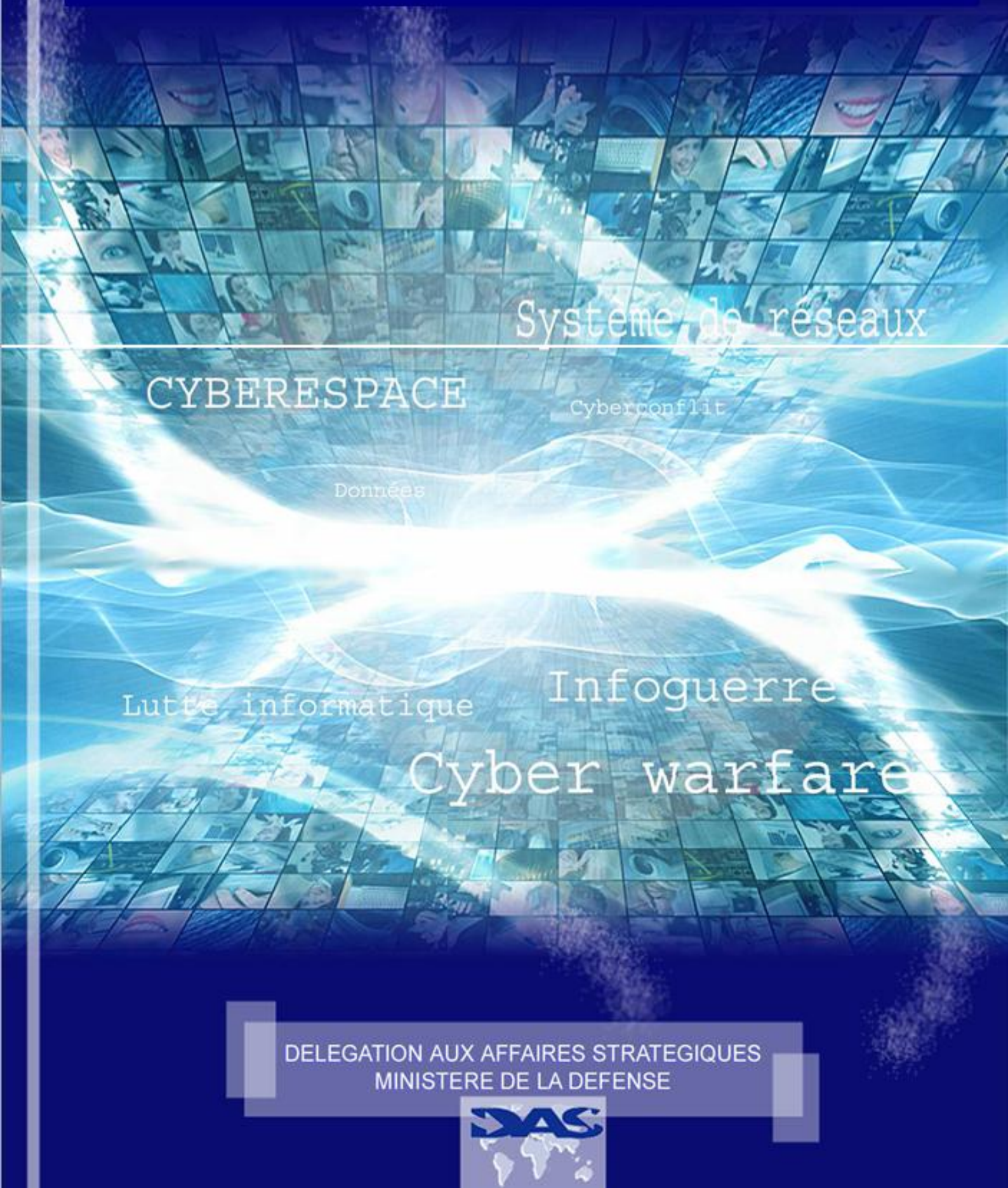
Observatoire du Monde Cybernétique
Trimestriel

Mars 2012



DELEGATION AUX AFFAIRES STRATEGIQUES
MINISTERE DE LA DEFENSE

La Délégation aux Affaires Stratégiques propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation.

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

A ce titre, la DAS a confié à la **Compagnie Européenne d'Intelligence Stratégique (CEIS)** cet Observatoire du Monde Cybernétique, sous le numéro de marché 1502492543.

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

Table des matières

1 Les enjeux actuels de la gouvernance d'Internet

Le 15 mars 2012, l'Europe publiait sa nouvelle stratégie sur la gouvernance d'Internet. Ce document signe la volonté des 47 Etats européens de devenir des acteurs essentiels du processus mondial de gouvernance, à travers l'affirmation de six domaines clés : l'universalité, l'intégrité et l'ouverture d'Internet ; la défense des droits et des libertés des internautes ; la protection des enfants ; la promotion de la démocratie et de la culture ; la lutte et la coopération contre la cybercriminalité ; et, surtout, la confidentialité et la protection des données.

Ce document, s'il est ambitieux, ne marque pas de rupture entre l'Europe et l'ICANN, institution majeure en matière de gouvernance d'Internet. La nouvelle stratégie européenne maintient le dialogue avec l'institution américaine, avec la volonté toutefois d'en influencer le fonctionnement et d'affirmer ce qui ressemble de plus en plus à un véritable modèle européen de la gouvernance d'Internet.

Se dessinent alors plusieurs axes de gouvernance. L'Europe se démarque du modèle américain, tandis que certains pays émergents ou en voie de développement tentent d'imposer leur modèle de gestion d'Internet. Retour sur l'actualité de la gouvernance Internet.

