleinement la thématique de sécurité (voir 5.2), y compris les questions de cyberdéfense et cybersécurité, au sein du 7ième PCRD. Même si le volume financier du PCRD reste faible par rapport au financement total de R&D en Europe, il constitue un moteur puissant de coopération entre les parties prenantes européennes (chercheurs publics et privés, industries, utilisateurs) avec un partage d'outils, de procédures et de savoir faire.

Les travaux sur l'**administration électronique** ont bénéficié depuis 2005 d'une adhésion politique générale au niveau des gouvernements. Ils ont donné lieu à la mise en œuvre de programmes de grande ampleur (LSP) sur des thèmes diversifiés (voir 5.8). Bien qu'ils ne soient pas encore achevés, ils conduisent d'ores et déjà à la mise en place d'applications viables, interopérables et sécurisés et à l'adoption de nouveaux standards. Ces applications pourraient à terme s'étendre à d'autres applications que l'administration électronique et à d'autres zones que l'Europe.

Les études sur la **résilience des infrastructures critiques d'information** constituent aussi un élément positif de l'action des Institutions européennes. Ces travaux s'inscrivent dans le double sillage, d'une part du cadre réglementaire du marché des communications électroniques (voir 5.1) en complétant les aspects sécurité esquissés dans les Directives, d'autre part du programme PEPIC de protection des infrastructures critiques (voir 5.9). ENISA s'est vu confié un rôle pilote dans ces études, d'abord pour une analyse de l'état de l'art et une concertation approfondie avec les parties prenantes, puis pour l'élaboration d'outils et de bonnes pratiques mieux harmonisées.

D'une manière un peu analogue, le rôle des Institutions européennes dans la **lutte contre la cybercriminalité** a pu s'affirmer du fait de deux facteurs : d'une part l'adoption de la Convention internationale du Conseil de l'Europe en 2001 (même si tous les Etats membres ne l'ont pas encore ratifiée), d'autre part l'existence d'une structure adaptée à sa prise en compte (Europol). Il ne s'agit pas de créer une nouvelle structure opérationnelle visant à coordonner, encore moins suppléer les structures nationales existantes, mais plutôt de mettre en place un réseau de

contacts et des outils d'échange de données et d'alerte plus efficaces. Ces réseaux et outils sont trop récents pour en faire dès à présent un bilan précis.

La même situation se présente en matière de **protection des données personnelles**. Disposant traditionnellement d'un soutien politique affirmé au sein du Parlement, ce thème est un élément notable de la Charte des Droits Fondamentaux et reste indissociable de la problématique de la défense et la cybersécurité. Les premières étapes (groupe de concertation entre les autorités nationales, études sur les PETs, schéma de certification Europrise) ont marqué des avancées importantes sans pour autant bouleverser les pratiques. Les trois principes retenus dans la Directive 2009/136 (privacy by design, certification, notification) devraient, lorsqu'ils auront été pleinement mis en œuvre, changer le paysage, mais là aussi il est encore trop tôt pour en tirer un bilan.

Parmi les programmes dont le résultat est plus discutable, on peut citer celui de la **protection des infrastructures critiques,** malgré l'ampleur du programme CIPS et la mis en place d'un réseau de point de contacts CIWIN (voir 5.9). Plusieurs raisons à cela : d'une part la distinction entre les infrastructures nationales et les infrastructures européennes n'est pas toujours simple à faire, ne serait ce que parce que les secteurs concernées sont maintenant déréglementés et donnent lieu à des nombreuses fusions et coopérations transfrontalières entre opérateurs privés. D'autre part, ce thème est placé sous le volet général de la lutte contre le terrorisme ce qui est très justifié pour le secteur des transports, mais le paraît beaucoup moins pour les systèmes d'information, bancaires ou de santé.

Un autre bilan pas encore convainquant est celui de la mise en œuvre d'une **politique de cyberdéfense et cybersécurité au sein même des Institutions européenne**s. Dix ans après l'adoption des premiers règlements, l'ensemble des éléments nécessaires à une protection efficace ne sont pas encore en place : le CERT-EU en est encore au stade probatoire et la culture de cybersécurité reste peu répandue hors des services spécialisés.

Reste la question de la **capacité militaire de cyberdéfense** (voir 5.5), qui là aussi est trop récente pour qu'il soit possible d'en faire un bilan. On peut simplement noter que l'EDA commence par le commencement avec d'une part le lancement d'une première étude pour analyser la situation de la cyberdéfense au sein des Etats membres, d'autre part la mise en place d'une équipe projet (Project Team). Sans anticiper les résultats de l'étude, les différences de conception et de stratégie entre les Etats membres risquent d'être une source de difficulté.

