Troisième partie – Opportunités pour l'Europe : pistes de réflexion stratégique

Les questions de surveillance, de défense et de sécurité dans le cyberespace posent aujourd'hui de nombreux défis à l'Europe, dont la devise initiale reste la circulation des biens, des personnes et des idées sur son territoire, et la création d'un marché ouvert. L'application de ces principes sur l'Internet devrait *a priori* orienter les politiques européennes vers la promotion d'une ouverture du réseau avec un minimum de cadres et de restrictions. Néanmoins, nous avons vu que les enjeux de sécurité, de défense, et quelquefois d'intérêt national, suscitent, à rebours, des interrogations sur les capacités des Etats à filtrer les flux entrant et sortant sur leur territoire, et ainsi remettre du contrôle à leurs frontières, quelle que puisse être leur définition pour le cyberespace. Ils soulèvent aussi des questions sur l'importance ou non de la localisation des données pour leur sécurisation – une donnée chiffrée est-elle sécurisée quelle que soit sa localisation ? – et des thématiques afférentes sur les moyens de protections techniques possibles pour protéger un ensemble d'institutions et de sites stratégiques.

Or, la difficulté de cette dynamique de sécurisation est d'assurer un ratio entre sécurité et communication. En clair, un système fermé, de type Intranet, semble *a priori* protégé de toute attaque extérieure (hors erreur ou négligence humaine), mais il est également inopérant, puisqu'il coupe l'usager de l'Internet. Plus les filtres techniques sécurisant un système sont forts, plus le système perd de sa vitesse et de sa rentabilité. La bonne stratégie repose ainsi sur la capacité à mettre en place le degré de sécurisation nécessaire à l'utilisateur en tenant compte des risques qu'il est prêt à consentir pour une utilisation optimale du Net. Enfin, ce volet technique pose là encore le problème du rapport de force existant au niveau international entre des Etats disposant sur leur territoire d'un haut niveau de technicité et de recherche par rapport à d'autres restant dépendants de l'offre extérieure. Il est donc important de penser la sécurité dans l'ouverture pour ne pas accroître la fragmentation et finir par s'enclaver sur le réseau, ce qui a des conséquences adverses. Cela suppose de définir en amont le niveau de risque acceptable et consenti qui permette d'assurer le bon *ratio* sécurité/circulation.

Car la sécurité engendre des coûts à plusieurs niveaux :

- Au niveau financier. De fait, la sécurisation d'Internet est devenue en quelques années un marché important et disputé, qui a vu l'émergence de nombreux acteurs

(Kaspersky, McAfee, Norton, etc.). Les failles de sécurité peuvent avoir de graves conséquences pour une entreprise en terme de productivité ou d'image (sabotage, perte d'information stratégique sur ses projets ou sur sa clientèle, etc.). Aussi, les contrats dans ce domaine ont-ils une forte tendance à la hausse, et le processus ne risque pas pour le moment de s'inverser.

- Aux niveaux de la créativité et de l'innovation, car si la sécurité suppose de réduire les dangers, elle peut donc brider la nouveauté, synonyme de prise de risque. Elle semble donc aboutir à étouffer la créativité.
- Au niveau de la performance. Cela est particulièrement visible sur le plan industriel, où, pour répondre aux exigences de sécurisation, ont été mis en place les SCADA (*Supervisory Control And Data Acquisition* ou systèmes de contrôle et d'acquisition des données). Or, ces systèmes font apparaître de nouvelles difficultés techniques et juridiques dans le cadre, par exemple, de firmes transnationales qui doivent adapter leur SCADA à cette configuration internationale. Les frontières nationales, vues ici sous l'angle industriel, ne sont plus des remparts défensifs mais au contraire, semblent devenir des obstacles à la cybersécurité de l'entreprise. La sanctuarisation nationale n'est pas compatible ici avec la compétitivité dans une économie globale et peut même dans le cas de firme multinationale être perçue comme un frein à la bonne sécurisation des entreprises.

Il est donc nécessaire de penser la sécurité à l'échelle européenne en termes de gestion du risque, c'est-à-dire en maintenant un équilibre entre sécurité et circulation, en accord avec les valeurs de l'Union européenne. Ceci implique de définir des priorités stratégiques prenant en compte différentes dimensions, quelquefois contradictoires, que sont la sécurité, la liberté, la souveraineté, les opportunités économiques ou encore le futur du réseau. Nous présentons ici quelques pistes de réflexion techniques et politiques.

1 Les pistes de réflexion techniques

1.1 La fragmentation du web comme stratégie de protection

La messagerie électronique est un outil qui est devenu indispensable, à la fois dans les échanges professionnels et les échanges privés.

Actuellement, aucune solution, au niveau des protocoles de l'Internet, ne propose une authentification de l'émetteur des messages électroniques. Seules des fonctions et applications complémentaires, parfois mal intégrées, gèrent cette authentification à l'aide d'un certificat de signature électronique. Des solutions anti-phishing comme DKIM permettent l'authentification du nom du domaine de l'émetteur et l'association entre celui-ci et le serveur de messagerie associé. C'est un début de solution, mais qui est limité et très insuffisant pour instaurer la confiance.

Les extensions de sécurité du protocole SMTP permettent d'établir un lien sécurisé (TLS/SSL) mais seulement de façon optionnelle et la plupart des ISP n'obligent pas à sa mise en place. En conséquence, les mots de passe d'accès aux serveurs POP ou IMAP transitent en clair (sans cryptage) sur le réseau et peuvent être aisément capturés, permettant ainsi l'usurpation du compte e-mail. De même, le contenu des messages est également transmis en clair sur le réseau.

La plupart des opérateurs de confiance et les ISPs rejettent le plus souvent l'idée de la confidentialité, sous le prétexte d'inutilité, de complexité ou de risque de perte des données sur le long terme. En fait, la crainte de voir la plupart des utilisateurs transférer des messages indéchiffrables (ou presque) semble être à l'origine de ce rejet. Pour ces raisons, les opérateurs de confiance ont émis des certificats de signature électronique de classe III qui ne peuvent pas être utilisés pour crypter un message.

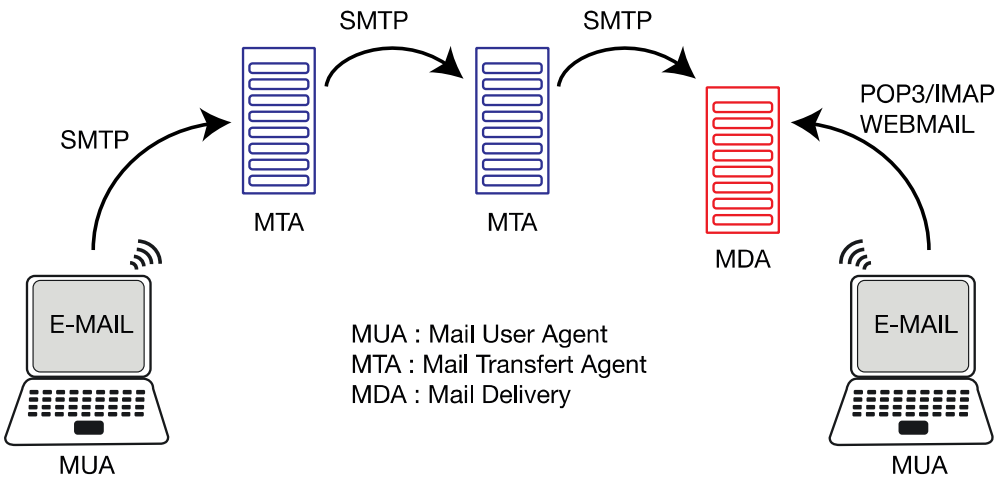
Les arguments liés à la durée de vie du certificat et à la complexité de gestion d'un mécanisme de récupération de clés appelé « key recovery » par le tiers de confiance ont été les bases de ce choix. Pourtant, le besoin de confidentialité est important et nécessaire afin de pouvoir transférer des documents en toute confiance, que ce soit pour des données sensibles comme de nouveaux développements de brevets, des courriers d'avocats, des chiffres confidentiels… La question de la confidentialité deviendra une question encore plus épineuse avec le développement du « *cloud computing* » dans lequel les données pourront être situées n'importe où dans le monde sans protection quant à leur accès par des tiers.

L'objectif de la confidentialité n'est pas la dissimulation, mais la sécurité des informations contenues dans des messages électroniques ou dans des documents. Aucune fonction de protection du contenu des messages n'étant en place dans les protocoles et la traçabilité des messages étant déficiente, il est particulièrement aisé d'altérer le contenu d'un message pour en modifier le sens. Particulièrement lors des transferts de messages, n'importe quel utilisateur se rend compte qu'il peut modifier le contenu du message qu'il a reçu et qu'il veut transférer.

En utilisant la fonction de son client de messagerie « transférer » (*forward*), le message d'origine est affiché et modifiable aussi simplement que la rédaction d'un message. Dès lors, il suffit de l'imprimer une fois modifié pour prétendre avoir reçu un message contenant ces éléments modifiés. Ce phénomène se rencontre souvent lors de la présentation en justice d'impression de messages prétendument reçus dont le contenu a été volontairement altéré.

1.1.1 Comment fonctionne une messagerie Internet ?

Fig. 10 – Schéma fonctionnement messagerie



L'utilisateur dont l'adresse est « emetteur@chezmoi.com », sur son poste de travail, va rédiger un message pour un utilisateur «user@domaineloin.com». Son logiciel de messagerie va transmettre ce message, en général, au serveur d'envoi (SMTP) de son domaine : « smtp.chezmoi.com ». Ce serveur va analyser la demande et en particulier

l’adresse du destinataire «user@domaineloin.com». Il va donc essayer de contacter le domaine « domaineloin.com » et lui demander par une requête DNS quelle est l’adresse de son serveur de messagerie, qu’il trouve dans le contenu de la table DNS (champ MX).

Le DNS est le mécanisme hiérarchique au niveau mondial qui permet d’associer un nom « lisible » et compréhensible par un humain, à l’adresse IP de l’ordinateur en question (ex : 213.186.33.5 en IPV4). Selon le cas, il peut avoir une réponse lui donnant directement l’adresse du serveur dont il s’agit, ou le nom d’un serveur « *relay* » qui, lui, pourra accéder au serveur de destination sollicité.

Le serveur « smtp.chezmoi.com » va donc établir une session avec soit le serveur de destination « smtp.domaineloin.com », soit avec un serveur « *relay* », et lui transmettre le message en y ajoutant des informations de ‘transit’ telles que son adresse IP et les date et heure de passage (« *timestamp* »).

Le serveur « smtp.domaineloin.com » recevant la demande, va vérifier s’il existe bien un utilisateur nommé « user » dans son domaine. Si tel n’est pas le cas, il renvoie un message d’erreur à l’émetteur du message, via le serveur SMTP émetteur (smtp.chezmoi.com).

Remarque : il convient de noter que dans le cas où l’adresse de l’émetteur n’existe pas ou est erronée, le message risque de générer des aller-retours entre les deux serveurs SMTP en boucle. C’est ce qu’on appelle le « bouncing ».

Si l’utilisateur existe bien dans son domaine, le serveur SMTP « smtp.domaineloin.com » va transmettre au MDA local (*Message Delivery Agent*) le message afin qu’il soit stocké dans l’attente de sa consultation par le destinataire.

Enfin, le destinataire, à partir de son poste de travail et de son client de messagerie (MUA), va se connecter sur le MDA via un des protocoles les plus courants, POP3 (Post Office Protocol) ou IMAP4 (Internet Message Access Protocol) pour aller télécharger ou consulter le message qui lui a été envoyé. Pour ce faire, il s’authentifie auprès du serveur (MDA) avec son e-mail (ou nom d’utilisateur) et son mot de passe, avant de pouvoir consulter son message.

Il est important de noter que le protocole SMTP a été conçu pour un environnement connecté de bout en bout, ce qui implique le fonctionnement permanent des serveurs de messagerie SMTP et l’existence des MDA (serveurs POP ou IMAP) pour accepter en permanence les messages alors que l’utilisateur n’est pas toujours connecté.

1.1.1.1 Structures des messages

Le fonctionnement historique de l'Internet et en particulier des serveurs SMTP, implique que seuls des caractères ASCII sur 7 bits sont acceptés par ces serveurs.

En conséquence, les envois sont transcodés de l'ASCII 8 bits vers l'ASCII 7 bits afin de pouvoir être transmis correctement, selon différents modes de codage de caractères, ce qui peut générer des erreurs de transcriptions lors de la réception (caractères accentués, étrangers..). Ceci devient d'autant plus flagrant que l'utilisation de l'Unicode peut entraîner des confusions supplémentaires qui sont largement utilisées par les « spammeurs ».

Les fichiers attachés sont généralement codés avec les extensions MIME (Multipurpose Internet Mail Extensions : RFC 2045 et 2046). Le codage des caractères fait parfois appel également à ces extensions.

Les références des protocoles de messagerie principaux sont les suivants :

• SMTP : RFC 5321

• POP3 : RFC 1939

• IMAP4 : RFC 3401

• Structure des messages : RFC 2822

• En-têtes des messages : RFC 5322

1.1.2 Types de messageries

On peut séparer le fonctionnement des messageries selon trois modes distincts :

1.1.2.1 Messageries d'entreprises :

Dans le cas des messageries d'entreprises, le(s) serveur(s) de messagerie SMTP sont hébergés au sein de l'entreprise elle-même et accessibles en permanence. Souvent, celles-ci sont du type Microsoft Exchange ou Lotus Domino, et moins fréquemment des produits comme Zimbra. Avec ce type d'architecture, les fichiers de messagerie sont conservés sur le serveur et les utilisateurs y accèdent directement via leur client de messagerie (Outlook, Notes…). Parfois, des copies de ces données sont répliquées sur le poste de travail, mais ce n'est pas systématique.

1.1.2.2 Client de messagerie utilisateur final :

Cette catégorie représente la plus grande partie des messageries utilisées à ce jour.

Le serveur de messagerie (MDA) est hébergé chez le fournisseur d'accès ou de gestion du domaine (chez l'ISP). L'utilisateur utilise le client de messagerie de son poste de travail pour accéder via les protocoles POP ou IMAP au contenu de sa messagerie stockée sur les serveurs (MDA). Pour IMAP, les messages sont simplement consultés localement mais conservés sur les serveurs, alors qu'avec le protocole POP, les messages sont téléchargés sur le poste de travail du client.

1.1.2.3 Fonctionnement distant (Webmail) :

Enfin, de plus en plus fréquemment, l'usage de serveurs distants accessibles essentiellement par un navigateur Internet, est employé par les particuliers. Dans ce cas, comme pour le protocole IMAP, les messages sont consultés à distance avec le navigateur et restent stockés sur le serveur en question (ex : Gmail, Yahoo, Hotmail…)

Dans les deux cas, on constate une forte majorité d'utilisateurs des logiciels Microsoft Outlook qui sont livrés soit avec le système Windows (Outlook express) soit avec Microsoft Office (Outlook 2000 à 2010). La part des « *webmails* » devient de plus en plus importante.

1.1.3 Les protocoles de messageries

Les RFC (*Request For Comment*) représentent la manière de normaliser les protocoles de l'Internet. Aux débuts de l'Internet, lorsque les protocoles d'échange ont été conçus, il a été nécessaire de les valider, puis de les améliorer au cours du temps. C'est ainsi que sont nés les RFC pour gérer les propositions et demandes d'amélioration des protocoles déjà en cours d'utilisation. Ceci a permis une accélération sensible de la mise en œuvre puis du développement de ces protocoles, et en particulier de TCP/IP. Par comparaison, en Europe, le principe a été différent : des ingénieurs ont commencé par rédiger des normes d'échange (X25) pendant plusieurs années afin de les normaliser. Puis, il a été demandé aux constructeurs de concevoir et fabriquer des matériels respectant ces normes, ce qui a encore demandé plusieurs années. Enfin, il a fallu mettre en œuvre tous ces matériels et normes autour d'un réseau physique de communication. Ces lourdeurs et le temps passé à normaliser ont eu pour conséquences tout d'abord un retard du démarrage des réseaux de communication entre ordinateurs et d'autre part un coût très élevé des systèmes de connexion proposés.