Définition

La gouvernance d'Internet a été définie lors du SMSI de 2005 comme « le développement et l'application par les **gouvernements**, le **secteur privé** et la **société civile**, dans leurs rôles respectifs, des principes, normes, règles, procédures décisionnelles et programmes communs qui façonnent **l'évolution et l'utilisation** de l'internet ». Mais cette définition ne rend pas compte des conflits d'interprétation dont souffre le concept de « gouvernance Internet ». Et si l'emploi du terme « gouvernance » pourrait laisser penser qu'elle n'est l'affaire que des institutions étatique, force est de constater que le caractère mondial et multilatéral inhérent à Internet implique des acteurs extrêmement divers.

1.1 La gouvernance d'Internet à l'américaine, un modèle fragilisé

Le glissement du débat de la gouvernance exercée par l'ICANN à une gouvernance centrée sur le Cloud computing. Les débats tournant autour du statut de l'ICANN sont désormais courants. La critique de l'étendue des pouvoirs de l'institution et de la mainmise des Etats-Unis sur Internet laisse cependant place à un débat nouveau, centré sur la question du Cloud computing et de la souveraineté des données.

1.1.1 L'étendue des pouvoirs de l'ICANN en matière de gouvernance Internet

L'ICANN, ou « la société pour l'attribution des noms de domaine et des numéros sur Internet » est l'institution gouvernant Internet. Son rôle prépondérant s'explique par sa maîtrise du « pouvoir d'adressage » : elle effectue la coordination technique entre noms de domaines et adresses IP.

Pour simplifier le rôle de l'ICANN, Internet consiste dans la réunion de deux « systèmes » : le premier vise la communication (les protocoles TCP/IP) et le second l'adressage (le Domain Name System, ou DNS[1]). Avant qu'un ordinateur puisse communiquer avec un autre, il émet une requête au DNS à l'aide de l'adresse IP de cet autre ordinateur. Le DNS est chargé de renvoyer l'URL correspondante. Le DNS consiste donc en une grande base de données de correspondance entre des adresses URL et des adresses IP. Ainsi, pour exister sur Internet, un ordinateur doit figurer dans la liste de l'espace de nommage du DNS[2].

Par conséquent, en gérant le DNS, l'ICANN a la possibilité de bloquer un nom de domaine, celui d'un Etat par exemple, et ainsi de couper l'accès à Internet à des millions d'utilisateurs.

L'ICANN est une société à but non lucratif de droit californien. Par conséquent, elle est soumise au ministre de la justice de cet Etat. Or, elle est de compétence mondiale et ses décisions s'imposent à tous les pays. L'ICANN bénéficie ainsi d'un statut ambigu très contesté, et ce, depuis sa création. Sa mise en œuvre a en effet été difficile en 1998. Alors que l'Union internationale des télécommunications souhaitait créer un organisme, le Council of registres, sous l'égide de l'ONU, c'est la création de l'ICANN qui a été retenue et imposée par le gouvernement américain.

Ce dernier dispose donc du pouvoir, au moins théorique, de couper l'accès à Internet de millions d'utilisateurs dans le monde par le simple blocage d'un nom de domaine. Rappelons qu'en vertu d'un accord signé le 25 novembre 1998 par l'ICANN (« Memorandum of understanding »)[3], cette dernière accorde un droit de véto au département du commerce américain sur la plupart de ses décisions.

De plus, le système de nommage, le DNS, est dirigé par 13 serveurs racines, et parmi ces 13 serveurs, 10 sont situés aux Etats-Unis, 2 en Europe (Londres et Stockholm) et 1 au Japon. Leur emplacement est un facteur de puissance, un atout considérable pour la résilience et la redondance des connexions. Et, bien qu'au quotidien ils soient supervisés par des sociétés privées, des universités ou des administrations, il ne s'agit que de délégations fournies par l'ICANN, décisionnaire en dernier lieu[4].

En disposant de l'ICANN sous leur juridiction, les Etats-Unis bénéficient d'un avantage sans précédent et peuvent directement influencer l'Internet mondial. Par exemple, les noms de domaine .af et .iq ont été fermés au cours des guerres menées par les Etats-Unis contre l'Afghânistân et l'Iraq[5].

---

[1] Service permettant de traduire un nom de domaine en informations de plusieurs types qui y sont associées, notamment en adresses IP de la machine portant ce nom. Source : wikipedia.

[2] http://smsi.francophonie.org/IMG/pdf/icann-klein.pdf

[3] Voir article V.A.1. du Memorandum Of Understanding, consultable ici : http://www.icann.org/en/general/icann-mou-25nov98.htm

[4] http://www.ege.fr/download/la_guerre_des_ondes.pdf

[5] http://www.ege.fr/download/la_guerre_des_ondes.pdf

1.1.2 L'autorité de l'ICANN remise en cause

1.1.2.1 L'ICANN désavouée lors de la révision du statut de l'IANA

Le jeudi 10 novembre 2011, les autorités américaines ont lancé un appel d'offres[6] sur la gestion de la fonction assurée par l'IANA. Intégrée à l'ICANN, l'Internet Assigned Numbers Authority recense l'ensemble des noms de domaine de premier niveau et les suffixes pays dans les URL. Or, priver l'ICANN de la gestion IANA revient à la « vider de sa substance »[7]. Quelques semaines plus tard, les autorités américaines annulaient l'appel d'offres au motif qu'elles n'avaient pas reçu de propositions satisfaisantes. L'annulation de la consultation fut l'occasion, pour la NTIA[8], de rappeler ses exigences en la matière : une séparation structurelle entre l'élaboration de la politique et sa mise en œuvre, une « solide » politique applicable en matière de conflit d'intérêt et des exigences de consultation et de reporting pour augmenter la transparence et la responsabilité vis-à-vis de la communauté internationale[9].