6.2 Perspectives

La disparité de stratégies et de moyens entre les Etats membres en matière de capacités militaires de cyberdéfense pourrait nécessiter un **travail de concertation** et une recherche de compromis. Pour un pays qui aura su dégager une position nationale claire, *a fortiori* la faire partager par quelques partenaires choisis, ceci pourrait être une bonne occasion de promouvoir sa position au plan européen.

Une des questions auxquelles les Etats membres et les Institutions européennes pourraient être ainsi confrontés est celle de la **frontière entre les domaines civil et militaires**. Il peut s'agir bien sûr de la capacité des systèmes militaires à utiliser à

bon escient les opportunités techniques et en matériel développées sur le marché civil (télécommunications spatiales par exemple). Mais il peut s'agir aussi de cyber-menaces stratégiques qui pourraient viser des structures non-militaires et pour lesquelles l'intervention de capacités militaires d'analyse, de réparation ou de riposte pourraient être requises (ce point est cité dans le politique de cyberdéfense de l'OTAN). Quant à la formalisation d'un pontage au niveau européen entre les secteurs civils et militaires en matière de cyberdéfense, ces questions sont trop complexes en pratique et les approches trop diversifiées entre Etat membres pour qu'il soit raisonnable de l'envisager à court terme.

D'ici 2013, un nouveau **mandat d'ENISA** doit être établi, en révisant les limites de son champ de compétences. Celui de 2004 restait circonscrit au premier pilier, excluant toute question relevant de la sécurité intérieure et de la défense, ainsi que toute activité à caractère opérationnel. Les choses ont commencé à évoluer, notamment pour ce qui concerne la cybercriminalité où Europol a proposé un échange d'information avec FRONTEX, SITCEN et ENISA.

Quant à une plus forte intégration de la cyberdéfense et le cybersécurité au sein des Institutions européennes, elle paraît difficile avec un bilan aussi diversifié : pour chaque thème d'activité, les réussites comme les échecs sont très liés au niveau de cohérence entre les points de vue politiques des Etats membres, qui varient d'un thème à l'autre. Quant à un allègement des structures, il est limités par les règles européennes de concertation, d'élaboration de textes et de prise de décision, qui ne peuvent évoluer que de manière globale, pas pour un thème spécifique.

Annexe : Possibilités d'implication des acteurs nationaux dans les questions de cyberdéfense et cybersécurité au sein des Institutions européennes

Il n'y a pas de mode d'implication des acteurs nationaux spécifique à la cyberdéfense. Les modes d'implication décrits dans ce chapitre sont bien sur aussi applicables à la plupart des autres thèmes d'activité européenne.

D'une manière générale, les services du Secrétariat Général aux Affaires Européennes (SGAE) à Paris et de la Représentation Permanente de la France à Bruxelles sont à même de soutenir les efforts pour renforcer l'implication de français dans les activités des Institutions européennes.

1. Consultations

La Commission pratique beaucoup les consultations publiques en ligne, notamment suite à la publication de communications en vue de préparer des résolutions ou des directives, ou lors de changements à préparer (évolution du statut d'ENISA par exemple, ou prolongement de l'initiative i2010 sur la période 2010-2015).
Les thèmes ouverts à consultation sont rassemblés sur un site spécifique de la Commission[124].

2. Experts auprès de la Commission

Les instances européennes fait couramment appel à des experts pour des actions spécifiques sur la base de listes constituées au préalable, notamment :

- La DG Justice sollicite des experts dans les différents domaines dont elle a la responsabilité, tels que **Safer-Internet**[125] (expertise rémunérée)
- Ce sont toujours des experts extérieurs qui procèdent à l'évaluation des propositions et/ou à des revues annuelles des projets financés dans le cadre **des programmes cadres de R&D**. Pour devenir expert évaluateur, il faut s'inscrire au préalable dans la base de données d'experts du FP7[126] où les DG concernées sélectionnent les experts dont elles ont besoin à chaque nouvel appel à projet. Ces travaux d'expertise sont rémunérés (450€/jour en 2009) et les frais de déplacement remboursés.
- Les priorités nationales pour les thèmes du PCRD sont préparées au plan national au sein des GTN (**Groupe Thématique Nationaux**) ouverts aux

[124] http://ec.europa.eu/yourvoice/consultations/index_en.htm
[125] http://ec.europa.eu/information_society/activities/ict_psp/cf/sip/login/index.cfm
[126] https://cordis.europa.eu/emmfp7/index.cfm

parties prenantes. Les aspects de cyberdéfense et cybersécurité sont traités par le GTN TIC[127] et le GTN PERS. L'articulation entre le niveau national et le niveau européen est assurée par les Points de Contact Nationaux[128] et le Service Français d'Accès à l'Information sur la Recherche en Europe (EUROSFAIRE)[129]