Ceci, entre autres, explique le rapide développement de TCP/IP aux dépens de X25.

Les principaux protocoles de messagerie que nous analyserons plus en détail sont les suivants :

• SMTP : RFC 5321 (anciennement 2821)

• POP3 : RFC 1939

• IMAP4 : RFC 3401

• Structure des messages : RFC 2822

• En-têtes des messages : RFC 5322

1.1.3.1 Le protocole SMTP

Simple Mail Transfer Protocol. Ainsi que son nom l'indique est un protocole très simplifié pour la transmission de messages en texte clair envoyés sur un lien permanent, c'est-à-dire entre plusieurs machines toujours présentes et actives sur l'Internet. Son ancienneté explique sa simplicité, car aux débuts de l'Internet on ne se préoccupait pas des problèmes de sécurité et encore moins des aspects liés à l'identification des émetteurs de messages. Le « spam » n'existait pas et les utilisateurs recevaient peu de messages. Sa simplicité explique également son succès et la vitesse de sa mise en œuvre dans l'Internet, car il est facile à implémenter dans un programme, et on trouve encore actuellement certains petits programmes le mettant en œuvre de façon simpliste, mais respectant l'ensemble des règles décrites dans son RFC initial 821, mis à jour par le RFC 2821 puis par le RFC 5321. Tous les MTAs (*Message Transfer Agent*) respectent cette RFC et le protocole SMTP.

De fait, ils en héritent les faiblesses intrinsèques ainsi que les éventuels problèmes d'implémentation. Plus précisément, le mécanisme de ces serveurs est basé sur un ou plusieurs fichiers de configuration au format texte (en clair) qui peut être facilement modifié dès lors que l'on peut avoir accès à l'ordinateur sur lequel il se trouve.

En fait, ces fichiers de configuration sont si « touffus » et complexes qu'il est peu recommandé d'éditer directement ceux-ci, en particulier le fichier de configuration principal du logiciel le plus répandu : « sendmail.cf ». Pour éviter les éventuels problèmes de configuration, un macroprocesseur pour modifier le fichier « sendmail.cf ».

1.1.3.2 Les protocoles POP et IMAP

Les MDAs (*Message Delivery Agent*) sont le plus souvent des serveurs supportant les protocoles POP6 et IMAP7 afin de permettre aux utilisateurs de se connecter de façon épisodique pour relever leurs messages de la même manière que nous allons chercher notre courrier papier dans notre boite aux lettres. Historiquement, les premiers MDAs stockaient

simplement les fichiers de façon individuelle dans des sous-dossiers du dossier personnel du destinataire, sur le disque dur de destination, qui était en permanence connecté. L'évolution de ces systèmes et la diffusion de l'Internet auprès des PME et des particuliers a développé la connectivité intermittente et, donc, l'usage des serveurs POP et IMAP. Les mécanismes de ces deux protocoles sont sensiblement différents. Initialement, seul le protocole POP existait et sa simplicité résidait dans le peu de fonctions qu'il comportait, essentiellement la connexion avec « login et mot de passe » et le téléchargement séquentiel des messages conservés sur le serveur. Puis, le développement de l'Internet a nécessité d'une part, des extensions successives au protocole POP : POP3 qui comporte des extensions de type UIDL pour identifier les messages ; POP-AUTH pour authentifier l'utilisateur, ou encore l'établissement d'un lien SSL entre le client et le serveur. Et d'autre part, la mise en œuvre d'un nouveau protocole, IMAP (actuellement IMAP4), pour gérer de façon plus étendue les fonctionnalités de la messagerie, en particulier le stockage permanent des messages sur le serveur et leur consultation distante. Le principe était lié à la faible vitesse des liens de transmission existants alors pour les particuliers, associée à l'augmentation du nombre et de la taille des messages transmis. Ce protocole évitait ainsi le téléchargement systématique des messages sur le poste de travail et la gestion distante de ces messages. Les évolutions actuelles en termes de vitesse des liens et les aspects liés à la confidentialité des données réduisent, de mon point de vue, sensiblement l'intérêt de ce protocole. Nous considérons que l'amélioration des fonctions sur le poste de travail au sein du logiciel « client » de messagerie est préférable, dès lors que l'on sécurise les fonctionnalités du protocole POP3. En effet, la conservation sur le serveur distant de l'ensemble des messages peut générer de nombreux risques :

- Difficulté de sauvegarde des données et risque de perte d'informations,
- Disponibilité des messages lorsque l'ordinateur n'est pas connecté à l'Internet,
- Plus grande facilité d'accès pour des tiers malveillants,
- Risques liés à la confidentialité des données présentes sur le serveur : au moins les administrateurs du serveur peuvent avoir accès au contenu des messages.

1.1.4 Points de faiblesses techniques des protocoles

1.1.4.1 Le protocole SMTP

Parmi les points de faiblesse que l'on retrouve dans les caractéristiques du protocole SMTP, il faut noter principalement les suivants :

• L’absence d’obligation de sécurisation du lien : les connexions au serveur SMTP sont le plus fréquemment réalisées en clair, sans vérification de l’adresse du serveur, facilitant ainsi d’une part, la possible récupération de mots de passe et d’autre part la possibilité de *spoofing* ou d’attaque « *man in the middle* ».

• L’authentification non systématique de l’émetteur sur le serveur : on voit souvent des messages émis avec un nom apparent qui est un leurre, comme par exemple le nom du destinataire lui-même.

• L’envoi de mots de passe en clair : la connexion au serveur se fait sans sécurisation du lien, mais de plus, les mots de passe sont transmis tel quels directement, lorsque le serveur SMTP demande une authentification, ce qui est peu fréquent.

• Un horodatage non fiable et facile à modifier : les dates et heures enregistrées dans les en-têtes des messages dépendent directement de l’heure des serveurs SMTP par lesquels ceux-ci transitent. Or, il est fréquent que ces serveurs ne disposent pas d’une heure correcte, ou celle-ci peut être aisément modifiée.

• L’absence de fonction garantissant l’intégrité du message transmis : le protocole SMTP n’ajoute aucun mécanisme de vérification de la bonne réception des messages, et en particulier de leur intégrité qui peut être altérée au cours des différents relais.

• La possibilité d’envoyer des messages sans nom ou adresse e-mail d’émetteur : Pour des raisons de gestion des messages de retour d’erreur, le protocole SMTP impose la possibilité d’envoyer des messages sans nom d’émetteur, ce qui est une grave erreur et facilite l’anonymat du « spam ».

• L’utilisation de la fonction VRFY pour obtenir des adresses e-mails distantes : cette fonction permet d’obtenir un retour du serveur SMTP de destination sur l’existence d’une adresse électronique sans même envoyer de message, ce qui autorise un robot à tester un ensemble important d’adresses dans un domaine jusqu’à ce qu’il obtienne des adresses valides, augmentant ainsi les possibilités de « spam ».

• L’absence de vérification des DNS émetteurs : le protocole SMTP ne vérifie pas que l’émetteur et son éventuel serveur SMTP sont bien identifiés dans les tables DNS.

• Les FQDN15 qui ne sont pas toujours implémentés : le chemin complet, normalement enregistré dans les DNS devrait être vérifié.

• Pas de création systématique d'un identifiant de message unique : le protocole SMTP n'oblige pas à identifier de façon unique un message envoyé par un client de messagerie. Bien entendu, et ainsi que le déclare le RFC 5321 lui-même, la simplicité du protocole fait sa force et il n'est pas conçu pour gérer les aspects de sécurité ou d'identification. Cela fait justement partie des points réfutés ici, et la relative complexité des mécanismes proposés n'alourdiront pas, outre mesure, cette simplicité de fonctionnement, ni de développement du protocole.

1.1.4.2 Le protocole POP

De même, au niveau du protocole POP3, plusieurs options ou fonctions ne sont pas adaptées ou sont inexistantes pour assurer une meilleure confiance :

• L'horodatage n'est pas fiable et est facile à modifier, simplement en modifiant l'heure de son ordinateur,

• La fonction garantissant l'intégrité du message transmis n'existe pas,

• De même, il n'y a pas d'obligation de sécurisation du lien,

• La gestion des identifiants de messages n'est pas effectuée au niveau du protocole,

• L'envoi des login et mot de passe sont fréquemment effectués en clair, permettant une possible écoute et capture de ceux-ci.

« *De futures extensions à POP3 sont en général déconseillées, car l'utilité de POP3 réside dans sa simplicité. POP3 est destiné à être un protocole de téléchargement et de suppression ; les capacités d'accès à la messagerie sont disponibles dans IMAP. Les extensions qui prennent en charge l'ajout de boîtes aux lettres supplémentaires, permettent le téléchargement de messages sur le serveur, ou qui dévient du modèle de téléchargement et suppression de POP sont fortement déconseillées et ont peu de chances d'être autorisées dans la perspective de la normalisation IETF*. »

(Extrait de la RFC 1939)

Pour les mêmes raisons évoquées déjà au sujet du protocole SMTP, il est indispensable que les protocoles de base contiennent des fonctions systématiques assurant un minimum d'identification et d'intégrité des données.

1.1.4.3 Le protocole IMAP

Le protocole IMAP permet une gestion distante des messages qui restent conservés sur le serveur (MDA) sans charger le lien entre le serveur et le poste de travail du client. Ce

protocole avait son intérêt lorsque les liens Internet étaient gérés par des modems à basse vitesse, évitant des temps de transfert de messages important. Par ailleurs, la conservation des messages par l'opérateur de messagerie permet d'alléger l'ordinateur local, et autorise une connexion à sa messagerie à partir de n'importe quel endroit.

IMAP contient de nombreuses possibilités de gestion des messages sur le serveur (le MDA), y compris au niveau des possibilités d'authentification (incluant Kerberos) et de sécurisation du lien.

D'autre part, ces sécurisations, tant du lien que de la confidentialité des mots de passe ne sont pas obligatoires et on peut retrouver des serveurs IMAP qui acceptent l'envoi de mots de passe en clair sur un lien non sécurisé. Cela peut être un inconvénient, aussi bien vis-à-vis de la localisation du contenu de sa boîte de messagerie que vis-à-vis de la confidentialité des données. En effet, l'évolution vers le « *cloud computing* » qui insiste sur la localisation répartie des applications et des contenus sur le web, ne permet pas de garantir un emplacement national de stockage, ni des moyens permettant de garantir la confidentialité des contenus ainsi répartis.

Il est donc important de conserver la possibilité de stocker localement, sur son poste de travail ou dans son réseau local le contenu de sa messagerie. C'est ainsi que fonctionnent d'ailleurs les messageries d'entreprises comme Microsoft Exchange ou Lotus Domino, et dont le mécanisme apporte des garanties sur la gestion des boîtes aux lettres des utilisateurs.

Enfin, les fonctions d'horodatage fiable et celles garantissant l'intégrité du message ne sont pas incluses dans ce protocole.

1.1.4.4 Le Webmail

Le fonctionnement du Webmail poursuit la même logique que le protocole IMAP en conservant systématiquement, et a priori sans limites de temps, l'ensemble des messages sur le serveur distant. La facilité d'accès qu'apporte le Webmail de se connecter à partir de n'importe quel endroit, que ce soit avec son propre ordinateur ou une machine en libre-service, ne doit pas faire oublier les contraintes et critères de sécurité, principalement au niveau de la sécurité du lien. En effet, dès lors que l'on se connecte d'un site extérieur (cybercafé, accès wifi gratuit…), on prend encore plus de risque sur l'écoute des informations qui transitent sur le lien Internet. Il est donc d'autant plus important que le lien d'accès au webmail soit sécurisé en SSL avant d'envoyer son login et mot de passe. Or ce fonctionnement n'est pas systématiquement proposé par les serveurs. Par ailleurs, les mêmes

inconvénients que pour le protocole IMAP, concernant la localisation et la confidentialité des données existent à l'identique, de même que l'absence d'horodatage fiable et de l'intégrité des données.

1.1.4.5 Sur TCP/IP

Le protocole de transport sur lequel s'appuient tous les protocoles de messagerie n'intègre pas de mécanisme de sécurité ni d'intégrité des paquets transportés. De même, aucun horodatage fiable n'est assuré à ce niveau. D'autre part, l'identification des émetteurs n'est pas assurée, à l'exception de leur adresse IP présentée qui peut être forgée, c'est-à-dire qu'un ordinateur peut utiliser une fausse adresse IP pour dissimuler l'origine des paquets émis, ce qui est fréquent dans le cas du « *spoofing* ». On ne peut donc pas compter sur cette couche de transport pour assurer les fonctions d'identification d'authentification, de sécurité ou d'intégrité, et il faut donc adapter les protocoles de messagerie directement.

1.2 Une nouvelle architecture de confiance « balkanisée »

Afin de pouvoir établir une nouvelle architecture de confiance, il faut établir la liste des fonctions et services nécessaires. La confiance est une chaîne qui doit être ininterrompue de l'émetteur au destinataire, et même au-delà dans la durée de conservation.

1.2.1 Comment identifier une source ?

La source d'un message correspond à l'ordinateur à partir duquel le message a été émis. L'identification de celui-ci est réalisée par la connaissance de son adresse IPqui, normalement, informe également sur sa localisation. Cette identification de la source d'un message est difficile à obtenir dans l'environnement actuel de l'utilisation des protocoles de l'Internet. En effet, les adresses IP des émetteurs de messages ne sont pas toujours «parlantes», car souvent noyées au sein d'un bloc d'adresses privé ne permettant pas l'identification d'un ordinateur précis, mais seulement le routeur d'entrée de l'entreprise. Ceci nous donne donc une information limitée, mais généralement réelle. Le cas d'utilisation d'un accès ouvert proposé par un hôtel ou restaurant par exemple, ne permet pas d'identifier la source d'un message, mais seulement le lieu à partir duquel le message a été envoyé, car l'ordinateur utilisé obtient une adresse IP spécifique dépendant du lieu de connexion. Plus difficile encore, le « *spoofing* » d'adresse IP est courant chez les spammeurs et dans les réseaux de zombies (botnets) utilisés pour diffuser massivement le « spam ». Dans ce cas, la donnée d'adresse IP émetteur n'a plus aucun sens et on ne peut ni identifier, ni localiser la

source du message. Prenant en considération l'ensemble de ces problèmes, le MAAWG (Messaging Anti Abuse Working Group), qui travaille sur les moyens de réduire le "spam" écrit : "*Trust in Email Begins with Authentication* (June 2008)" "*Les mécanismes d'authentification peuvent aider à distinguer le courrier électronique légitime du pourriel. Lorsqu'ils sont utilisés comme partie d'un programme anti-abus à multiples facettes, ils deviennent un outil efficace pour aider à protéger les marques commerciales de la contrefaçon et les attaques de hameçonnage », a déclaré Dave Crocker, conseiller principal de MAAWG. Les mécanismes d'authentification de courrier électronique sont utilisés pour valider l'identité d'un expéditeur de message, en étouffant ainsi les prétendus polluposteurs qui faussent souvent le champ 'De' du courrier électronique pour déjouer les mesures de détection.* "

Un protocole comme DKIM permet d'identifier de façon assez sécurisée le serveur de messagerie de l'émetteur et de garantir que ce serveur est bien celui qui est référencé dans le DNS du domaine correspondant. En conséquence, si un utilisateur essaye d'utiliser le serveur SMTP d'un autre domaine que le sien, celui-ci sera détecté et le destinataire en sera informé. Par ailleurs, l'identification de l'adresse IP de l'émetteur du message est transmise au serveur SMTP qui devrait vérifier si sa valeur est bien en relation avec le domaine auquel il appartient afin d'éviter le « *spoofing* » d'adresse IP. Cette vérification a ses limites, car l'adresse IP d'un utilisateur itinérant pourra varier fréquemment alors même que son message sera « valide ».