1.1.2.2 La pression de la Chine et de la Russie en faveur d'un transfert de compétences à l'ONU.

Certains Etats, tels que la Chine ou la Russie, contestent le modèle actuel de gouvernance ayant comme institution principale l'ICANN, organisme de droit californien. En cause : l'impossibilité, pour les pays en développement, de suivre correctement les débats et de s'assurer une pleine participation aux processus de décision dans la gouvernance d'Internet telle qu'assurée aujourd'hui. Selon la Chine, l'Iran ou encore la Russie, c'est une organisation intergouvernementale, à l'image de l'UIT, qui doit gouverner Internet.

Les Etats de l'OCS (Russie, la Chine, l'Ouzbékistan et le Tadjikistan entre autres) ont par exemple déposé en septembre 2011 une résolution à l'Assemblée générale de l'ONU afin d'instaurer un Code de conduite sur Internet. Leur volonté : assurer un contrôle mondial sur les échanges d'informations et mettre fin à la mainmise des Etats-Unis sur la gouvernance Internet[10].

Un signal faible

La volonté de l'UIT de jouer un rôle important dans la gouvernance de l'Internet se traduit également par des signaux diplomatiques faibles. Exemple en 2006, lorsque l'UIT a orthographié le terme « Internet » avec un « i » minuscule au lieu du « I » majuscule usuel. Certains ont pu, lors de la conférence de l'UIT d'Antalya de novembre 2006, interpréter cela comme la traduction de l'intention de l'UIT de traiter Internet comme les autres systèmes de télécommunications déjà internationalement régis par l'UIT. Pensons notamment au télégraphe, téléphone, radio, télévision, etc.

Selon le Brésil, l'Inde et l'Afrique du Sud, il fallait plutôt créer une nouvelle organisation internationale destinée à remplacer l'UIT. Liée aux Nations Unies, cette « Organisation Internationale de

[6] https://www.fbo.gov/index?s=opportunity&mode=form&id=c564af28581edb2a7b9441eccfd6391d&tab=core&_cview=0
[7] http://www.lemonde.fr/technologies/article/2011/11/14/la-racine-du-net-soumise-a-un-appel-d-offres_1603342_651865.html

[8] National Telecommunications and Information Administration : agence du Département du commerce américain, chargée de conseiller le Président des Etats-Unis en matière de télécommunications. Elle est à l'origine de l'appel d'offres en question.

[9] http://www.lemondeinformatique.fr/actualites/lire-l-icann-s-attaque-a-la-racine-de-ses-conflits-d-interets-48149.html
[10] http://premier.gov.ru/eng/events/news/15601/

l'Internet »[11] serait basée sur un nouveau traité, intégrerait et superviserait les institutions déjà chargées de la gouvernance d'Internet et arbitrerait les différends pouvant naître entre les États concernant le réseau[12].

L'argument revenant systématiquement est donc celui d'une gouvernance assurée par un organisme international et légitime : les Nations Unies.

En ce sens, des négociations se sont ouvertes le 27 février entre les 193 Etats membres de l'UIT à propos de l'élaboration d'un nouveau traité sur la gouvernance Internet. Mais toute volonté de réforme de la gouvernance actuelle risque d'être mal accueillie par les Etats-Unis. Ces derniers soutenant, à l'image de ce qu'a pu affirmer Robert McDowell, membre de la Commission fédérale des communications (FCC), que « toute tentative d'étendre les pouvoirs intergouvernementaux à Internet devrait être rejetée », et que le transfert de compétences à l'ONU représente un risque pour la liberté d'Internet[13].

1.1.3 Un modèle qui fonctionne encore

1.1.3.1 L'ICANN confortée dans son rôle de régulateur technique

Un contrat taillé pour l'ICANN ?[14] Selon certaines sources, l'appel d'offres sur la fonction IANA serait « taillé pour l'ICANN » et il serait très peu probable que l'organisation en perde le contrôle. Il s'agirait ainsi d'un faux-débat, cette consultation n'étant que la traduction de la volonté des autorités américaines d'affirmer leur indépendance quant à l'ICANN. Enfin, Neelie Kroes, vice-présidente de la Commission européenne, a eu l'occasion de rappeler que le contrat était « réservé aux entreprises américaines, ce qui est une honte étant donné qu'Internet est une ressource pour le monde entier »[15].

Un organisme qui a su gagner en légitimité. Malgré les critiques qui lui sont portées, force est de constater que la solution rassemble toujours de nombreux partisans. D'après Bernard Benhamou, spécialiste des questions de gouvernance d'Internet, il est difficile d'envisager une gestion internationale d'Internet sans risque pour les libertés et la neutralité du Net. L'expert a notamment souligné que « si on reprend le principe d'une voix par pays, une majorité d'État(s) non démocratique(s) pourrait(ent) exiger un rôle croissant ». Il y aurait ainsi « un risque de dérive et de fragmentation d'Internet, une remise en cause des trois principes fondamentaux : la neutralité, l'ouverture et l'interopérabilité des réseaux »[16].

Selon d'autres, l'ICANN aurait aujourd'hui capitalisé une compétence technique incontestable en matière de gestion de système de nommage. De plus, avec un fonctionnement multi-acteur, elle reflèterait à juste titre la diversité des noms de domaines à l'échelle mondiale[17]. Changer d'autorité serait un véritable pas en arrière.