- Pour le programme ICT du PCRD, outre le Comité de programme, la Commission s'appuie aussi sur un Comité d'orientation et de suivi (ou Advisory Group) : **ISTAG**[130]. Les membres d'ISTAG sont nommés par la Commission et rémunérés.
- Pour le volet Sécurité du PCRD, la Commission s'était appuyée sur un comité européen d'orientation et de suivi : **ESRAB**[131] dont les membres était nommés par la Commission *intuitu personae*. Ils n'étaient pas rémunérés mais leurs frais étaient remboursés.
- L'organisation d'ENISA inclut un Groupe Permanent des Parties prenantes (**PSG**) qui propose des orientations et assure un suivi des actions. Les membres du PSG sont nommés à titre personnel pour 2 ans et demi par le Directeur d'ENISA[132]. Leurs travaux ne sont pas rémunérés, leurs frais sont remboursés.

3. Experts désignés par leur pays les représenter au sein des Institutions européennes

- Pour la préparation, les orientations et le suivi de ses programmes, la Commission s'appuie sur un **Comité de programme** composé d'experts désignés par les Etats membres (en France, sous couvert du SGAE) :
  - Comité de programme CIPS : Jacqueline Turc, services du HFDS ministère de l'Industrie pour le programme (changement prévu au printemps 2012)
  - Comité de programme FP7-ICT : Patrick Schouller (ministère Industrie), Alain Brenac (ministère Recherche), Caire Ferte (UBIFrance)
  - Comité de programme FP7-PERS : Raphaël Prenat (ministère Recherche), François Murgadella (Ministère de la Défense – DGA), Olivier Fuhanno (ministère de l'Intérieur)
- Les agences européennes sont supervisées par un Conseil d'administration où siègent souvent des représentants nationaux. Dans le cas d'ENISA, le Directeur de l'ANSSI a été désigné pour occuper le siège de la France

[127] http://www.eurosfaire.prd.fr/index-gtn.htm l
[128] http://www.eurosfaire.prd.fr/7pc/doc/PCN-7PC_18-05-2009.pdf
[129] http://www.eurosfaire.prd.fr/7pc/pcn.php
[130] http://cordis.europa.eu/fp7/ict/istag/home_en.html
[131] http://ec.europa.eu/enterprise/policies/security/files/esrab_report_en.pdf ainsi que http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:191:0070:0072:EN:PDF
[132] http://www.enisa.europa.eu/pages/03_03.htm

Les relations du gouvernement et de l’administration française avec les Institutions européennes sont supervisées par le Secrétariat général aux Affaires Européennes (SGAE) qui en assure le suivi et la cohérence

4. Experts nationaux détachés

Les Institutions européennes accueillent des experts nationaux détachés (END) qui viennent travaillent sur place, pour une durée de trois ans, éventuellement quatre[133].

Pendant cette période, les END doivent rester administrativement affiliés à un organisme qui assure leur salaire, la Commission leur versant une indemnité mensuel complémentaire en fonction de l'éloignement de leur lieu d'origine. Les END travaillent sous la direction d'un fonctionnaire européen, ils ne peuvent pas représenter la Commission.

En principe, les END ont vocation à retourner travailler dans leur pays d'origine et y favoriser les interactions avec les instances européennes.

5. Participation à des projets d'étude ou de recherche

Des études financées soit dans le cadre de programmes structurés, soit ponctuellement (*funding opportunities*), sont régulièrement proposées par la DG INFSO[134] et la DG Justice[135].

Pour ce qui concerne le PCRD, les appels d'offre sont regroupés par thèmes et publiés à raison de une à deux fois par an.
Le Service Français d'Accès à l'Information sur la Recherche Européenne (EUROSFAIRE[136]) aide à diffuser ces appels d'offres auprès des équipes françaises, ainsi qu'à la préparation de propositions compétitives. Il s'appuie sur les points de contact nationaux (PCN) répartis par thème (ICT[137] et PERS[138] pour la SSI).
L'EUROSFAIRE organise régulièrement des réunions de présentation et de promotion sur les appels d'offre en cours.

[133] http://ec.europa.eu/civil_service/job/sne/index_fr.htm#1
[134] http://ec.europa.eu/information_society/newsroom/cf/news.cfm?item_type=fo&item_subtype=tenders&itemTime=future&currentPage=2
[135] http://ec.europa.eu/justice/grants/index_en.htm et http://ec.europa.eu/justice/contracts/index_en.htm
[136] http://www.eurosfaire.prd.fr/7pc/
[137] http://www.eurosfaire.prd.fr/7pc/ict/
[138] http://www.eurosfaire.prd.fr/7pc/security/