1.2.2 Comment authentifier l'émetteur ?

L'émetteur d'un message électronique est identifié par son adresse e-mail, et non par son identité civile, même si, dans le cas de certificats de signature électronique de type II ou III son identité civile est incluse et validée par une autorité de confiance. Au-delà de l'identification de la source, il convient donc d'authentifier l'émetteur du message, ce qui a beaucoup plus de valeur que l'identification de la source. Il est nécessaire de préciser, ici, la distinction faite entre l'identification d'un ordinateur par exemple, avec l'authentification de l'utilisateur qui se trouve derrière l'ordinateur et qui envoie le message. En effet, si, par l'adresse IP, même valide et vérifiée, on peut identifier l'ordinateur ayant émis un message, on ne peut garantir qui a utilisé cet ordinateur. Ceci est particulièrement vrai dans le cas d'utilisation des cybercafés ou de points d'accès publics. Par contre, si on peut authentifier l'utilisateur qui émet le message, quel que soit l'ordinateur qu'il utilisera pour envoyer son message, nous disposerons d'une information fiable. Cette authentification est d'autant plus importante qu'il est fait référence, dans les dispositions du Code civil à une identification

précise de la personne dont émane un document ou un message. Autrement dit, la meilleure façon d'authentifier l'émetteur d'un message est de banaliser et généraliser l'utilisation de la signature électronique simple (Classe I). Ce niveau de certificat ne permet que de valider l'adresse e-mail du demandeur et non pas son identité civile. Cette création de certificat et la gestion des clés correspondantes peuvent être simplifiées dans l'idée de ce simple objectif. Or, sans chercher à garantir que le logiciel de messagerie de « Monsieur Martin » n'a pas été utilisé à son insu, on peut, pour le moins, garantir que la signature électronique qu'il a utilisée est bien celle de son adresse email. Il peut s'agir aussi bien de certificats électroniques de type X509 comme ceux couramment utilisés chez les opérateurs de confiance français ou étrangers, que des certificats de type PGP dont la confiance n'est pas issue d'une structure de type PKI, mais par une confiance de proximité, de connaissance en connaissance. Les deux solutions techniques ont leurs avantages, et la solution de confiance à mettre en place doit accepter les deux types de certificats. L'aspect important dans ce cas est de garantir que l'adresse e-mail utilisée par l'émetteur d'un message existe, et que c'est bien à partir de celle-ci que le message a été envoyé.

1.2.3 Solutions de sécurisation

Les échanges entre l'émetteur et le serveur de messagerie, entre les serveurs de messagerie successifs, puis, enfin, avec le client de messagerie du destinataire doivent être sécurisés et cryptés afin de ne pouvoir intercepter le contenu des échanges (soit par écoute ou par attaque de type « man in the middle »), et de pouvoir garantir l'authenticité des serveurs utilisés. La sécurisation du lien entre le poste de travail et le MDA (Serveur POP ou IMAP ou Webmail) doit être systématiquement mise en place. Au-delà de l'établissement du lien TLS, il faut ajouter une vérification automatisée du certificat utilisé par le serveur afin de l'identifier de façon quasi certaine. L'accès à un serveur LDAP fournissant un annuaire garanti par une Autorité de Certification permet à l'émetteur de vérifier que son serveur de messagerie (MTA) est bien le sien et donc d'éviter un éventuel « *spoofing* » de celui-ci. Du côté du serveur (MTA), il lui faut également vérifier auprès du même serveur LDAP l'existence et la validité de l'e-mail de l'émetteur et de son certificat. Une fois la sécurité du lien établie, il convient de fiabiliser l'authentification de l'utilisateur qui se connecte pour accéder à sa boîte de messagerie en utilisant les extensions adaptées des protocoles (POP ou IMAP par exemple).

Les extensions APOP cryptant simplement le mot de passe lors de son envoi, ou POP-AUTH qui utilise une méthode de « *challenge-response* » pour s'assurer de la validité du mot

de passe sont trop limitées. L'utilisation du certificat de signature électronique de classe I permettra d'authentifier l'utilisateur lors de sa connexion au serveur POP et remplacera le mécanisme habituel de « *login-password* », lui garantissant ainsi qu'il sera le seul à pouvoir y accéder. Dans le cas d'un utilisateur itinérant, la copie de son certificat et de ses clés publiques et privées sur un support externe sera possible dès lors qu'il prendra les précautions nécessaires à la conservation sécurisée de ceux-ci. Enfin, il convient de sécuriser et de rendre confidentiel le stockage des messages sur les MDAs afin que, même les administrateurs de ces systèmes ne puissent avoir accès à ces données.

1.2.4 Garantir l'intégrité des messages dans un web balkanisé

Un message « intègre » est un message dont le contenu n'a pas été altéré. Compte tenu du fait qu'il est impossible de reconstituer un message d'origine qui aurait été altéré, on doit se contenter de la garantie de la vérification de l'intégrité du contenu. Celle-ci est réalisée grâce à un mécanisme de calcul d'empreinte (hash) appelé aussi condensé ou empreinte cryptographique permettant d'identifier de façon quasi-unique un document quelconque à l'aide d'une valeur de 160 bits pour la fonction SHA-1 par exemple. Or, nous avons vu que des paramètres sont ajoutés à chaque étape de la transmission du message par les différents serveurs SMTP qui se chargent du transfert du message. En effet, les en-têtes des messages sont modifiés à chaque passage par un « relais » de messagerie et ce jusqu'au destinataire final. Chacun de ces serveurs ajoute, au moins, les informations d'horodatage et d'adresse IP du serveur. Souvent d'autres informations sont ajoutées telles qu'une identification de type DKIM, une analyse du niveau de « spam »…

En conséquence, à chaque étape une vérification d'intégrité doit être réalisée, puis le serveur ajoute ses paramètres, et génère un nouvel élément permettant de garantir l'intégrité des données qu'il a ajoutées. Cela peut se faire soit en recalculant une empreinte (hash) globale du message avec ses en-têtes, soit en calculant plus simplement une empreinte complémentaire liée uniquement aux données ajoutées par le serveur. Dans tous les cas, l'utilisation du calcul d'empreinte est la seule manière fiable et standardisée d'assurer l'intégrité des données. A ce titre, et compte tenu des évolutions de la technologie, il faut utiliser, a minima, le mode SHA-1 ou SHA-256 pour se garantir, tant que possible, d'éventuelles « collisions » d'empreintes (deux fichiers différents donnant la même empreinte). Idéalement, l'empreinte est calculée à partir du certificat électronique du serveur SMTP permettant ainsi de garantir l'identité de celui-ci. Pour ce faire, même si l'utilisation de

la signature électronique simple côté émetteur est la meilleure solution, celle-ci n'est pas suffisante, car elle ne concerne que le contenu lui-même du message.

1.2.5 Solutions de traçabilité

Pour garantir l'origine d'un message, il faut être capable de retracer son chemin, et pour cela, le contenu des en-têtes des messages est essentiel. La solution de traçabilité des messages s'appuie tout d'abord sur l'intégrité de ceux-ci en utilisant les méthodes décrites dans le paragraphe précédent. Mais au-delà de cette technique, il convient également de garantir un horodatage fiable des messages qui transitent. En effet, il est facile de modifier la date et l'heure d'un serveur dont on a le contrôle afin d'enregistrer des données d'horodatage erronées (volontairement ou non) dans les en-têtes des messages. Cela implique d'une part l'utilisation de serveurs d'horodatage sécurisés TSS : *Time Stamping Serve*r intégrés ou non au serveur de messagerie SMTP, ainsi que la modification du format des dates enregistrées dans les en-têtes des messages pour se conformer aux standards et formats d'horodatage que sont d'une part le RFC3161 et la norme ISO 8601 et d'autre part, de pouvoir disposer d'une identification quasi certaine du serveur de transit ou d'envoi. A ce titre, l'utilisation de certificats électroniques sur les serveurs de type MTA faciliterait à la fois la mise en œuvre de l'intégrité et de la traçabilité des messages. Par ailleurs, il conviendrait pour ces mêmes serveurs de mettre en place une vérification automatisée des adresses IP présentées par un « reverse DNS » car l'absence d'un nom d'ordinateur associé à une adresse IP est un premier signe laissant penser à une utilisation détournée de la messagerie. Dans le cas où chaque serveur MTA utiliserait des certificats électroniques, la recherche dans l'annuaire LDAP de l'Autorité de Certification correspondant permettrait facilement d'assurer la validité du serveur.

1.2.6 Envisager l'archivage sur le long terme

La valeur des informations de transit des messages pour les serveurs d'une part, et celle des messages électroniques eux-mêmes d'autre part, induit un besoin réel de sauvegarde sécurisée de ces éléments. Plus encore, un archivage sur le long terme, lui-même sécurisé, de ces messages permettra de disposer de documents qui auront une valeur probante au regard des dispositions du Code civil. Cet archivage sera lui-même garanti par des certificats électroniques, horodatages et calculs d'empreintes. L'archivage des données de transit (logs) des serveurs sera également indispensable sur une durée qui sera fonction des contraintes de conservation juridique de ces traces qui sont spécifiques à chaque pays. Ces conditions de

conservation doivent également tenir compte des spécifications relatives aux données personnelles telles que le « droit à l'oubli » défini par la CNIL en France.

1.2.7 Solutions de confidentialité

La confidentialité réside dans l'impossibilité pour un tiers de lire le contenu d'un message ou d'un document. Un premier niveau doit être assuré lors du transit des messages. Des solutions au niveau global d'un serveur de messagerie de type MDA sont nécessaires afin qu'un tiers pouvant avoir accès à ce serveur ne puisse lire les données de l'utilisateur. Par ailleurs, vis-à-vis de messages spécifiques, un deuxième niveau de confidentialité peut être appliqué localement par l'utilisateur, soit à partir de son certificat de signature électronique, soit à partir d'une clé de codage symétrique. Ces différences de fonctionnement nécessitent une courte explication sur les fonctionnements des deux modes courant de chiffrement que sont le chiffrement symétrique et le chiffrement asymétrique. A l'image du protocole SSL utilisé par la plupart des serveurs Web pour sécuriser un lien, il est possible d'utiliser le chiffrement asymétrique pour échanger de façon sécurisée un mot de passe ou une clé de chiffrement symétrique qui pourra être utilisée en toute confiance. Dans le cadre de cette nouvelle architecture de confiance, il convient de disposer de certificats de signature électronique autorisant également le chiffrement. Une fois ceux-ci déployés, il devient possible d'assurer la confidentialité des données, soit en utilisant simplement le chiffrement asymétrique, soit en combinant cette dernière avec le chiffrement symétrique.

1.2.8 Solution de durée de vie d'un message

Dans le cadre de la confidentialité, ou même dans un cadre marketing, il est intéressant de donner une durée de vie limitée à un message. Pour ce faire, on utilisera plutôt un cryptage symétrique en faisant héberger la clé de décryptage sur un site distant tel qu'un annuaire LDAP pendant une durée limitée. Ceci aura pour effet de ne pouvoir décrypter ledit message que pendant une période précise. Ensuite, la clé sera effacée et le message ne pourra plus être décodé. Bien entendu, cela n'empêche pas l'utilisateur ayant décodé le message pendant sa durée de vie, de le copier déchiffré, puis de le stocker sous cette dernière forme. Néanmoins, dans ce cas, les attributs de traçabilité et d'intégrité pourraient ne pas être conservés.

1.2.9 Sécurisation des données stockées

Les messages électroniques sont stockés sur les MDAs dans l'attente de la connexion de l'utilisateur avec son client de messagerie. De plus en plus fréquemment, les utilisateurs

conservent leurs messages sur ces serveurs, en particulier dans le cas de l'utilisation du «Webmail». Or, dans la plupart des cas, n'importe quel ingénieur système disposant d'un accès privilégié aux ordinateurs hébergeant les MDAs peut obtenir le contenu d'un message stocké sur celui-ci. Ce point est d'autant plus critique, que ces serveurs sont hébergés dans des pays dans lesquels la protection des données personnelles ne s'applique pas. Aussi, convient-il de sécuriser les messages électroniques stockés sur ces serveurs afin que personne ne puisse accéder à leur contenu en-dehors de l'utilisateur lui-même. Ceci implique, a priori, un chiffrement des données sur ces serveurs. Afin d'en assurer la confidentialité pour l'utilisateur final, la solution préconisée sera d'utiliser la clé publique de l'utilisateur sous réserve de son existence. Dans ce cas, l'utilisateur utilisera sa clé privée pour accéder à ses données déportées et confidentielles.

1.2.10 Conséquences sur les protocoles

Historiquement des tentatives d'amélioration du logiciel « sendmail », le plus couramment utilisé sur l'Internet comme serveur SMTP, ont eu lieu avec le développement de la version « sendmail X » qui devait prendre en compte plusieurs aspects de sécurisation et d'identification des émetteurs. Ce projet a été arrêté en 2007 et remplacé par le projet « MeTA1 »20 mais en se focalisant sur la fiabilité et l'efficacité du protocole, plutôt que sur les aspects liés à l'authentification des émetteurs. Or, pour assurer la mise en œuvre des recommandations précédentes sur l'identification de la source, l'authentification de l'émetteur, la sécurisation des transferts, l'intégrité et la traçabilité des messages ainsi que la confidentialité, il convient tout d'abord d'adapter le protocole SMTP pour lui permettre d'assurer, au niveau du protocole lui-même, ces différentes fonctions. Une nouvelle version du protocole, que j'appellerai pour l'instant CEMTP pour CErtified Mail Transfer Protocol, pourrait ainsi devenir le « standard de fait » des MTAs afin d'élever sensiblement le niveau de confiance dans la messagerie. De même, il convient d'adapter les contraintes liées aux MDAs (serveurs POP / IMAP) afin de garantir ces éléments d'intégrité, d'authentification, de traçabilité et de confidentialité de bout en bout et d'imposer l'utilisation de certaines extensions déjà existantes. Plus précisément, certaines fonctionnalités du protocole POP3 devraient être obligatoires et non optionnelles telles que l'authentification avec un certificat, ou pour le moins une séquence « *challenge-response* » de type POP-AUTH, et d'autres devraient être ajoutées comme la sécurisation du lien avec le serveur SMTP et surtout la confidentialité des données sur le serveur. Enfin, pour gérer du point de vue de l'utilisateur l'ensemble de ces contraintes et de ces protocoles, tout en gardant une rétro-compatibilité, il

est indispensable de développer un « client » de messagerie (MUA) permettant une gestion simple et transparente de tous ces critères : « certitrustmail » par exemple.

Celui-ci aura pour objectifs :

- l'accès simplifié à la demande et à l'utilisation de certificats de signature électronique de Classe I (e-mail) permettant le cryptage des données,
- L'authentification de l'utilisateur pour ses connexions à l'aide de ce certificat,
- La gestion de la confidentialité des données localement et à distance,
- L'établissement d'un lien sécurisé avec le serveur CEMTP,
- La connexion automatisée aux serveurs LDAP gérant les clés publiques et la vérification systématique des certificats,
- La séparation des fonctions de gestion des messages électroniques,
- La mise en œuvre des mécanismes d'intégrité des messages, même en dehors de l'utilisation des serveurs CEMTP,
- La gestion d'un horodatage fiable permettant d'assurer une bonne traçabilité.

1.3 Propositions de modifications des protocoles

1.3.1 Qu'est-ce qu'une RFC ?

Les RFC (*Request For Comment*) représentent la manière de normaliser les protocoles de l'Internet. Le fonctionnement des RFC est le suivant :

« Les RFC sont rédigées sur l'initiative d'experts techniques, puis sont revues par la communauté Internet dans son ensemble. Cela diffère d'une publication d'institution telle que l'ANSI. La majorité des RFC utilisent les termes MUST, MUST NOT, SHOULD, MAY, etc. tels que définis dans la RFC 2119 pour définir leurs exigences (obligation, interdiction, recommandation, etc.). Pour plus d'informations à propos des RFC et les procédures associées, voyez la RFC 2026 « Procédures Standards d'Internet. Révision 3 ». Les RFC font d'abord l'objet d'un draft (brouillon). Tout le monde peut écrire un draft. Ils n'ont donc aucune valeur. Après avoir écrit un draft, on peut le soumettre à l'IETF en le transmettant à rfc.editor@rfc.editor.org. Tous les drafts n'étant pas dignes d'intérêt, ils ont une date de péremption. Si le draft attire l'intérêt de la communauté, un groupe de travail peut être créé pour la rédaction d'une RFC. La RFC 2223 donne les instructions pour les futurs auteurs. Quelques RFC finissent par devenir des standards d'Internet. La procédure complète pour la transcription d'une RFC en standard est la suivante : RFC → Proposed Standard → Draft

Standard → Internet Standard. Malgré leur nom, les RFC sont le plus souvent stables. Toute modification apportée à une RFC entraîne l'écriture d'une nouvelle RFC, qui rend la précédente obsolète. »

Source : Wikipedia : simplification traduite des informations du site de l'IETF.