---

[11] http://www.culturalivre.org.br/artigos/IBSA_recommendations_Internet_Governance.pdf
[12] http://www.lefigaro.fr/hightech/2012/02/22/01007-20120222ARTFIG00627-les-etats-unis-pressent-pour-garder-le-controle-d-internet.php
[13] http://online.wsj.com/article/SB10001424052970204792404577229074023195322.html
[14] http://www.lemonde.fr/technologies/article/2011/11/14/la-racine-du-net-soumise-a-un-appel-d-offres_1603342_651865.html
[15] http://blogs.ec.europa.eu/neelie-kroes/new-iana-contract-details-published-encouraging-news-for-the-future-of-the-internet/
[16] http://www.lefigaro.fr/hightech/2012/02/22/01007-20120222ARTFIG00627-les-etats-unis-pressent-pour-garder-le-controle-d-internet.php
[17] http://www.domainesinfo.fr/interview/118/cedric-manara-le-droit-des-noms-de-domaine-le-premier-ouvrage-dedie-au-nommage-sur-internet.php

Un pouvoir à double tranchant. En théorie, les Etats-Unis ont la possibilité de « retirer un pays de l'Internet ». Mais ce pouvoir est à double tranchant. S'il permet d'affirmer leur autorité, un tel acte pourrait nuire aux Etats-Unis eux-mêmes en mettant en péril le réseau. Cela aurait également pour effet de motiver certains pays, certaines régions, à se protéger d'un tel scénario en développant leurs propres « Internets » régionaux ou nationaux. Ce qui va à l'encontre de l'idée que les Etats-Unis se font du réseau : un espace où s'impose leur « soft power » qui n'a de raison d'être qu'en présence d'autres puissances étrangères. Les Etats-Unis semblent en avoir pris conscience, à travers l'« Affirmation of Commitment » signé entre l'ICANN et le Département du Commerce américain.

L'ICANN prend les mesures nécessaires à sa pérennité. Face aux critiques qui lui sont faites, l'ICANN réagit en prenant des mesures favorisant une gestion plus internationale de certains actifs d'Internet. A titre d'exemple, une « Root convention » a été proposée. Son objectif : confier à la communauté internationale la surveillance de la politique des serveurs racines, ou confier aux Etats les droits nécessaires sur la gestion de leurs domaines nationaux. Autre exemple : l'introduction des noms de domaine non-ASCII pour l'arabe et le chinois. Une telle proposition réduit le risque de désintégration du DNS Internet et affirme la légitimité de l'ICANN à assurer la gouvernance des infrastructures Internet.

Vers un changement de statut. Le Protocole d'accord de 2006 entre l'ICANN et le Département du Commerce des Etats-Unis ouvrait déjà la perspective de l'internationalisation du statut de l'ICANN. Cette tendance a été affirmée suite à l'élection de Barack Obama, partisan du multilatéralisme qui influence désormais fortement le fonctionnement de l'ICANN. L'organisation est aujourd'hui régie par l'« Affirmation of Commitment » signé le 1er octobre 2009 avec le Département du Commerce des Etats-Unis. Là encore les griefs portés contre l'ICANN semblent être pris en compte, puisque le document envisage la transformation de l'ICANN en institution plus indépendante. En faisant évoluer ainsi son statut, l'ICANN souhaite tenter le compromis : conserver les avantages actuels de sa structure tout en répondant aux exigences des partisans d'une gouvernance plus internationale.

1.1.3.2 La mainmise des Etats-Unis encore largement affirmée dans le cadre de la lutte contre les atteintes à la propriété intellectuelle

SOPA et PIPA. La volonté des Etats-Unis d'assurer leur mainmise sur Internet s'est récemment traduite par l'introduction à la Chambre des représentants, en octobre 2011, du projet de loi Stop Online Piracy Act dit SOPA. Le texte donne la possibilité à l'autorité judiciaire d'imposer aux entreprises américaines de cesser toute activité avec un site accusé de violer les droits d'auteur, et impose aux FAI américains de rendre inaccessibles ce type de sites. En mai de la même année, le Protect IP Act, dit PIPA, proposait déjà des mesures similaires. Ces projets sont aujourd'hui l'objet d'une forte contestation de la part de la société civile et du secteur privé. Le vendredi 13 janvier, l'une des dispositions les plus contestées du texte SOPA (prévoyant d'imposer le blocage des sites aux fournisseurs d'accès) a été supprimée du projet. Face au tollé provoqué par ces textes, les sénateurs ont repoussé leur vote à une date ultérieure.

La saisie de nom de domaines et de serveurs. Si l'ICANN fait l'objet de nombreuses critiques, la gestion de l'infrastructure principale d'Internet n'est pas le seul moyen pour les Etats-Unis d'affirmer leur rôle en matière de gouvernance Internet. L'affaire dite « Megaupload » est l'illustration de la mainmise encore importante des autorités américaines sur cette gouvernance. En effet, sur simple injonction de la justice américaine, il est possible pour les Etats-Unis de saisir et de désactiver serveurs et noms de domaines, dès lors que ceux-ci sont gérés par des sociétés américaines ou sur le territoire américain. C'est en effet une société américaine ayant son siège en Californie, Verisign, qui gère les

95 millions de noms de domaine en .com (sur un total de 220 millions de noms de domaine)[18]. Le porte-parole de l'Immigration and Customs Enforcement (ICE) a eu l'occasion de le confirmer[19] et de rappeler que « les noms de domaine en .com, .net, .org, .cc, .tv et .name sont tous gérés par des organismes installés sur le sol américain comme VeriSign ou le Public Interest Registry ».