1.3.2 Quelles normes existent ?

Les RFC, c'est-à-dire l'IETF21 bien entendu, mais aussi l'ISO (X509 ; PDF/A…), l'ETSI, … sont les organismes qui rédigent des normes sur le fonctionnement de l'Internet. Néanmoins, compte tenu du nombre important de ces standards et normes, nous nous limiterons aux plus significatifs, en particulier les protocoles de messagerie principaux qui sont les suivants :

- SMTP : RFC 5321 (anciennement 2821)
- POP3 : RFC 1939
- IMAP4 : RFC 3401
- Structure des messages : RFC 2822
- En-têtes des messages : RFC 5322

1.3.3 Demander la modification d'un RFC

Une demande de publication d'une RFC commence par la rédaction de celui-ci selon les formats définis dans la RFC 2223 qui la structure. Il convient alors d'envoyer sur le site de l'IETF, une première version qui sera un « draft » revu par des membres de l'IETF, comportant, le cas échéant, plusieurs échanges pendant 6 mois. A l'issue de ce processus, et s'il est positif, un numéro de « RFC » est attribué. Le document est alors publié à l'ensemble des membres des listes de diffusion correspondant au domaine d'application, dans notre cas, la messagerie électronique, et qui comportent la plupart des spécialistes mondiaux du domaine. Le document devra être revu à la lumière des retours et critiques de ces membres. Enfin, si les retours sont positifs et si les organes de gestion de l'IETF considèrent que le document le justifie, il devient un RFC définitif.

1.3.4 Propositions pour le protocole CEMTP

Un certain nombre de points et de fonctionnalités doivent être ajoutés et/ou modifiés dans le protocole SMTP pour le transformer en protocole original CEMTP. Pour ce faire, les critères à retenir sont les suivants :

- Sécurisation des échanges
- Identification de la source
- Authentification de l'émetteur
- Intégrité des messages de bout en bout
- Traçabilité
- Confidentialité des données
- Archivage des logs (traces) de façon sécurisée

En premier lieu, l'établissement de liens sécurisés lors des échanges, que ce soit entre l'utilisateur et le serveur (MUA et MTA) ou entre deux serveurs (MTAs), DOIT être systématique. Ensuite, il convient d'assurer l'identification du serveur de messagerie de l'émetteur, pour les relais ou les réceptions de messages. A ce titre le protocole existant DKIM est parfaitement adapté et devrait être utilisé.

Détail du RFC 4871 expliquant DKIM :

DomainKeys Identified Mail (DKIM) defines a mechanism by which email messages can be cryptographically signed, permitting a signing domain to claim responsibility for the introduction of a message into the mail stream. Message recipients can verify the signature by querying the signer's domain directly to retrieve the appropriate public key, and thereby confirm that the message was attested to by a party in possession of the private key for the signing domain.

The approach taken by DKIM differs from previous approaches to message signing (e.g., Secure/Multipurpose Internet Mail Extensions (S/MIME) [RFC1847], OpenPGP [RFC2440]) in that:

o the message signature is written as a message header field so that neither human recipients nor existing MUA (Mail User Agent) software is confused by signature-related content appearing in the message body;

o there is no dependency on public and private key pairs being issued by well-known, trusted certificate authorities;

o there is no dependency on the deployment of any new Internet protocols or services for public key distribution or revocation;

o signature verification failure does not force rejection of the message;

o no attempt is made to include encryption as part of the mechanism;

o message archiving is not a design goal.

DKIM:

o is compatible with the existing email infrastructure and

```
transparent to the fullest extent possible;
     o requires minimal new infrastructure;
     o can be implemented independently of clients in order to
reduce deployment time;
     o can be deployed incrementally;
     o allows delegation of signing to third parties.
```

Cependant, pour qu'il soit le plus efficace possible, il conviendrait que chaque serveur CEMTP ou SMTP dispose d'un certificat électronique l'identifiant, et que celui-ci soit associé à la bonne entrée DNS correspondante. Ensuite, il convient d'authentifier l'émetteur du message lui-même. Autrement dit, qualifier de façon quasi certaine la partie gauche de l'adresse e-mail. Pour ce faire, l'émission et l'utilisation d'un certificat électronique de classe I, c'est-à-dire prouvant l'existence de l'adresse électronique de l'émetteur, DOIT être fortement recommandée, voire imposée.

De plus, il faut systématiquement utiliser, a minima, la fonction STMP-AUTH pour pouvoir utiliser le serveur SMTP de son domaine. En même temps, il convient d'éviter l'utilisation possible d'un serveur SMTP extérieur à son propre domaine.

Néanmoins, l'authentification par le certificat électronique de l'utilisateur sera préférable, voire obligatoire s'il dispose dudit certificat. De même, la possibilité d'envoi de message sans spécifier d'adresse e-mail d'émetteur DOIT être interdite, contrairement au protocole SMTP classique. Dans le protocole SMTP, l'obligation d'accepter des messages ne comportant pas d'adresse e-mail d'émetteur était liée aux difficultés rencontrées avec les retours de messages d'erreurs des envois de messages. Ces messages renvoyés par les serveurs, pour éviter des allers-retours récurrents (*bouncing*), ne comportent pas d'adresse email d'émission. Cette simplicité et faiblesse ont été largement utilisées par les spammeurs pour diffuser de façon importante des messages sans risquer d'être perturbés par des retours d'erreur ou des messages de rejet des utilisateurs. Les problématiques liées au « *bouncing* » de messages de traitement des erreurs DOIVENT être gérées à l'aide d'emails de types génériques associés au certificat électronique de chacun des serveurs de messagerie. L'intégrité du message lui-même doit être traitée à l'aide d'empreintes (hash MD5, SHA-1 ou SHA-256) à chaque étape de la transmission du message par chaque serveur CEMTP, au niveau même du protocole. Dans le cas de l'utilisation par l'émetteur d'un certificat de signature électronique, la fonction de calcul d'empreinte est intégrée au niveau de l'envoi du

message. Aussi, le serveur CEMTP n'a-t-il besoin que de vérifier ladite empreinte à chaque étape pour en garantir l'intégrité. Néanmoins, il convient d'ajouter une empreinte complémentaire dans un champ spécifique des en-têtes qui représentera le calcul fait sur l'ensemble des données ajoutées : Horodatage, adresse IP du serveur et son nom DNS, sa clé DKIM et l'adresse IP du serveur suivant. Le serveur suivant agira de même et son calcul d'empreinte intégrera également la valeur de l'empreinte du serveur précédent. Dans le cas où l'émetteur n'utilise pas de certificat de signature électronique, le serveur d'envoi CEMTP (le MSA), intégré dans le client de messagerie, DOIT calculer l'empreinte du message avant sa transmission au serveur CEMTP.

En réception, le client de messagerie du destinataire vérifie automatiquement la validité de l'empreinte reçue et peut ainsi garantir que le message n'a pas été altéré lors de son transfert ou de sa réception. Idéalement, l'empreinte du message, intégrant, bien entendu, l'adresse email de l'émetteur et la date d'envoi (si possible certifiée par un horodatage fiable), devrait être utilisée comme identifiant unique du message (Message-ID=UID), facilitant ainsi, aussi bien la transmission de l'empreinte que l'identification du message par les MDAs (serveurs POP ou IMAP). Ces derniers éléments assureront ainsi la traçabilité du message.

Concernant les aspects liés à la confidentialité des données, la sécurisation du lien entre chaque relais de messagerie permet de s'affranchir des problèmes de confidentialité des données lors de la transmission du message. Les autres points liés à la confidentialité des données sont gérés par les MDAs et les MUAs. Enfin, la conservation et l'archivage des logs (traces) doivent être réalisés de façon sécurisée, en signant chacun d'entre eux avant archivage, de préférence au jour le jour.

Les conditions de conservation des logs seront dépendantes des réglementations de chaque pays et des contraintes liées à la gestion des données personnelles. En France, il convient de vérifier, le moment venu, avec la CNIL si ces traces et leur conservation doivent ou non entrer dans le cadre du « droit à l'oubli » spécifié par ses services.

1.3.5 Propositions pour le protocole POP et IMAP

Le MDA (*Message Delivery Agent*) qui est utilisé pour stocker les messages dans l'attente de leur téléchargement ou consultation par l'utilisateur via son MUA (Message User Agent), doit respecter les mêmes contraintes et critères que ceux décrits dans le protocole CEMTP, savoir :

- Sécurisation des échanges
- Authentification de l'émetteur
- Intégrité des messages de bout en bout
- Traçabilité
- Confidentialité des données
- Archivage des logs (traces) de façon sécurisée

Ces évolutions du protocole permettront d'obtenir une nouvelle version CEPOP, à l'image de CEMTP, pour améliorer la confiance. La sécurisation des échanges avec le MUA (poste client) doit respecter les contraintes de l'établissement d'un lien TLS. Dans le cas des MDAs, l'identification de la source n'a pas lieu d'être et se trouve intégrée dans l'authentification réciproque entre le MDA et la MUA à l'aide des certificats de signature électronique. Cette même authentification de l'utilisateur remplacera le couple « *login-password* » pour permettre à celui-ci d'accéder à ses données. L'intégrité des messages ayant été suivie par les MTAs CEMTP, le MDAs n'aura qu'à vérifier le calcul d'empreinte pour valider cette intégrité. La traçabilité sera traitée de la même manière que pour les MTAs, en ajoutant dans les en-têtes un horodatage fiable et une empreinte qui validera le moment où l'utilisateur aura téléchargé ou consulté son message. Cette fonction permettra également d'ajouter facilement une réelle opération d'accusé de réception ayant une valeur probante tant que les systèmes d'horodatage en jeu et les certificats des serveurs auront toute leur validité, sans avoir besoin de mettre en place une infrastructure lourde. La confidentialité des données stockées sur le MDA est un ajout important mais essentiel afin d'éviter une consultation possible des messages par un tiers. La méthode proposée et recommandée s'appuie une fois encore sur le certificat de signature électronique simple de l'utilisateur. En effet, il devient simple pour le MDA recevant le message d'accéder au serveur LDAP de l'Autorité de Certification afin d'obtenir la clé publique de l'utilisateur propriétaire de la boîte aux lettres. A partir de cette clé, le MDA peut aisément crypter le message à destination unique du propriétaire de la clé privée associée. En conséquence, seul le destinataire pourra accéder à sa boîte de messagerie et décoder ses messages pour les télécharger. Si l'on considère que ce mécanisme est trop lourd en termes de ressources pour le MDA, il est possible de conjuguer les bénéfices du cryptage symétrique avec le cryptage asymétrique, en cryptant une clé symétrique avec la clé publique de l'utilisateur afin qu'il puisse en disposer, puis de crypter les données sur le MDA. Le choix de la clé symétrique peut être initié à la demande de l'utilisateur qui cryptera celle-ci avec la clé publique du MDA. Un identifiant unique permet

de différencier facilement les messages. Selon les conventions, il est recommandé que celui-ci soit composé du nom de domaine de l'émetteur et d'une valeur dérivée de la date. Néanmoins, même si cette utilisation reste possible, je recommande de modifier la structure de l'UID (et de la fonction UIDL) en utilisant l'empreinte du message (le hash SHA-1, ou même un simple MD5), accompagné, le cas échéant d'un numéro séquentiel qui pourrait faciliter la tâche du protocole CEPOP lors de la réception des messages afin que le MUA puisse facilement vérifier la présence d'un message déjà téléchargé et d'en vérifier les séquences. Comme pour le protocole CEMTP, le MDA se doit d'organiser un archivage sécurisé de ses logs (traces) incluant l'horodatage des connexions et téléchargement des messages par le MUA. Bien entendu, cet archivage sera signé par le MDA afin d'apporter un niveau de preuve suffisant. Les contraintes de conservation liées aux données personnelles sont les mêmes que pour le protocole CEMTP déjà détaillées.

1.4 La réalité de la menace

Les révélations faites par E. Snowden ouvrent de nouvelles pistes de réflexion quant au rôle pouvant être joué par la France vis-à-vis de ses partenaires, notamment africains. Ainsi, la fragmentation voulue et programmée du web peut servir à des fins protectives, comme nous allons l'expliquer dans les paragraphes qui suivent. La figure 1 illustre une collection de cartes de visites d'officiels obtenues lors de colloques.

Fig. 11 – Échantillons de cartes de visites de fonctionnaires internationaux

L'ensemble de ces cartes présente une caractéristique commune : les adresses email des fonctionnaires concernés sont gérées par Yahoo, Google (Gmail) ou d'autres opérateurs privés accessibles directement par la NSA. Dans plusieurs cas il s'agit de très hauts fonctionnaires (par exemple des Ministres d'Etat) dont les communications électroniques se trouvent ainsi directement exposées. Dans la plupart des cas, les pays concernés n'ont pas la capacité numérique suffisante de déployer des solutions alternatives à Yahoo et à Gmail. Dans d'autres cas il s'agit d'emails créés dans un but de facilité.

1.4.1.1 Un déploiement simple

Balkaniser le web permettra d'offrir à ces nombreux pays une solution échappant à la surveillance directe de la NSA à ces nombreux pays.

La solution que la France pourrait promouvoir et sponsoriser, consistera à créer en territoire neutre (par exemple, les locaux des Nations Unies), un serveur similaire en tous points à ceux gérés par un fournisseur de services de messagerie tels que Google ou Yahoo (les données seraient soit préservées au sein des locaux neutres ou sauvegardées de manière chiffrée, signée et résilientes à l'extérieur des locaux neutres), la procédure d'ouverture de compte sera similaire à celle de Gmail ou de Yahoo. Par contre les installations, les codes source gérant la messagerie, les conditions de stockage et les procédures de ce service de messagerie seraient évaluables par des Etats, des associations et par des individus souhaitant le faire. Ainsi, la création d'un espace « balkanisé » de messagerie pourrait permettre d'échapper à la surveillance de la NSA et réduire la dépendance des Etats.

2 Les pistes de réflexion politiques, économiques et stratégiques

Les pistes de réflexion techniques ne peuvent se penser indépendamment d'une politique industrielle et de gouvernance de l'Internet. Elles ne peuvent en effet aboutir qu'à condition que l'Europe puisse structurer une industrie performante basée sur la confiance entre Etats-membres partenaires, dans un dialogue efficace entre les secteurs publics et privés. Sur le plan diplomatique et politique, cela suppose d'établir des liens de coopération et de confiance, qui vont à l'encontre des tentations de repli souverain mais qui s'avèrent indispensable pour peser face aux géants non-européens de l'industrie high-tech et aux plate-formes dominantes du web, à l'égard desquels les pays européens conservent une très forte dépendance. Malgré des limites que constituent les fortes disparités de moyens, les rivalités politiques et les crispations nationales, l'Europe dispose d'un réel pouvoir normatif et règlementaire sur lequel elle peut s'appuyer pour peser dans les débats sur la gouvernance du cyberespace, et y défendre ses valeurs et ses intérets.

2.1 Politique économique et industrielle : vers une offre de confiance ?

Compte tenu des importants enjeux économiques et politiques liés à la dépendance à des industries extra européennes, il est devenu urgent de structurer une Base Industrielle Européenne du Numérique (BIEN). Sur toute la chaine de valeur du numérique, sur les marchés des moteurs de recherche (Google) jusqu'à celui de la détection des intrusions

(SourceFire), peu d'entreprises européennes offrent la même qualité de service que leurs homologues américaines à un prix compétitif leur permettant de s'imposer sur les marchés internes mais aussi étrangers.

Reproduire l'ensemble de la chaine d'approvisionnement à l'échelle nationale est impossible compte tenu de la taille limitée du marché. En revanche, l'UE présente un marché bien plus important et peut également contribuer politiquement aux développements de la BIEN par des investissements de la Commission via le programme Horizon 2020. Le développement de la BIEN doit aller au-delà du seul segment de la cybersécurité. Les services numériques et les composants COST devraient être au centre d'une réflexion globale du citoyen/consommateur à l'industrie.

> La mise en œuvre d'une politique industrielle globale constitue une urgence dans le débat touchant les questions numériques. Il s'agit de structurer un écosystème cohérent d'entrepreneurs (grands groupes et PME), de laboratoires de recherche (universitaires et privés) et d'investisseurs capable d'assurer une innovation continue et un socle technologique répondant aux enjeux sécuritaires et économiques.

Deux dimensions devraient particulièrement sous-entendre la *BIEN* :

- La compétitivité : une offre pour être valable doit pouvoir se vendre à un prix compétitif et à un large portfolio de clients.
- La confiance : le but est de développer des solutions maitrisées par des fournisseurs sur le territoire européen qui peuvent garantir l'absence de moyens de contournement.

Depuis 2008, les instances européennes ont affiché leur volonté de faire de la politique industrielle une priorité de l'Europe de demain. Des documents significatifs ont marqué cette volonté :

- La Communication 2008 «Plan d'action pour une consommation et une production durables et pour une politique industrielle durable »[181] met en évidence la nécessité d'une politique commune en matière industrielle ;

- La Stratégie EU de cybersécurité, février 2013, définit comme priorité le développement d'une industrie européenne de cybersécurité[182] ;

[181] Plan d'action pour une consommation et une production durables et pour une politique industrielle durable
[182] Stratégie Européenne de cybersécurité

- La Communication 24 juillet 2013 « Vers un secteur de la défense et de la sécurité plus compétitif et plus efficace en EU »[183] souligne la nécessité du partage des ressources en matière de sécurité

- La contribution de la Commission au débat sur l'Economie Numérique d'octobre 2013[184] montre que le marché européen des télécommunications souffre de la résistance des frontières nationales et empêche le développement de l'économie numérique.

Cependant la politique industrielle de l'UE développée depuis quelques années a été limitée par un double effet : d'un côté, les législations très contraignantes en matière d'utilisation des données et de l'autre, des considérations très diverses des Etats-membres sur le rôle de l'Etat en matière de régulation des marchés. L'affaire Snowden a participé à l'accélération du processus de prise de conscience de la vulnérabilité des Etats européens. Mais les réactions sont pour l'instant principalement développées dans un cadre national alors même que tous, Etats comme industries, soulignent l'enjeu de la dimension des marchés. A ce stade, la volonté politique de l'Europe semble manquer. Il s'agit désormais pour l'Europe de penser aussi à la notion d'industrie européenne en parallèle de la défense du consommateur.

Voici une liste non exhaustive des propositions en matière de politique industrielle qui nous semblent cohérentes dans le contexte que l'on vient de décrire :

2.1.1 Structuration du dialogue public-privé sur les questions de politique industrielle

La constitution d'une plateforme européenne d'échange public-privé constitue un préalable à toute autre proposition. Les représentants du secteur numérique, des OIV, des grands groupes de la sécurité et des fournisseurs de systèmes industriels mais aussi des PME et des centres de recherches ont besoin de se fédérer et d'échanger ensemble mais aussi avec les pouvoirs publics européens.

L'objectif principal d'une telle initiative sera d'identifier quelles solutions pourraient être développées au niveau européen.

Depuis juin 2013 la plateforme *Network and Information Security* (NIS)[185] offre déjà un cadre d'échange, mais la thématique industrielle n'est abordée qu'indirectement via le groupe de travail « recherche et innovation ». L'élargissement du mandat de ce forum

[183] Vers un secteur de la défense et de la sécurité plus compétitif et plus efficace en EU
[184] La contribution de la Commission au débat sur l'Economie Numérique
[185] https://resilience.enisa.europa.eu/nis-platform

permettrait de faire rencontrer offre et demande et ainsi combler le manque existant. En s'inspirant de l'expérience française, on pourrait penser à l'institution d'un CoFIS du numérique européen. C'est-à-dire un comité regroupant les représentants les pouvoirs publics à niveau européen, des experts nationaux, des membres de la recherche et de l'industrie. L'ENISA qui aujourd'hui vise à recentrer son approche sur les bénéficies économiques[186] de ses activités, pourrait ainsi être la chaine de transmission vis-à-vis des instances communautaires.

Dans une première phase, les travaux préliminaires à développer seront :

- D'élaborer une cartographie des forces et faiblesses du tissu industriel européen dans le secteur numérique, y compris la cybersécurité (offre) ;
- Et de définir le champ d'action de ce qui rentre dans le domaine de souveraineté nationale et ce qui peut être partagé au niveau européen (demande);

Le comité pourrait ensuite se pencher sur la création de cercles de confiance et l'élaboration d'une feuille de route concrète avec des recommandations. Compte tenu de la territorialisation des compétences existantes, il s'agirait de lancer un dialogue sur une base volontaire entre Etats et industries et de concevoir des périmètres plus larges offrant un écosystème attractif pour l'industrie européenne. Ce dialogue pourrait commencer à partir de quelques pays ou par une approche sectorielle (aérospatial ou finance).

Dans ce sens, France et Allemagne ont déjà exprimé leurs souhaits d'une coopération plus étroite. Cependant, l'initiative ne doit pas être cantonnée aux seuls Etats. Les centres de recherche et nombreuses entreprises travaillent déjà en réseaux et pourraient ainsi se porter leaders de cette initiative. En effet, nombreux OIV, des grands groupes industriels ont des sites multidomestiques et partagent ainsi les mêmes intérêts à la coopération: se défendre sur plusieurs sites et vendre les solutions sur plusieurs pays.

Dans le cadre d'une coopération franco-allemande, on peut citer deux exemples pratiques de cercle de confiance. L'industrie du logiciel française a déjà manifesté sa volonté

[186] Source : http://www.lemagit.fr/actualites/2240224106/LEnisa-se-penche-sur-les-benefices-economiques-de-la-cybersecurite

de coopérer aves ses collègues allemands[187]. L'autre exemple est celui de l'industrie aéronautique composée par des grands groupes et d'une chaine d'approvisionnement présente dans les deux pays.

Ces mêmes cercles de confiance au sein de la plateforme public-privé pourraient constituer des groupes de travail sectoriel visant l'échange d'informations anonymes sur les bonnes pratiques mais aussi la menace.

2.1.2 La qualification d'industrie de confiance

La création d'un label européen de confiance pourrait être un levier pour la constitution d'un marché interne. Dans les secteurs considérés comme critiques, comme la cybersécurité des OIV, les marchés pourraient être réservés à des « entreprises de confiance », dont les critères de certification seraient définis par la plateforme public-privé (point 1). Cette initiative peut démarrer sur la base de travaux au sein d'un petit groupe d'Etats (les plus avancés) voire débuter sur un dialogue bilatéral par exemple avec l'Allemagne pour ensuite s'élargir à tous les Etats de l'UE. Le principe est le suivant : une certification est dispensée à une entreprise par les autorités nationales respectives des Etats mais répondra à des critères communs ou au moins à des accords de réciprocité. Par exemple, l'ANSSI donne la certification à une société française qui répond également aux critères définis par son homologue allemand. L'entreprise sera ainsi certifiée dans les deux pays.

Une certification européenne obligatoire pour certaines solutions permettrait ainsi de développer une offre de confiance renforçant l'efficacité de la sécurité européenne.

2.1.3 Paquet Soutien aux PME

Les PME sont le moteur de l'innovation dans le numérique : elles sont un élément indispensable pour répondre à l'évolution extrêmement rapide des usages, des technologies et des avancées scientifiques. Aujourd'hui, malgré un tissu dynamique de pépites technologiques, leur taux de survie et leurs rythmes de croissance ne sont pas au niveau pour atteindre la taille critique suffisante pour s'ouvrir aux marchés étrangers. Après une première phase de croissance, de nombreuses PME éprouvent des difficultés à pérenniser leurs investissements : elles sont ainsi rachetées trop tôt par des grands groupes, souvent étrangers,

[187] Livre blanc rédigé de l'Association Française des Éditeurs de Logiciels et Solutions Internet *Cyber-sécurité : Hisser les acteurs français au niveau de la compétition mondiale*, juin 2014.

ou arrêtent d'investir. Dans tous les cas, elles cessent d'être innovantes au détriment d'un écosystème compétitif.

Afin de remédier à cela, l'UE pourrait :

- Etablir des marchés publics communs (par exemple les firewall SCADA) et les réserver aux PME sur le modèle du *Small Business Act* américain. Ces marchés permettraient aux PME de consolider leur stratégie et se développer.
- Intensifier et mieux cibler le financement de la R&D dans le cadre du H2020. Le programme Horizon 2020 consacre 1.7Md€ à la sécurité ; le principale problème est de faire de l'innovation une solution commerciale. La plateforme public-privé, dans ce cadre peut jouer un rôle important en aidant l'Europe à cibler la recherche sur des thématiques importantes pour le monde industriel et accompagner les PME dans la commercialisation de leurs produits et services.

Les années 2013 et 2014 ont été très importantes pour le paysage numérique européen : lancement d'une stratégie en matière de cybersécurité, proposition de la directive sur la sécurité de l'information et des réseaux, débats sur la protection des données personnelles, etc.

Contraindre les industries européennes à se protéger ou imposer aux acteurs tiers de respecter les droits des citoyens européens, sont sûrement des initiatives fondamentales. Cependant, tant qu'il n'existera pas d'offre européenne robuste, cela ne garantira pas une autonomie d'action, une croissance économique et une protection des valeurs européennes. Dans le contexte actuel de crise et de forte compétition, le soutien à une industrie européenne du numérique est une opportunité économique, stratégique et politique pour bâtir l'Europe de demain.

2.2 Puissance normative et règlementaire de l'Europe

La question des normes est centrale dans l'Union Européenne, comme le rappelle le politologue Zaki Laïdi, auquel nous empruntons la notion de « puissance normative »[188].

[188] Laïdi, Z. (2005), La norme sans la force – L'énigme de la puissance européenne, Presses de la Fondation Nationale des Sciences Politiques, Paris, 159p.

Remarquons d'emblée que « puissance » et « normes » sont a priori des notions contraires. La norme en réfère à la règle partagée, à laquelle chacun se soumet quel que soit son rang, quand la puissance en appel à la force, qui se joue des règles et des contraintes. Pourtant, Zaki Laïdi définit ce qu'est la puissance normative européenne, puissance, dont l'identité et la stratégie se fondent sur une préférence pour la généralisation de règles comportementales applicables aux Etats. Selon lui, les normes présentent trois caractéristiques essentielles qui conditionnent la conception internationale promue par l'Union Européenne : elles sont négociées et non imposées ; elles sont légitimées par des instances internationales ; elles sont opposables par tous les acteurs, indépendamment de leur rang et de leur position hiérarchique dans le système international.

En ce sens, l'Europe est devenue un modèle au niveau mondial en termes d'intégration économique et politique (Union Européenne), de gouvernance et de gestion partagée par la norme (Union Européenne, Conseil de l'Europe). Ce modèle rayonne aujourd'hui en particulier en Asie où des dynamiques d'intégration régionale sont en cours. Pionnière au niveau de l'intégration et des normes, l'Europe peut donc jouer un rôle important dans ce domaine sur l'Internet. De fait, plusieurs textes européens sont cités en référence dans de nombreux pays comme des modèles à suivre (Convention de Budapest, Data Protection Regulation). Or, ce pouvoir normatif et règlementaire dont dispose l'Europe, peut se traduire par une puissance d'influence qui joue en sa faveur.

2.2.1 Protection des données personnelles et *Big data*

L'actualité en matière de protection des données personnelles en Europe illustre le caractère brulant des débats en Europe. Et à l'heure où l'Europe tente difficilement de mettre en place une législation en matière de protection des données personnelles face aux lobbies des géants du web, il convient de revenir la conception même de la vie privée afin d'en faire un atout économique pour l'EU mais aussi l'outil d'influence et de promotion des valeurs européennes.

Comme évoquées dans la deuxième partie de cette étude, la puissance des géants de l'Internet et l'extra-territorialité de la législation américaine peuvent mettre en danger notre conception de la vie privée et des libertés civiles. Pour répondre à ces deux préoccupations, le régime juridique européen devra bien sûr limiter fortement les abus (surveillance) mais sans pour autant limiter la collecte de données qui constitue un enjeu économique majeur.

Une conception trop restrictive de la protection des données empêche à ce jour le développement des savoirs faire et des outils qui permettront à l'UE et ses Etats-membres d'être compétitifs à l'avenir. Il faut permettre aux entreprises européennes de collecter, traiter, croiser les données afin de développer les outils et la compétitivité pour générer de la valeur et assurer le traitement des données sensibles par des entreprises européennes.

Il s'agit en effet de protéger les libertés civiles en développant un cadre règlementaire qui soit suffisamment solide et équilibré pour :

- Etre reproduit par d'autres pays particulièrement intéressés par le modèle d'intégration politique et économique de l'UE et ainsi d'exercer un pouvoir d'influence. C'est notamment le cas en Asie où les coopérations régionales existantes cherchent davantage d'intégration notamment économique (ASEAN) et où l'Europe est perçue comme un partenaire économique de choix mais également comme un acteur de poids dans la diplomatie internationale, face à la forte influence des Etats-Unis.
- Etre attractif pour que les entreprises souhaitent héberger leurs données sous le régime juridique européen. L'attraction des flux de données permettra de générer de la valeur. Ainsi le régime de protection des données peut servir de levier économique et politique pour inciter les géants du Net à adopter dans leurs CGU (conditions générales d'utilisation) les normes mais aussi les valeurs européennes comme la conception de la protection de la vie privée européenne, des droits des citoyens
- Et constituer un levier pour contrecarrer l'extra-territorialité des Etats-Unis

Il s'agit pour l'Europe de penser également les outils de gouvernances, notamment en matière de règlement des litiges dans la gestion des espaces de co-souveraineté, à l'image des travaux engagés par le projet Internet et Juridiction[189].

2.2.2 Convention de Budapest sur la cybercriminalité

Adoptée par le Conseil des ministres du Conseil de l'Europe le 8 novembre 2001, elle vise, selon le rapport explicatif du Parlement européen à « *1) à harmoniser les éléments des infractions ayant trait au droit pénal matériel national et les dispositions connexes en matière de cybercriminalité, 2) à fournir au droit pénal procédural national les pouvoirs nécessaires à l'instruction et à la poursuite d'infractions de ce type ainsi que d'autres infractions*

[189] http://www.internetjurisdiction.net/about/

commises au moyen d'un système informatique ou dans le cadre desquelles des preuves existent sous forme électronique, et 3) à mettre en place un régime rapide et efficace de coopération internationale. ». De manière inédite, cette convention permettait ainsi au niveau européen d'adopter une terminologie et un diagnostic commun sur les questions relatives à cybercriminalités et de fournir les cadres juridiques nécessaires pour mettre en place des coopérations interétatiques en termes de lutte et de prévention dans ce domaine.

Or, si elle a été pensée à l'échelle européenne, cette convention a aujourd'hui des conséquences plus larges. De fait, 44 pays l'ont aujourd'hui ratifiée, dont certains ne font pas partie du Conseil de l'Europe, à l'instar des Etats-Unis, du Japon, ou de l'Australie. D'autres pays sont en cours de ratification comme le Canada et l'Afrique du Sud. Mais son impact est plus large encore, puisque plus de 120 pays au total ont collaboré avec le Conseil de l'Europe pour renforcer et harmoniser leur législation sur la cybercriminalité. L'Europe a donc ici joué un rôle d'initiateur et de promoteur pour la coopération internationale, coopération essentielle dans le cadre de la lutte contre la fraude et la criminalité. En ce sens, elle promeut une conception de la sécurité internationale sur le Net fondée sur la coopération et l'échange, sûrement plus attractive, que le modèle de « police mondiale » mis en avant par les Etats-Unis, avec les abus inévitables d'un tel monopole, comme l'ont montrés les révélations d'Edward Snowden.