Ce débat a été ravivé après la fermeture, par le FBI, des noms de domaines[20] : megaupload.com, megaupload.org, megavideo.com, megavideoclips.com, etc.

Mais les autres exemples en la matière sont nombreux : début 2012, 307 noms de domaines de sites Internet accusés de diffuser illégalement des matchs de Superbowl ont été saisis. Début 2011, 84 000 sites légitimes étaient bloqués par erreur par les autorités américaines, lors d'une opération similaire.

Les Etats-Unis ne sont pas les seuls à exercer cette prérogative. La Lybie a eu l'occasion de fermer le nom de domaine vb.ly, estimant le contenu du site contraire aux conditions d'utilisation fixées par le registre.

S'il n'y a pas, ou peu de cas de saisie de noms de domaines français relatés dans la presse, le droit français permet la suppression d'un nom de domaine en .fr. Selon l'article L45-2 du code des postes et des communications électroniques, un nom de domaine peut être supprimé lorsqu'il est susceptible de porter atteinte à l'ordre public ou aux bonnes mœurs, à des droits de propriété intellectuelle ou de la personnalité, ou identique ou apparenté à celui d'un acteur public. Mais cette suppression est conditionnée à une notification préalable du titulaire du nom de domaine : celui-ci devra présenter ses observations afin de justifier d'un intérêt légitime, prouver qu'il a agi de bonne foi et/ou régulariser sa situation s'il souhaite conserver son nom de domaine.

Ainsi, « toute activité en ligne est entièrement suspendue à la chaîne de nommage qui permet d'y donner accès »[21].

1.1.4 La régulation du Cloud computing désormais au centre des débats de la gouvernance Internet ?

Comme la problématique du Web 2.0 et des réseaux sociaux a pu bousculer les débats en 2010, l'intégration croissante du Cloud computing (ou informatique en nuages[22]) semble prendre le pas sur les problématiques classiques de gouvernance Internet et pose des questions nouvelles.

Le Cloud computing se développe en raison de la dépendance croissante des particuliers, entreprises privées et acteurs publics aux services en ligne. Sa stabilité et sa sécurité sont donc des enjeux majeurs de la gouvernance d'Internet.

Le Cloud computing constitue également un challenge pour la gouvernance technique. La mutualisation des ressources à l'échelle nationale implique en effet la possibilité de transfert des données. Des

[18] http://www.lapresse.tn/21012012/43935/un-exemple-eloquent-de-la-mainmise-americaine-sur-internet.html
[19] http://www.wired.com/threatlevel/2012/03/feds-seize-foreign-sites/all/1

[20] Mais aussi megastuff.co, megaworld.com, megaclicks.co, megastuff.info, megaclicks.org, megaworld.mobi, megastuff.org, megaclick.us, mageclick.com, HDmegaporn.com, megavkdeo.com, megarotic.com, megaclick.com, megaporn.com.

[21] http://domaine.blogspot.fr/2012/02/en-france-peut-on-saisir-suspendre-ou.html

[22] http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000022309303

transferts qui ne se réaliseront qu'en présence de standards communs aux opérateurs de Cloud computing.

Le Cloud computing est enfin un véritable défi pour la gouvernance juridique d'Internet. Dans sa définition de l'informatique en nuage, la Commission générale de terminologie et de néologie précise qu'il s'agit d'une « forme particulière de gérance de l'informatique, dans laquelle l'emplacement et le fonctionnement du nuage ne sont pas portés à la connaissance des clients »[23]. Se pose ici la question de la loi applicable à ces données. Par exemple, les principaux acteurs du Cloud étant basés aux Etats-Unis (HP, Amazon, Google, IBM, Intel, Oracle, Red Hat, Microsoft[24]), les données dans le nuage sont-elles soumises à la législation américaine et, plus précisément, à l'USA Patriot Act ? Les Etats sont de plus en plus nombreux à réagir en se lançant dans la création de Clouds souverains afin de protéger leurs données et celles de leurs citoyens.

Déjà, en 2005, le GTGI (Groupe de travail sur la gouvernance de l'Internet) considérait[25] la protection des données et le respect de la vie privée comme des « questions d'intérêt général qui se rapportent à la gouvernance de l'Internet ». Or, le Cloud implique l'externalisation du stockage de données, notamment de données à caractère personnel. Quid de la gestion et de la protection de ces données ? Quel est leur statut juridique ?

C'est notamment sur ce terrain que l'Europe souhaite affirmer son modèle de gouvernance de l'Internet.

[23] http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000022309303

[24] http://virtualization.sys-con.com/node/1386896

[25] http://www.itu.int/wsis/wgig/docs/wgig-report-fr.pdf

1.2 Vers l'affirmation d'un modèle européen de gouvernance

L'Europe affirme aujourd'hui sa volonté de peser dans les débats sur la gouvernance Internet. Face à l'ICANN, par exemple, la Commission européenne a affirmé sa position quant au financement et à la transparence de l'institution. Elle a également affirmé son point de vue quant à l'apparition des nouveaux domaines génériques[26]. Enfin, le Cloud constitue un domaine où l'Europe entend imposer sa vision de la protection des données personnelles comme norme au niveau international.

1.2.1 Clouds souverains versus USA Patriot Act, la réaction européenne

La tendance est à la mutualisation des ressources de stockage et de calcul. Le Cloud computing prend une place de plus en plus importante dans l'utilisation de l'outil informatique. Mais les entreprises européennes – et surtout les gouvernements - s'inquiètent désormais de l'endroit où résident leurs applications et données situées dans le Cloud. Or, les principaux acteurs du Cloud sont américains, et sont, par conséquent, soumis à l'USA Patriot Act.