Ainsi, la conférence « Octopus » les 21, 22 et 23 novembre 2011, à l'occasion des dix ans d'existence de la convention, réunissait de nombreux acteurs gouvernementaux (appartenant aux différents pays membres et pays observateurs comme le Canada ou le Japon), mais aussi internationaux (ONU, UE, mais aussi des agences de renseignements intergouvernementales comme Europol ou Interpol) et des entreprises privées (Microsoft, Symantec, Visa, etc.). L'Europe peut donc se targuer d'avoir réussi par cette convention à suggérer des normes acceptables pour parties très divergentes et à poser les cadres d'un débat plus large entre des instances nationales et internationales, publiques et privées. Et la diffusion actuelle de ce modèle normatif montre sa pertinence. De fait, une convention sur le modèle de celle de Budapest est à l'étude au niveau des Nations Unies, bien que les obstacles à cette échelle restent très nombreux.

Aussi, lors de la dernière décennie, avons-nous ainsi vu se formaliser une forme de doctrine européenne de la sécurité, basée sur la coopération entre pays membres et l'échange d'informations, tant au niveau de la sécurité informatique que dans celui plus général de la sécurité territoriale d'une part, et sur le respect de la vie privée et des droits individuels

d'autre part, qui attire aujourd'hui de nombreux Etats et organisations de par le monde. Bien que perfectible, l'expérimentation de cette coopération en termes de sécurité est visible à travers diverses agences comme Europol ou Frontex, dont le fonctionnement se révèle plus transparent et plus concerté que celui des agences de sécurité américaines. A ce niveau, l'Europe (UE, Conseil de l'Europe) pourrait jouer un rôle de premier plan pour promouvoir cette conception de la « sécurité partagée », déjà en partie à l'œuvre au sein de l'Union européenne.

La convention de Budapest représente donc un pas affirmé dans cette direction. Elle demeure néanmoins une convention qui, treize ans après sa mise en place, reste imparfaite et pourrait être améliorée pour pousser à plus de coopération entre les divers acteurs. Ainsi, même si de l'avis de tous, elle reste le meilleur dispositif international à l'heure actuelle dans la lutte contre la cybercriminalité, il convient de la développer et de la parfaire, au vu des nouvelles menaces et de s'en servir comme levier pour rayonner et mettre en place des outils de coopération policière et judiciaire au niveau opérationnel qui permette de défragmenter le cyberespace dans la lutte contre la cybercriminalité.

2.3 L'Europe, acteur de la gouvernance de l'Internet

La richesse et la diversité des débats qui s'ouvrent à l'échelle mondiale autour de la gouvernance du cyberespace témoignent d'un moment particulier dans l'histoire. Alors que l'Internet amorce le virage des 3 milliards d'utilisateurs, les défis se multiplient de façon conjuguée : montée en puissance des pays émergents dont le rattrapage en taux de pénétration promet d'être fulgurant grâce à l'Internet mobile, scandale de la surveillance, multiplication des cyberattaques de plus en plus ciblées et sophistiquées, cyberespionnage qui atteint des proportions industrielles, développement de cybercapacités offensives, conflits de juridictions à propos des activités transfrontières dans le cyberespace, volonté affirmée des Etats de reprendre la main et défendre leur souveraineté dans le cyberespace, remise en cause de la suprématie américaine et revendications des Etats non occidentaux de peser dans la gouvernance et le futur de l'Internet. Le moment est historique car toutes ces questions sont à l'agenda des négociations internationales, même si les enceintes appropriées et le —ou les— bon cadre du débat restent à déterminer. Il existe dès lors une réelle fenêtre d'opportunité pour l'Europe de peser dans les discussions qui permettront 1) de redéfinir la gouvernance de l'Internet au niveau mondial et 2) d'établir les nouveaux cadres de la sécurité collective à

l'âge des réseaux interconnectés. C'est le moment pour l'Europe de peser dans ces débats, à condition de se donner les moyens de le faire.

Ces deux débats, comme nous l'avons démontré, recèlent des enjeux économiques et de souveraineté majeurs pour les nations européennes. Face à la suprématie des Etats-Unis et à la taille critique des puissances émergentes, les pays d'Europe peuvent difficilement peser individuellement. L'Europe, on le sait, est traversée de divisions politiques, d'intérêts concurrents et de disparités colossales qui constituent un frein à la coopération, particulièrement dans les domaines perçus comme régaliens. Mais les Etats-membres partagent néanmoins des valeurs, des intérêts économiques, politiques et sécuritaires ainsi qu'une expérience de la gouvernance qui devraient motiver l'élaboration d'une vision commune afin de peser dans ces débats plutôt que les subir.

Au-delà de la définition de stratégies nationales, il semble nécessaire d'articuler une position commune sur la gouvernance autour des valeurs de l'Europe pour assurer l'avenir de l'Internet et de la sécurité collective, dans le respect de la souveraineté des Etats membres et des valeurs qui les unissent.

2.3.1 Peser dans les débats sur la gouvernance de l'Internet

Le sommet NetMundial et la réforme de la fonction IANA sont deux événements exceptionnels qui se sont tenus au cours de l'année 2014 et représentent une réelle ouverture pour réformer la gouvernance de l'Internet. Tous deux ont été précipités par les révélations d'Edward Snowden mais résultent d'évolutions qui semblaient inéluctables.

Sous le leadership de Fadi Chehade depuis 2012, l'ICANN avait d'ores et déjà entrepris son ouverture vers l'Asie et les pays émergents avec la promesse de rendre l'organisation plus globale et plus inclusive, avec notamment la création d'un nouveau hub à Singapour puis à Istanbul. La décision de l'intention de transférer « à la communauté globale multi-acteurs » la supervision des fonctions IANA, jusque là confiée à la direction nationale de l'information et des télécommunications du Département du Commerce (NTIA), a été annoncée quelques semaines avant le sommet du NetMundial, en signe d'ouverture aux perspectives de réforme et de globalisation de la gouvernance, ce qui a aussi permis de désamorcer certaines tensions liées au scandale de la surveillance et déplacer le débat. Cette annonce répond à des revendications anciennes des Etats, notamment européens, régulièrement pris entre deux feux dans les débats sur la gouvernance. La France, parmi

d'autres, s'est régulièrement insurgée de la supervision par les Etats-Unis du fichier racine de l'Internet et des fonctions d'adressage, tout en ne pouvant cautionner l'alternative proposée par la Chine ou la Russie, qui reviendrait à confier ces fonctions à l'IUT ou autre organisation multilatérale dans laquelle les démocraties occidentales se retrouveraient minoritaires et qui pourrait conduire à la fin du modèle multi-parties prenantes.

Cette transition s'avère ainsi un moment historique et offre une opportunité rare de réformer la structure et le fonctionnement d'ensemble de l'ICANN, entreprise de droit américain construite autour des valeurs, cultures et pratiques anglo-saxonnes. Qui doit superviser les fonctions de l'ICANN et comment ? A qui l'ICANN doit-elle rendre des comptes ? Quels sont les recours possibles à ses décisions ? Qui doit être représenté au board des directeurs ? Comment assurer une organisation plus globale et inclusive (langues, représentation, pratiques, normes juridiques, redistribution des ressources) ? C'est l'objet de la discussion parallèle sur la « redevabilité » (accountability) de l'organisation.

Face à ces questions, la position des Etats-Unis est claire et réitérée à travers les multiples forums de discussion, par une représentation très large d'experts. L'ICANN a accompagné la croissante exponentielle du réseau sans problème technique majeur, le modèle fonctionne malgré ses défauts, il faut certes le réformer mais avec prudence, sans prendre le risque d'une trop grande mainmise des Etats qui ne partageraient pas la même vision d'un Internet libre, global et ouvert.

Les pays européens, en revanche, avancent souvent en ordre dispersé. La France s'est particulièrement illustrée en faisant, dans un premier temps, cavalier seul sur la question du « .vin », « .wine », avec l'appui cependant de la Commissaire européenne Neelie Kroes. D'une part, les entreprises françaises ont peu candidaté à l'obtention de ces nouvelles extensions lorsque l'ICANN a lancé le programme de nouveaux gTLDs (Generic Top Level Domain Names), ce qui rend les choses plus difficiles à rattraper aujourd'hui, alors que près de 2000 demandes ont été déposées. D'autre part, ce qui inquiète plus fortement les autorités et l'industrie viticole, la société américaine Donuts, qui a obtenu la gestion de ces extensions, pourrait vendre des noms de domaines qui correspondent à des appellations d'origine contrôlée, comme « bordeaux.vin », qu'elles ne représentent pas. Dans une lettre datée du 12 septembre 2013, la Commissaire européenne chargée de la société numérique Neelie Kroes a demandé à l'ICANN de ne pas attribuer les .vin et .wine tant que les règles permettant de protéger les indications géographiques. La demande est restée sans effet puisque les noms de

domaine ont été attribués. Mais des négociations directes semblent en cours pour résoudre ce problème.

La focalisation de la France sur ce sujet est problématique à plus d'un titre. Alors que l'ensemble des nations lors du NetMundial et du high-level meeting du 50ème sommet de l'ICANN à Londres célébraient la perspective d'une transition sur l'IANA et affirmaient leur engagement à travailler à travailler à la réforme des institutions pour défendre une vision partagée de l'Internet au nom de l'intérêt général, la France s'engageait dans un bras de fer au nom de la défense de ses intérêts particuliers. Certains arguments avancés par la Secrétaire d'Etat chargée du numérique Axelle Lemaire n'auraient pas été reniés par la Chine ou la Russie, notamment la nécessité de renforcer le pouvoir des Etats et la possibilité de défendre leurs intérêts au sein de l'ICANN. Ce mélange des genres poussé jusqu'à l'ultimatum a conduit la France à menacer de quitter la table des négociations à un moment crucial, alors même que se discute l'avenir de la gouvernance.

Il ne fait aucun doute que la bataille du .vin, .wine puisse relever des intérêts de la France, bien défendus par le lobby de l'industrie viticole, et qu'il soit nécessaire d'établir un rapport de force avec l'organisation pour se faire entendre. Quelle que soit l'efficacité de cette tactique, lier ce rapport de force à la question bien plus globale et importante de la réforme de l'ICANN pose problème. La France a adopté une posture très critique mais sans proposer d'alternative, à part la satisfaction de ses revendications comme condition de sa participation au plus vaste chantier de réforme. Quels sont les mécanismes que la France souhaite mettre en place pour que ce type de situation ne se reproduise pas ? Quels recours auprès de l'ICANN ? Il ne faut pas perdre de vue que tout ce que l'on revendique pour soi doit pouvoir s'appliquer aux autres et les risques de dérive dans les revendications étatiques ne manquent pas. L'intérêt est peut-être justement de séparer les enjeux et de les traiter dans les forums appropriés, en s'appuyant sur des jeux d'alliances, notamment au niveau européen.

En l'occurrence, la question relève d'un différend de politique de libre-échange sur lequel, depuis des décennies, les gouvernements ne parviennent à se mettre d'accord au sein de l'Organisation Mondiale du Commerce semblerait un forum plus adapté. Pour l'Europe (et particulièrement la France) et les Etats-Unis (et leurs proches), la crainte était justement qu'un accord au sein de l'ICANN ne crée un précédent pour les négociations OMC, ce qui explique que la bataille ait été aussi violente. La possibilité de s'appuyer sur l'OMC pour mettre la question en suspens auprès de l'ICANN est une piste. L'ICANN n'a pas vocation à se substituer aux autres instances multilatérales pour trancher des contentieux internationaux. Il

aurait été sans doute été possible, au sein de l'ICANN, par une discussion entre les acteurs eux-mêmes, de trouver une solution pragmatique qui ne créé de précédent ni dans un sens, ni dans l'autre. Proposer d'inclure dans la réforme de l'ICANN la possibilité de faire appel des décisions qui touchent à des contentieux non résolus est une autre piste. Les rapports de force, enfin, peuvent s'établir dans le cadre de discussions bilatérales à un autre niveau, au nom des intérêts partagés entre pays de culture similaire, ce que les Américains appellent *like-minded countries*.

La préservation d'un modèle multi-parties prenante est une motivation forte pour faire avancer les discussions, afin de rendre les représentants américains plus sensibles aux intérêts de leurs partenaires. Car l'autre alternative est le renforcement du pouvoir des Etats au sein de l'ICANN, ce qui peut remettre en question la prédominance que les Etats-Unis souhaitent conserver dans la gouvernance de l'Internet et/ou conduire à des conflits d'intérêts qui entraîneraient des dysfonctionnements susceptibles de perturber le fonctionnement ou fragmenter le système. La séparation des questions de gouvernance au sein de forums adaptés, couplée avec le système multi-parties prenantes a des avantages. En fonction des forums et des enjeux, ce ne sont pas nécessairement les mêmes configurations d'acteurs ni les mêmes rapports de force qui s'installent. Cela ouvre la possibilité de nouer des alliances avec un acteur (gouvernement, business) sur un sujet, même si l'on se trouve en rivalité avec ce même acteur sur un autre sujet. Cela permet aussi de tirer partie des intérêts concurrents qui existent au sein de chaque Etat, et de s'appuyer par exemple sur les conjonctions d'intérêts économiques entre entreprises du même secteur pour faire levier politique.

Peser dans la gouvernance de l'Internet implique ainsi d'être actifs dans les débats et de jouer à la fois de la coopération et du rapport de force. De ce point de vue, une coalition d'Etats européens a plus de chances de peser dans les débats, à tous les niveaux, qu'un Etat isolé. La réflexion menée par la France à l'égard de la réforme de l'ICANN bénéficierait d'une concertation avec ses partenaires européens.

Pour aller plus loin, il serait évidemment souhaitable qu'une concertation européenne débouche sur une vision claire et une force de proposition pour le futur du réseau. Dans le cadre de la défense de ses valeurs, l'Europe pourrait être à l'initiative de la promotion des libertés civiles, à l'image des efforts entrepris par la Freedom Online Coalition. Enfin, le financement, national et européen, de projets de recherche collaboratifs pluridisciplinaires au niveau européen pour le développement d'une réflexion stratégique, d'une vision et d'un développement de l'Internet du futur permettrait d'œuvrer en ce sens. Cette réflexion est tout

aussi indispensable au positionnement de l'Europe à l'égard des normes de comportement des Etats dans le cyberespace, dont les enjeux sont liés.

2.3.2 Peser dans les débats sur les normes de comportement des Etats

La question des normes de comportement responsable des Etats et de l'application du droit international dans le cyberespace est très discutée au sein du centre d'excellence de l'OTAN et au sein du groupe gouvernemental des experts de l'ONU (UNGGE). Le Manuel de Tallinn, bien que largement critiqué, fait néanmoins office de document de référence en l'absence d'autre alternative sérieuse. Là encore, la position européenne peine à émerger et la culture du secret limite les interactions intra-gouvernementales et avec le milieu académique dans bien des pays, dont la France.