1.2.1.1 L'USA Patriot Act

Adopté le 25 octobre 2001, le « Uniting and Strengthening America by Providing Appropriate Tools Required to intercept and Obstruct Terrorism Act » créé à l'attention des sociétés américaines et leurs filiales, ainsi qu'aux sociétés non américaines dont les serveurs ou les plateformes se trouvent aux Etats-Unis, des obligations[27] de laisser accéder les services d'enquête aux données stockées dans leur serveur notamment sur leur plateforme Cloud, y compris les données stockées en Europe par des sociétés américaines, à l'insu des titulaires des données sans qu'ils en soient immédiatement informés[28].

Sont ainsi mis à contribution directement les sociétés gérant les données circulant sur l'Internet telles que Google, Microsoft, Facebook, etc.

La loi a notamment confirmé l'autorisation accordée au FBI d'installer un logiciel de surveillance, nommé Carnivore (DS 1000), chez certains FAI, afin d'épier la circulation des messages électroniques et de conserver les traces de la navigation sur le Web de toute personne suspectée de contact avec une puissance étrangère. Et pour ce faire, seul l'aval d'une juridiction spéciale, dont les activités sont confidentielles, est nécessaire. Le texte de la loi allonge également la liste des informations que les enquêteurs peuvent exiger des FAI sans l'aval d'un juge. Il autorise ces derniers à remettre aux autorités, de leur propre initiative, des informations qui ne sont pas relatives au contenu, telle la navigation sur le Web. En contrepartie, le prestataire n'a aucune obligation d'avertir le propriétaire des données.

Selon l'Electronic Frontier Foundation, Google répondrait à des milliers d'injonction de ce type.

L'USA Patriot Act, des conflits d'interprétation

[26] http://blog.internetgovernance.org/pdf/EC-TLD-censorship.pdf
[27] Ces accès sont autorisés par Ordonnance d'un Juge dans le cadre de la section 215 du USA PATRIOT ACT, ou hors du contrôle juridictionnel – même réduit – dans le cadre des sections 504, 505 et 358 du USA PATRIOT ACT
[28] http://lecercle.lesechos.fr/entreprises-marches/high-tech-medias/internet/221144488/usa-patriot-act-risque-majeur-confidentialit

Cegid, éditeur de logiciels français, compte basculer son infrastructure sur les serveurs Cloud d'IBM à partir de juin 2012. Le nouvel hébergement se fera dans le *datacenter* d'IBM France, société de droit français située en territoire français - selon Alain Bénichou, président d'IBM France, les données stockées ne seraient donc pas sujettes à l'*USA Patriot Act*.

Cette affirmation semble néanmoins contradictoire avec les propos tenus par Gordon Frazer, directeur de Microsoft UK, l'été dernier. Interrogé sur le Patriot Act et sa potentielle application sur les données hébergées en Europe chez un fournisseur américain, Gordon Frazer a répondu que Microsoft ne pouvait pas « fournir cette garantie » et « qu'aucune autre société ne le peut »[29].

1.2.1.2 La réaction européenne

Face à ce que l'Europe considère comme une menace pour les données tant stratégiques que personnelles, des projets de « Clouds souverains » ont émergé. Les avantages de ces Clouds souverains sont nombreux :

- Contenir les données stratégiques sur le territoire national afin d'en conserver la maitrise ;
- Soumettre ces données à la législation nationale ou européenne ;
- Favoriser les prestataires de service européens dans un marché largement dominé par les acteurs américains.

[29] http://www.usinenouvelle.com/article/cegid-adopte-le- Cloud-made-in-france-d-ibm.N169900

1.2.2 La protection de la vie privée et des données personnelles, axe majeur de la stratégie européenne de gouvernance d'Internet

1.2.2.1 Le « Safe Harbour » et la directive de 1995, des textes dépassés

Dès 1995, l'Union européenne a développé une législation visant à protéger les traitements de données à caractère personnel. Ce texte pose deux principes :

- les systèmes de traitement de données sont au service de l'homme et doivent - quelle que soit la nationalité ou la résidence des personnes physiques - respecter les libertés et droits fondamentaux de ces personnes, notamment la vie privée[30].

- l'établissement dans un pays tiers à l'Union Européenne du responsable du traitement de données ne doit pas faire obstacle à la protection des personnes.

C'est en ce sens que le « Safe Harbor Agreement » a été adopté. Institué afin d'encadrer les transferts de données à caractère personnel vers les Etats-Unis, cette « sphère de sécurité » permettait aux entreprises américaines de s'auto-certifier en adhérant aux principes de protection des données personnelles et de la vie privée posés par la Commission européenne. Mais cette « sphère de sécurité » est aujourd'hui inopérante.

En effet, la Commission européenne n'a reconnu la validité du Safe Harbour qu'en 2000, antérieurement à la publication de l'USA Patriot Act. Cette validité est désormais caduque, le Patriot Act étant en totale inadéquation avec les principes de la directive de 1995.

Le Safe harbour a également été vivement critiqué par le parlement européen. Il était peu utilisé par les entreprises américaines : une étude démontre que sur 1597 compagnies ayant souscrit au système « Safe Harbour », seules 348 (soit 22%) en remplissent effectivement les exigences (notamment en matière de respect de la vie privée et de protection des données personnelles)[31].