Par exemple, l'ANSSI met aujourd'hui en avant dans les réunions internationales de haut niveau, une position qui tient pour responsable d'une cyberattaque l'Etat dans lequel se trouve le dernier proxy d'où elle est provient. L'idée est de contraindre l'Etat en question à coopérer pour stopper l'attaque s'il en a les moyens, ou le cas échéant en ouvrant l'accès à ses réseaux pour une intervention extérieure. Si l'on comprend la logique opérationnelle qui l'a guidée, on peut toutefois s'interroger sur les implications géopolitiques et juridiques d'une telle prise de position, qui mériterait d'être confrontée à la recherche académique. Les Etats les moins dotés et les moins sécurisés pourraient se trouver pris entre deux feux, d'une part le risque d'être utilisés massivement comme proxy dans des attaques, d'autre part celui de devoir abandonner leur souveraineté sur leurs réseaux à des Etats tiers. On peut aussi s'interroger sur les conséquences diplomatiques et juridiques d'une attaque non traçable opérée par un Etat ou un acteur non-étatique (A), via un Etat (B) contre un autre Etat (C) avec lequel les relations sont particulièrement tendues. L'application de ce principe pourrait alors conduire à une forte montée des tensions entre les Etats B et C, voire des représailles s'il n'existe pas de processus de collaboration entre eux. Cette position n'est par ailleurs pas exempte de risque pour la France, qui pourrait involontairement véhiculer une attaque via ses réseaux et en être tenue responsable. Plutôt que prendre une position isolée, la France pourrait par ailleurs chercher à rallier plusieurs pays européens pour défendre une idée des normes et régulations compatibles avec ses valeurs et intérêts. Pour l'heure, les Etats-Unis dominent assez largement le débat.

Les enjeux sont importants car à la logique de coopération et défragmentation du cyberespace pour lutter contre la cybercriminalité évoquée plus haut, s'oppose une logique de

compétition et de maximisation de la puissance des nations par le développement de cybercapacités y compris offensives. Or la question du cyberespionnage, comme nous l'avons vu, complique la discussion. Accroître la coopération pour améliorer la cybersécurité pour l'ensemble de l'Europe implique de limiter certaines activités entre partenaires de confiance. Cette étape est difficile à franchir pour les Etats. En particulier, les Etats-Unis se défendent d'utiliser les informations recueillies par biais du renseignement pour en tirer avantage économique et cherchent aujourd'hui à convaincre leurs partenaires de leur bonne foi, mais pour l'heure pas au point de renoncer à des activités de renseignement très poussées.

Le contexte actuel est celui d'une montée en puissance des moyens et des discours, avec des déclarations fortes sur les représailles possibles à des cyberattaques, laissant entrevoir un fort potentiel d'escalade des conflits. Ces discours s'inscrivent aussi dans un contexte d'intense rivalité entre les Etats-Unis et la Chine, dont la dernière étape en date est la mise en examen de cinq officiers chinois de l'armée populaire, qui ont conduit à la suspension du dialogue bilatéral entre les Etats-Unis et la Chine sur le cyber. Le discours politique et médiatique américain établit un lien discursif entre les cyberattaques relevant de l'espionnage économique (à but de profit), les menaces sur les infrastructures critiques et les risques pour la sécurité nationale. La focalisation sur l'espionnage économique a ainsi compromis —pour un moment au moins— les négociations sur les normes de comportement responsables des Etats et autres règles du jeu dans le cyberespace entre les deux pays.

Cette situation ouvre une opportunité pour l'Europe de se positionner en interlocuteur dans un débat très clivé entre les Etats-Unis et la Chine, d'autant que l'Europe est perçue par les Etats-Unis mais aussi par la Chine et plus généralement les pays émergents comme un partenaire crédible. Or impliquer la Chine et la Russie dans l'élaboration de nouvelles règles de sécurité collective augmenterait —évidemment sans la garantir— leur inclination à les respecter.

L'Europe pourrait ainsi avoir une position à défendre en accord avec ses intérêts et ses valeurs, afin de limiter la rhétorique guerrière en plein essor pour privilégier la coopération internationale et la sécurité. Force de proposition, elle pourrait être le levier qui pousse à restreindre les comportements agressifs dans le cyberespace et impliquer les Etats émergents dans la discussion pour construire les nouvelles bases de la sécurité collective. A minima, elle pourrait faire entendre une autre voix…

Conclusion générale

Au terme de cette étude, il apparaît clairement que le terme de « balkanisation » n'est pas un concept opératoire mais bien une représentation géopolitique qui sert des intérêts divers selon qui l'emploie, dans quel contexte et à propos de quel débat.

Comme nous l'avons précisé en introduction, il couvre sous le même vocable des débats aussi divers que le filtrage, la segmentation et la fragmentation potentielle résultant des politiques de sécurité nationale ; le maintien de l'interopérabilité du réseau et d'un fichier racine commun ; les conflits autour des enchevêtrements de juridictions et de l'application extensive de la loi américaine dans le cyberespace via le principe d'extra-territorialité ; le contrôle national des contenus et des usages dans le cyberespace, notamment par des régimes non-démocratiques; le modèle de gouvernance multi-acteurs par opposition à la montée en puissance d'un modèle intergouvernemental ; les pressions commerciales qui cloisonnent les contenus numériques via les algorithmes sélectifs, les systèmes d'exploitation mobiles ou les *app stores* exclusifs.

Largement répandu dans les médias, le vocable est également très populaire auprès des leaders de la communauté Internet qui l'utilisent comme une arme dans les débats, notamment lorsqu'il s'agit de faire évoluer les règles de gouvernance de l'Internet ou de lutter contre l'expression de la souveraineté des Etats dans le cyberespace (technique, politique ou juridique). Or ces évolutions récentes entraînent —et sont causées par— une remise en question de la suprématie des Etats-Unis dans le cyberespace. Elles défient aussi une vision idéaliste inspirée par les pionniers de l'Internet, d'un espace indépendant, transfrontière, autogéré, libre de toutes contraintes et régulations. Il n'est donc pas surprenant des les retrouver fréquemment dans le discours des experts, officiels et représentants américains, comme dans celui des organisations de défense des libertés individuelles et numériques.

La connotation très péjorative du terme de « balkanisation », la diversité des débats qu'il recouvre et l'ambiguité qu'il installe quant à ses implications invitent à l'utiliser avec la plus grande circonspection, particulièrement dans le cadre des négociations internationales. Il est préférable d'être clair et précis dans les termes que l'on emploie pour désigner les dynamiques multiples et parfois contradictoires de fragmentation/ouverture qui s'opèrent à différents niveaux sur la couche physique, logique et sémantique du cyberespace. Cela ne veut pas dire qu'il faille ignorer les dangers d'un processus de cloisonnement qui pourrait

affecter certaines dimensions du réseau, mais ce processus n'est pas global, uniforme, ni nécessairement irrémédiable tant il est soumis à de constantes pressions politiques, sociales et commerciales. Il est aussi, par certains aspects, (souveraineté juridique, contrôle des contenus, pratiques linguistiques et culturelles) déjà une réalité, comme nous l'avons démontré. Le terme de « balkanisation » n'aide pas la discussion, il la complique et la politise.

Séparer les enjeux en utilisant des termes précis permet aussi de traiter les problèmes dans des cadres appropriés, avec les acteurs concernés, qui ne sont pas nécessairement les mêmes selon qu'on aborde les conflits de juridiction et les enjeux de l'extra-territorialité dans le cyberespace, la protection du secret des affaires ou encore l'interopérabilité. L'intérêt d'une dynamique de fermeture ou de cloisonnement peut s'avérer légitime et/ou productive pour certains enjeux et certains acteurs, contreproductive et/ou illégitime pour d'autres. Or la configuration des rapports de force et des logiques de coopération/compétition entre acteurs n'est pas la même en fonction des enjeux. Définir une stratégie pour la France ou l'Europe nécessite de comprendre finement ces dynamiques, leurs différents enjeux, en les distinguant au mieux même s'ils sont liés, pour s'appuyer sur les bonnes coopérations et établir les bons rapports de force afin de défendre leurs objectifs.

Des dynamiques multiples et parfois contradictoires

Les dynamiques que nous avons identifiées, et les risques qui y sont associés, sont de plusieurs ordres. Contrairement à certaines représentations qui circulent, il n'existe pas un mais des cyberespaces. Notre étude montre clairement que si les réseaux qui constituent l'Internet sont connectés et interopérables au niveau mondial, si l'interaction des utilisateurs est globale et si les pratiques sociales tendent à s'uniformiser, le cyberespace est néanmoins constitué de sous ensembles linguistiques, politiques et culturels qui engendrent une grande diversité des expériences du web selon l'endroit d'où l'on se connecte sur la planète. L'idée d'un cyberespace libre, ouvert, où l'information circule sans restriction et où tout est accessible à tous à partir de n'importe où relève largement du mythe.

Deuxième point important, la suprématie américaine reste extrêmement importante dans le cyberespace à tous les niveaux, aussi bien du point de vue de l'infrastructure physique, de la couche logique ou des contenus. Elle est tout aussi prégnante dans le domaine politique de la gouvernance, de la gestion technique de l'architecture et du fonctionnement du réseau, des activités militaires et de renseignement ou encore du domaine juridique, étendu par le principe d'extraterritorialité. L'affaire Snowden a considérablement accéléré les tendances de fond de remise en question de cette suprématie, alors que le centre de gravité de

l'Internet se déplace vers l'Asie et le Sud. Les pays émergents où le nombre d'utilisateurs est en croissance exponentielle font face à de multiples défis et entendent désormais peser dans la gouvernance du cyberespace.

Plus globalement, les révélations sur la surveillance massive opérée via les réseaux, par les Etats-Unis mais aussi par d'autres pays qui désormais ne s'en cachent plus, entraîne une prise de conscience politique et une montée en puissance des revendications de souveraineté numérique. Cela se traduit par des initiatives aussi bien politiques, qu'industrielles ou juridiques permettant de préserver l'intégrité et la confidentialité des données des appétits de gouvernements étrangers. Les enjeux de défense et de sécurité nationale engendrent par ailleurs une logique de repli souverain susceptible d'entrer en contradiction avec les logiques de coopération internationale nécessaires à la lutte contre la cybercriminalité.

Enfin, la marchandisation des services en ligne entraîne aussi des dynamiques de fragmentation sur les couches supérieures du cyberespace, comme la remise en cause de la neutralité du Net ou encore le développement de systèmes d'exploitation mobile et *app stores* exclusifs. Mais elle entraîne aussi une dynamique opposée sur les couches inférieures car tous les acteurs économiques cherchent à développer leurs activités à l'échelle globale et ont dès lors un intérêt clair à maintenir l'ouverture et l'interopérabilité de l'Internet.

Il n'y a donc pas de logique unique de fragmentation et encore moins de « balkanisation », ni de la part d'un Etat particulier, ni comme tendance générale même si par ailleurs, des initiatives peuvent fragmenter certaines dimensions de l'Internet avec des conséquences dommageables (contenus limités, accès restreint, etc.). On observe des intérêts concurrents entre les différents acteurs (étatiques, privés, citoyens, techniques) au sein de chaque Etat. L'étude de cas de la Russie est à ce titre éclairante. Elle montre à la fois la volonté politique de défendre la conception d'un Internet souverain, le « RuNet » (développement stratégique de l'infrastructure physique, services adaptés à la langue et la culture, investissement de la couche sémantique) et la volonté de bénéficier des opportunités économiques (protectionnisme économique, politique d'innovation, maintien de l'interopérabilité). Une grande diversité d'acteurs sont impliqués dans la gestion et le développement de l'Internet et, en raison des intérêts concurrents qui peuvent exister entre eux au sein même d'un Etat, cela permet de nouer des alliances pour lutter contre certaines dynamiques de fragmentation ou tout au moins en limiter l'impact.

Les enjeux pour l'Europe

Les enjeux pour l'Europe sont importants dans tous les aspects de sa souveraineté, aussi bien politique, économique, juridique qu'en termes de défense et sécurité. Les enjeux politiques et économiques sont particulièrement liés à la question de l'espionnage et de la maîtrise des données. La dépendance des pays européens, et plus particulièrement la France, aux équipements étrangers (principalement chinois et américains) et aux plates-formes étrangères — géants du web américains en particulier— est très forte ; l'exposition à la surveillance est donc très importante et les retombées économiques de la captation des flux de données leur échappe en grande partie. Les pays européens sont donc particulièrement exposés au risque de vol de propriété intellectuelle et de secret des affaires. L'absence de maîtrise des données met en jeu les bases de la croissance économique future (les données sont considérées comme l'or noir du 21ème siècle), la protection des données personnelles et plus généralement, la défense des valeurs de l'Europe.

La réforme de la législation relative à la protection des données à caractère personnelle est de ce point de vue un test intéressant de la capacité de l'Europe à élaborer un cadre cohérent et efficace pour préserver ses intérêts économiques et défendre ses valeurs. La mise en œuvre par Google de la décision de la Cour de Justice Européenne sur le « droit à l'oubli » montre toute la complexité et l'intrication des enjeux politiques, juridiques, économiques voire éthiques.

Les politiques de *data localization* et autres propositions de « *cloud* souverain » permettent certes de faire émerger l'offre alternative qui bénéficie aux entreprises européenne et réduit quelque peu la dépendance à l'offre américaine, bien que l'inversion des rapports de force à moyen terme soit peu probable. Elle permet aussi de faire pression sur les entreprises américaines —et par leur biais sur le système politique et judiciaire comme en témoigne le bras de fer entre Microsoft et le Département de la Justice— pour tenir compte des revendications de confidentialité de leurs clients européens. Mais ces initiatives montrent des limites : elles ne peuvent être viables si elles se limitent au marché national doivent donc s'inscrire dans un projet de développement européen et international pour être compétitives ; elle ne résolvent pas la problématique de l'extra-territorialité et la question de l'accès aux données reste entière.

Les enjeux de sécurité et de souveraineté entraînent de la part des nations européennes une volonté de sanctuarisation du territoire, une forme de repli souverain qui comporte aussi des risques et des effets paradoxaux. Cette sanctuarisation peut s'avérer difficilement réalisable d'un point de vue opérationnel et juridique, d'autant que les infrastructures vitales

sont largement détenues et opérées par le secteur privé ; elle pose problème pour la coopération internationale nécessaire à la lutte contre la cybercriminalité ou le partage d'informations pour la cybersécurité ; elle recèle des risques d'escalade des conflits liés à une maladresse ou une erreur de calcul entre acteurs étatiques, en l'absence de processus de coopération et de règles du jeu clairement définies.

Cette logique contribue à la difficulté de faire émerger des solutions au sein de l'Union européenne, malgré les enjeux. La limite de souveraineté est difficile à dépasser d'autant que la disparité des moyens entre les Etats est très forte et que les logiques bilatérales, notamment avec les Etats-Unis, prévalent. Ces difficultés nuisent au développement de la coopération industrielle, économique et de défense au sein de l'Union européenne et incitent les Etats les moins avancés à se tourner vers les Etats-Unis et l'OTAN.

Pistes de réflexion stratégique pour l'Europe

Notre étude ouvre sur quelques pistes de réflexion stratégique. Nos conclusions n'ont nulle prétention à être exhaustives. Elles émanent des enseignements tirés de nos observations générales et des études de cas que nous avons menées. D'une manière générale, des initiatives conduisant à une certaine fragmentation —voire un repli souverain — peuvent avoir du sens et s'avérer nécessaires dans certains domaines spécifiques qui touchent aux intérêts les plus sensibles d'un Etat, ses infrastructures ou ses informations les plus stratégiques (entreprises privées, secteur public). Mais la sécurité a un coût : en termes financiers ; en termes de créativité et d'innovation car elle bride la prise de risque ; en termes de performance car les initiatives nationales peuvent faire émerger des difficultés techniques et juridiques pour les entreprises et entraver leur fonctionnement ou décourager les personnels de les respecter. Des mesures trop restrictives au plan national peuvent aussi limiter la capacité à collecter, analyser, exploiter de grandes masses de données, ou encore collaborer efficacement pour lutter contre la cybercriminalité ou réduire les risques d'escalade des conflits. Il est donc essentiel de penser ces enjeux dans une logique de gestion du risque et d'envisager la sécurité dans l'esprit d'ouverture qui a fait le succès du réseau et fera la croissance économique de demain.