1.2.2.2 La mise à jour de la directive 95/46/CE

A travers la proposition de règlement « General Data Protection Act »[32], l'Europe souhaite reprendre la main sur le traitement des données à caractère personnel en Europe et hors de l'Europe. Le texte prévoit en effet une série de garanties à la charge de l'Etat souhaitant accueillir des données européennes. Citons, par exemple la nécessaire existence et activité dans le pays tiers d'une autorité indépendante de protection des données personnelles (article 38.2 (a)).

Le choix d'un texte plus contraignant

[30] Selon le considérant n°2 de la directive 95/46/CE du Parlement Européen et du Conseil du 24 octobre 1995

[31] (2008) The US Safe Harbor – Fact or Fiction? Galexia. Disponible sur: http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf

[32] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_fr.pdf

Le choix de l'Europe de légiférer sur la question de la protection des données personnelles par un règlement et non une directive traduit sa volonté claire d'imposer sa vision au pays membres comme aux pays non membres.

Aux pays membres d'une part, puisque le règlement européen est directement applicable au sein du droit national, sans besoin d'une transposition dans l'ordre juridique interne des Etats. Il s'applique de manière simultanée à l'ensemble des Etats membres de l'Union. A l'inverse, la directive laisse une marge de manœuvre confortable aux Etats, qui en transposent l'essentiel dans le but d'atteindre les objectifs qu'elle pose dans un certain délai.

Aux pays non-membres ensuite, puisque le texte encadre les transferts de données personnelles hors de l'Union européenne.

1.2.2.3 Des exigences présentes dans la nouvelle stratégie européenne de gouvernance Internet[33]

Le texte publié le 15 mars 2012[34] par le Conseil de l'Europe cette fois-ci, place la protection des données personnelles et la modernisation de la convention 108 (convention du Conseil de l'Europe sur la protection des données à caractère personnel) au cœur de son agenda. L'Europe souhaite également développer un droit à l'oubli sur Internet en procédant à « l'élaboration à l'intention des Etats, du secteur privé et de la société civile de lignes directrices fondées sur les droits de l'homme au sujet de la protection des données, à la lumière des tendances et défis de l'Internet (par exemple en ce qui concerne les données de santé, en particulier les données génétiques, les données biométriques, la prise en compte du respect de la vie privée dès la conception, « **l'informatique dans les nuages** », « **l'Internet des objets** », la demande de **faire retirer de l'Internet les données à caractère personnel**, le traçage par géolocalisation et le consentement éclairé aux conditions générales d'un service) »[35].

Europe/Etats-Unis, vers une vision commune de la promotion des droits et libertés sur Internet

Dans sa nouvelle stratégie de gouvernance Internet, l'Europe souligne sa volonté de « renforcer au maximum les droits et les libertés des usagers de l'Internet ». Ce renforcement se traduira notamment par « l'examen des possibilités d'utilisation positive des technologies de l'information et de la communication (TIC) dans la lutte contre les violations des droits de l'homme ».

---

33 https://wcd.coe.int/ViewDoc.jsp?Ref=CM(2011)175&Language=lanFrench&Ver=final&Site=COE&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

34 https://wcd.coe.int/ViewDoc.jsp?Ref=CM(2011)175&Language=lanFrench&Ver=final&Site=COE&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

35 https://wcd.coe.int/ViewDoc.jsp?Ref=CM(2011)175&Language=lanFrench&Ver=final&Site=COE&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

Dans sa stratégie « No Disconnect », Neelie Kroes appelait déjà au développement d'« outils technologiques destinés à améliorer la protection de la vie privée et la sécurité des populations qui utilisent des TIC dans des régimes non démocratiques ». La Commission européenne souhaitait ainsi fournir aux dissidents des « logiciels qui peuvent être installés sur un ordinateur de bureau, un ordinateur portable, un smartphone ou tout autre appareil »[36]. Avec ce texte, l'Europe s'aligne sur la stratégie américaine visant à promouvoir les outils de lutte contre la censure dans les pays dictatoriaux. Les *« kits de survie sur Internet »* évoqués par Neelie Kroes ne sont en effet pas sans rappeler les fameuses valises « Internet fantôme » imaginées par les Etats-Unis. Un budget de 2 millions de dollars US avait été affecté au développement de ce produit essentiellement destiné aux dissidents de pays où les réseaux mobiles et Internet seraient coupés. L'administration Obama soutient donc déjà activement ces technologies. A l'aide de leur concept de *« diplomatie numérique »*, les Etats-Unis ont pu, par exemple, appuyer les révolutions[37].

Pour en savoir plus, consulter « Commotion Wireless, projet prometteur ou coquille vide » (p. 8, lettre n°69 de décembre 2011, OGI) et « Le marché de la cybersurveillance bousculé : quelles évolutions à venir ? » (p. 5, lettre n° 2 de février 2012, OMC).

[36] VPN, proxys ou autres technologies permettant de garder l'anonymat sur Internet

[37] Notamment en envoyant des équipes former et soutenir les cyberactivistes égyptiens, grâce à des programmes financés par le Département d'Etat ou des fondations privées (Freedom House ou la FED).

1.3 Conclusion

1.3.1 La régionalisation du cyberespace

1.3.1.1 L'apparition de frontières techniques chez les modèles émergents et la notion d'Internet national

La conception initiale d'un Internet sans frontières est mise à mal par l'existence de différents modèles de gouvernance. D'un côté, la protection de la vie privée et des données personnelles portée par l'Europe tant à s'imposer de plus en plus, même si elle s'oppose à certaines législations nationales, notamment au Patriot Act américain.