D'un point de vue technique, l'enjeu est de parvenir à utiliser de façon sécurisée une infrastructure par définition non sécurisée, ce qui comprend une part de fragmentation pour le stockage des données sans remettre en question la logique d'ouverture. La proposition

consiste à construire une architecture de confiance pour créer un espace de messagerie sécurisé. Raisonner en termes de confiance implique d'en penser toute la chaîne qui doit être ininterrompue de l'émetteur au destinataire, et de penser dans le temps pour la conservation des données. L'utilisation sécurisée est permise par l'établissement de liens systématiquement sécurisés —entre chaque relais de messagerie—, et une double identification du serveur de messagerie de l'émetteur -avec si possible certificat électronique - et de l'émetteur lui-même. Au-delà de la vérification de l'authenticité, il est nécessaire de garantir et donc d'être en mesure de vérifier l'intégrité des messages, d'assurer leur confidentialité et leur traçabilité. Enfin, il est nécessaire de penser l'archivage de façon sécurisée, à la fois par une réflexion sur la durée de vie des messages et sécurisation des données stockées.

D'un point de vue économique, il est indispensable de développer une politique industrielle de confiance à l'échelle européenne. Le développement de l'offre en cybersécurité ne peut suffire, la structure de la Base Industrielle Européenne du Numérique (BIEN) doit s'appuyer sur toute la chaîne de valeur numérique. Il s'agit de structurer un écosystème cohérent d'entrepreneurs (grands groupes et PME), de laboratoires de recherche (universitaires et privés) et d'investisseurs pour développer une politique d'innovation et un socle technologique. Deux considérations sont essentielles pour le succès de cette politique. D'une part, il faut s'assurer de la compétitivité des entreprises, or la taille du marché national est trop limitée pour développer une offre compétitive vis-à-vis des homologues américains, il faut donc la développer au niveau européen et international. D'autre part, il faut développer la confiance, qui peut s'installer entre quelques partenaires puis s'étendre à d'autres pays européens, en pensant des solutions maîtrisées par des fournisseurs européens qui peuvent garantir l'absence de moyens de contournement. Enfin, il est nécessaire de structurer le dialogue public-privé sur les questions de politique industrielle et d'envisager, par exemple, la création d'un label européen de confiance et de mener une politique de soutien aux PME.

D'un point de vue politique, le pouvoir normatif et règlementaire dont dispose l'Europe pourrait se traduire par une puissance d'influence mise à disposition de ses intérêts et ses valeurs dans le cyberespace. L'Europe est un modèle d'intégration économique et de gouvernance, et de gestion partagée de la norme. Le modèle rayonne en Asie. Des textes européens (Protection des données à caractères personnels, Convention sur la cybercriminalité) sont cités en référence dans de nombreux pays. Ce pouvoir peut aussi servir des intérêts économiques. Développer un régime juridique de protection des données

personnelles qui soit à la fois solide et équilibré pourrait permettre : 1. Qu'il puisse être reproduit par d'autres pays et exercer ainsi un pouvoir d'influence ; 2. Qu'il puisse être attractif pour que les entreprises étrangères souhaitent héberger leurs données sous le régime juridique européen, ce qui permettrait par leurs flux de données de générer de la valeur ; 3. Qu'il constitue un levier politique et juridique pour contrecarrer l'extra-territorialité des Etats-Unis.

Enfin, une fenêtre d'opportunité s'ouvre pour que l'Europe émerge comme acteur de la gouvernance du cyberespace, à un moment particulier de l'histoire où l'Internet amorce le virage des 3 milliards d'utilisateurs et de nombreux débats sont à l'agenda des négociations internationales. A condition de s'en donner les moyens, l'Europe pourrait peser dans les discussions et les décisions qui permettront d'une part de redéfinir la gouvernance de l'Internet au niveau mondial et d'autre part d'établir les nouveaux cadres de la sécurité collective à l'âge des réseaux interconnectés. Cela implique d'articuler une position commune aux pays européens sur la gouvernance du cyberespace pour assurer l'avenir de l'Internet et de la sécurité collective, dans le respect de la souveraineté des Etats membres et des valeurs qui les unissent. Cette réflexion est indispensable si l'on souhaite que l'Europe devienne une force de proposition et un levier politique pour façonner et non subir le cyberespace du futur.

BIBLIOGRAPHIE

Arsène, Séverine, Internet et politique en Chine. Les contours normatifs de la contestation, Paris, Karthala, coll. « Recherches internationales », 2011, 420 p.

Benhamou Bernard et Sorbier Laurent, « Souveraineté et réseaux numériques », *Politiques étrangère* 3/2006 (Automne), p. 519-530

Benhamou Bernard, "Organiser l'architecture de l'internet", *Esprit*, No 5, 2006

Benhamou Bernard, 2014, « Quelle gouvernance mondiale de l'Internet apèrs l'affaire Snowden ? », *Revue de l'Ecole Nationale d'Administration*, avril 2014

Brown Ian, *Research Handbook on Governance of the Internet*, Edward Elgar Pub, 2013

Castro Daniel, « How Much will PRISM Cost the U.S. Cloud Computing Industry ? », *Information Technology and Innovation Foundation*, août 2013

Center for European Economic Research, *Effective Tax Levels unsig the Devereux / Griffith Methodology*, 2012

Chander Anupam et Le Uyen, « Breaking the Web : Data Localization vs. The Global Internet », *UC Davis Legal Studies Research Paper Series*, Université de Californie, 2014

Chiche N., « Internet : pour une gouvernance ouverte et équitable », *Les études du Conseil économique, social et environnemental*, 2014
Conseil d'Etat, « Le numérique et les droits fondamentaux », Les rapports du Conseil d'Etat, 2014

Cox, Noel, "The regulation of cyberspace and the loss of national sovereignty", *Information and Communications Technology Law*, Vol.11, No3, pp. 241-253, 2002

Christou George et Simpson Seamus, "The European Union, multilateralism and the global governance of the Internet", *Journal of European Public Policy*, Vol. 18, No 2, 2011

Christou George et Simpson Seamus, "The influence of Global Internet Governance Institutions on the EU" in *The Influence of International Institutions on the EU : When Multilateralism hits Brussels* (dir. Oriol et Knud), Palgrave Macmillan, 2012

David Lonsdale, *The nature of War in the Information Age : Clausewitzian Future*, Frank Cass Publishers, 284p., 2003

Deibert, Ronald, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, *Access Contested: Security, Identity and Resistance in Asian Cyberspace*, The MIT Press, 2012

Douzet Frédérick, « Les frontières chinoises de l'Internet », *Hérodote*, n°125, 2007

Douzet Frédérick (sous la dir.), Enjeux géopolitiques du cyberspace, *Hérodote*, n°152-153, 2014

Dunn Cavelty, Myriam and Mike Suter, "Public-Private Partnership are no silver bullet : An expanded governance model for critical infrastructures protection", International Journal of Critical Infrastructure Protection, Vol.2, No 4, pp.179-187, 2009

Dunn Cavelty, Myriam, Cyber-Security and Threat Politics, London, New York, Routledge, 2008

Erhel C. et La Raudière L., « Le développement de l'économie numérique française », Rapport d'information de l'Assemblée Nationale par la Commission des affaires économiques, mai 2014

Etude de suivi des compétences numériques, *eSkills Monitor*, Commission européenne, 2009

European Centre for International Political Economy, « The Economic Importance of Getting Data Protection Right : Protecting Privacy, Transmitting Data, Moving Commerce », 2014`

European Commission, An area of freedom, security and justice serving the citizen, COM(2009) 262 final, Brussels, 2009.

European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Agenda for Europe, COM 2010(245) final, 20 May 2010b. http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0245:EN:NOT

European Commission, Communication from the Commission, Europe 2020: A strategy for smart, sustainable and inclusive growth, COM2010 (2020), Brussels, 3 March 2010a.

European Commission, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23 November 1995, p. 31–50.

European Commission, Europe 2020 Flagship Initiative - Innovation Union, COM(2010) 546 final, Brussels, 6 October 2010c.

European Commission, Ministerial Declaration of the 4th Ministerial e-Government Conference, Lisbon, 19 Sept 2007.
http://ec.europa.eu/information_society/activities/egovernment/conferences/2007/conference_main/index_en .html

European Commission, Working together for growth and jobs: A new start for the Lisbon Strategy, Communication to the Spring European Council from President Barroso in agreement with Vice-President Verheugen, COM(2005) 24, Brussels, 2 Feb 2005.

Executive Office of the President, *Big Data : Seizing Opportunities, Preserving Values*, Maison Blanche des Etats-Unis, mai 2014

Franzese, Patrick, "Sovereignty in Cyberspace: Can it exist?", Air Force Law Review, Vol 64, pp.1-42, 2009

Gartner, « Forecast: PCs, Ultramobiles, and Mobile Phones, Worldwide, 2010-2017, 4Q13 Update », 2013

Goldsmith Jack et Wu Timothy, "Digital Borders", *Legal Affairs*, Janvier-février 2006

Goldsmith Jack et Wu Timothy., *Who controls the Internet Illusions of a Borderless World?*, oxford University Press, 2006

Hare, Forrest, "Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security?", in The Virtual Battlefield : Perspectives on Cyber Warfare, Vol. 3, pp. 88 - 105, 2009

Hariharan G., *Marci Civil da Internet : Brazil's 'Internet Constitution'*, The Center for Internet and Society, 3 avril 2014

Hill Jonah Force, "A Balkanized Internet? The Uncertain Future of Global Internet Standards", *Georgetown Journal of International Affairs*: International Egagement on Cyber 201: Establishing Norms and Improving Security, 2012

Hill Jonah Force, *Internet Fragmentation – Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policy Makers*, John F. Kennedy School of Government, Harvard University, 2012

Hill Jonah Force, « The Growth of Data Localization post-Snowden : Analysis and Recommendations for U.S. Policymakers and Industry Leaders », *Lawfare Research Paper Series*, Vol. 2, n°3, 2014

Ito Joichi, "The internet", 11 juillet 2005, blog Joi Ito: http://joi.ito.com/weblog/2005/07/11/the-internets.html

Kalathil Shanthi et Boas Taylor, *Open Networks, Closed Regimes: The impact of the Internet on Authoritarian Rule*, Carnegie Endowment for International Peace, Washington DC., 2003

Kluver Randolph, « The Architecture of Control: a Chinese Strategy for e-Governance », Journal of Public Policy, Vol 25, No 1, Mai 2005, pp 75-97

Kroes, Neelie, “Data Is the New Gold”, Speech presented at the Press conference on Open Data Strategy, Brussels, 12 December 2011.
http://europa.eu/rapid/press-release_SPEECH-11-872_en.htm?locale=en

Labarre Jérémy, « La Cybersécurité Europeenne : de l’importance d’une politique industrielle », rapport au Conseil de l'Union européenne, 2014

La dépendance de la France en matière de données et services numériques, Assemblée Nationale,
http://www.assemblee-nationale.fr/14/cr-oecst/programme_AP_risque_numerique.pdf

Laïdi, Zaki, *La norme sans la force – L’énigme de la puissance européenne*, Presses de la Fondation Nationale des Sciences Politiques, Paris, 2005

Lescure Pierre , « Culture – Acte 2 », Mission « Acte II de l’exception culturelle », *Contribution aux politiques culturelles à l’ère numérique* , 2013

Lessig L, Code and other laws of cyberspace, New York, Basic Books, 1999

Libicki Martin, *Crisis and Escalation in Cyberspace*, RAND Corp., 2012

Libicki, Martin, *Cyberdeterrence and Cyberwar*, RAND Corporation, 2009

Livre blanc rédigé par l’Association Française des Éditeurs de Logiciels et Solutions Internet, *Cyber-sécurité : Hisser les acteurs français au niveau de la compétition mondiale*, 2014

Mathiason John, *Internet Governance: The new frontier of global institutions*, Routledge, 2009

Market and Market, *Industrial Control Systems (ICS) Security Market Market Forecast & Analysis (2013 - 2018)*, 2013

Maurer Tim et Morgus Robert, « Tipping the Scale : An Analysis of Global Swing States in the Internet Governance Debate », *Internet Governance Papers*, Paper No.7, Center for International Governance Innovation, 2014

Mayer-Schoenberger V. et Ziewitz M., « Jefferson Rebuffed – The United States and the Future of Internet Governance », *Faculty Research Working Papers Series*, Harvard University, 2006

McKinsey Global Institute, *Big data : The next frontier for innovation, competition and productivity*, 2011

Mell Peter et Grance Tomothy, “The NIST Definition of Cloud Computing”, *NIST Special Publication*, n° 800-145, US Department of Commerce, Computer Security Division, 2011

Minkel J.R., “Could the Internet fragment? [domain name system], *Spectrum IEEE*, Vol.43, No 6, 2006

Morin-Desailly, Catherine, L'Union européenne, colonie du monde numérique ?, Rapport d'information pour la commission des affaires européennes n° 443 (2012-2013) - 20 mars 2013, http://www.senat.fr/noticerapport/2012/r12-443-notice.html

Morin-Desailly Catherine, « Nouveaux rôle et nouvelle stratégie pour l’Union européenne dans la gouvernance mondiale de l’Internet », Rapport d’information pour la commission des affaire européenne du Sénat, juillet 2014

Mueller Milton, *Networks and States: The global politics of Internet governance*, MIT Press, 2010

Nicholson Jessica et Noonan Ryan, Digital Economy and Cross Border Trade : The Value of Digitally-Delivrable Services, US Department of Commerce, Economics and Statistics Administration, 2014

Nye, Joseph, Cyber Power, Center for Science and International Affairs, Harvard Kennedy School, 2010

Nye J., *Bound to Lead : The Changing Nature of Americain Power*, New York, Basic Books, 1990

Pew Research Center, “Net Threats”, 2014

Pew Research Center, « The Internet of Things », 2014

Rapport du Parlement Européen sur l’achèvement du marché unique numérique, 2012 - http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2012-0341+0+DOC+XML+V0//FR

Rapport du Parlement Européen sur une stratégie pour la liberté numérique dans la politique étrangère de l’Union, 2012 - http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2012-0374+0+DOC+XML+V0//FR

Rapport Colin & Collin sur la fiscalité du secteur numérique - 18/01/2013, http://www.redressementproductif.gouv.fr/rapport-sur-fiscalite-secteur-numerique

Rapport du Department for Business, *Innovation and Skills (BIS) Impact Assessment of NIS Directive*, 2013

Reding Viviane, Member of the European Commission responsible for Information Society ans Media, « Internet of the future: Europe must be a key player”, discours du 2 février 2009 à Bruxelles lors du Future of the Internet initiative of the Lisbon Council

Renaissance numérique, « Netmundial, vers une gouvernance post-Snowden de l'Internet », 2014

Rose Richard, "Language, Soft Power and Asymmetrical Internet Communication", *OII Research Report No 7*, 2005

Seng Ching Hong James, "Internationalisation and Localisation of the Internet", http://james.seng.sg/files/public/internationalisation_localisation.pdf

Schafer Valérie, "Internet l'illusion démocratique : de "la République des ingénieurs" à la gouvernance", in *Internet et politique*, Coutant Alexandre (dir.), Paris, CNRS, 2012, 188p.

Shackleford S. et Craig A., « Beyond the New 'Digital Divide' : Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity », *Legal Studies Research Paper Series*, n°290, Indiana University, 2014

Special Eurobarometer 404, Cyberserity Report, Novembre 2013

Sunstein Cass, *Republic 2.0*, Princeton University Press, 2009

Todorova Maria, *Imagining the Balkans*, Oxford University Press, 1997

US Chamber of Commerce et Hunton & Williams, *Business Without Borders : The Importance of Cross-Border Data Transfers to Global Prosperity* », 2014

Visiongain, *Global Cyber Seucrity Market Report 2013-2023*, 2013

Werle Raymund, "Lessons learnt from the Internet. Hands off, hands on, or what role of public policy in Europe?", Druzboslovne razprave, Vol 18, No 40, p.63-82

Wu, Timothy, "Cyberspace Sovereignty? The internet and the International System", *Harvard Journal of Law & Technology*, Vol. 10, No.3, pp.647-66, 1997

Wu Tim, "The Filtered Future: China's bod to divide the Internet", 11 juillet 2005: http://www.slate.com/articles/news_and_politics/jurisprudence/2005/07/the_filtered_future.html

Xerfi, « La cybersécurité : Enjeux et perspectives d'un marché en pleine mutation », 2012

Zittrain Jonathan, *The future of the Internet ans How to stop It*, Yale University Presse, 2008