De l'autre, des pays comme la Russie ou la Chine, allant vers une restriction accrue de la liberté d'expression sur Internet, souhaitent se démarquer de la mouvance occidentale de protection des droits et libertés des Internautes et peuvent se diriger vers des « Internets nationaux ». Leur objectif : contrôler les contenants (infrastructures), les contenus (données, correspondances, etc.) et rendre leurs systèmes « étanches » au reste du réseau mondial. La multiplication de ces initiatives participe à l'émergence de frontières d'ordre technique dans le cyberespace[38].

1.3.1.2 L'apparition de frontières juridiques

La volonté des Etats de soumettre leurs données à leurs propres régimes juridiques entraine l'apparition de nouvelles frontières au sein du cyberespace. Ces données qui, dans le modèle européen, ne peuvent être exportées sans que le pays d'accueil ne respecte une série de critères sont alors confinées dans une juridiction déterminée.

La juridiction semble être l'un des éléments principaux rattachant Internet au territoire géographique. En effet, la localisation des infrastructures physiques ou de l'utilisateur Internet peut déterminer une juridiction susceptible de régler les différends naissant sur Internet. La prédétermination de cette juridiction et de la loi applicable d'un point de vue contractuel soumet le cyberespace à des frontières de nature juridique.

Ces frontières juridiques peuvent avoir des répercussions plus concrètes, à l'image de la législation luxembourgeoise qui, en interdisant l'exportation des données hors de leur pays, créent des Clouds souverains « de fait ».

1.3.2 Les défis restant à relever pour la gouvernance Internet

1.3.2.1 L'Object Naming service, le DNS de l'Internet des Objets

Aujourd'hui, l'interface historique d'accès à Internet, le fameux couple clavier/écran, laisse petit à petit place au l'émergence du tactile. Les moteurs de recherche deviennent de plus en plus pertinents. De plus en plus d'applications utilisent la technologie dite d'identification par radiofréquence ou RFID (passeport biométrique, Pass Navigo…). La quantité d'objets connectés augmente de façon

[38] Voir la volonté de l'Iran de développer son propre Internet national (http://online.wsj.com/article/SB10001424052748704889404576277391449002016.html).

exponentielle (téléphones portables, tablettes numériques, voitures, télévisions…) et certains objets communiquant se font progressivement une place sur le marché. Mais surtout, Internet s'étend au monde réel par un mécanisme de superposition, avec des procédés tels que la réalité augmentée ou encore grâce à l'utilisation de codes QR (imprimés sur des affiches de publicité, etc.) dont la simple lecture à partir d'un téléphone portable déclenche l'ouverture d'un site web sur celui-ci. Toutes ces évolutions conduisent au développement de l'Internet des objets, qui consiste en l'extension d'Internet aux objets de la vie quotidienne[39].

La place grandissante qu'est en train de prendre Internet dans la vie quotidienne entrainera la transposition des rapports de force sur ces nouveaux enjeux, mais aussi l'émergence de nouvelles vulnérabilités. Et, par conséquent, la volonté des Etats de tenter d'en maîtriser les données essentielles se traduira, par exemple, par l'obligation de conservation de données de connexion de ces objets connectés à Internet, mais aussi par la volonté de sécuriser ces objets et d'intégrer cet aspect aux futures stratégies de cybersécurité étatiques.

La gestion de cet Internet des Objets entrainera également un renouveau de la gouvernance Internet. En effet, si la gouvernance Internet est aujourd'hui centrée sur le DNS, l'internet des objets déplacera son centre de gravité vers un Object Naming Service, ou ONS[40]. Cet ONS concentrera des enjeux majeurs, car omniprésent tant dans le secteur industriel que dans l'usage des objets au quotidien. Cet ONS placera également la question de la gestion des données personnelles et du respect de la vie privée au cœur des débats, puisque de nombreuses données seront collectées au quotidien pour son bon fonctionnement. Cette problématique est clairement identifiée par l'Europe dans sa nouvelle stratégie de gouvernance Internet[41].

1.3.2.2 Le passage d'IPv4 à IPv6

L'intégration de la version 6 du protocole Internet est un véritable défi pour les instances de gouvernance Internet, surtout pour l'ICANN, qui aura bientôt épuisé l'espace d'adressage IPv4 (cet épuisement était prévu pour 2011)[42]. Face à cette pénurie d'adresses IP, de véritables places de marché se créent et proposent la vente d'espace d'adressage encore disponible. Ne s'agirait-il pas d'une « ressource commune à protéger »[43] dans le cadre de la gouvernance Internet ?

La sécurisation des réseaux : vers l'intégration de la sécurité au cœur du système.

Conçu pour sécuriser les données envoyées par le DNS, le protocole DNSSEC (« Domain Name System Security Extensions ») standardisé par l'IETF[44] pourrait résoudre nombre de problèmes de sécurité inhérents au protocole DNS. L'intégration d'IPv6 aurait également pour effet d'améliorer la sécurité des échanges sur Internet.

---

[39] Comme le définit Eric BESSON dans son discours d'ouverture de la réunion ministérielle sur l'Internet du futur (6 octobre 2008), http://www.sig.premier-ministre.gouv.fr/pm_article.php3?id_article=61284

[40] http://david.fayon.free.fr/interview/bernard-benhamou.htm

[41] Voir ligne d'action III, paragraphe « e »
https://wcd.coe.int/ViewDoc.jsp?Ref=CM(2011)175&Language=lanFrench&Ver=final&Site=COE&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

[42] http://www.itu.int/itunews/manager/display.asp?lang=fr&year=2009&issue=03&ipage=13&ext=html

[43] http://cidris-news.blogspot.fr/2012/02/ip-vendre.html

[44] Internet Engineering Task Force : groupe de travail informel - de dimension internationale - qui participe au développement de standards pour le monde de l'Internet.

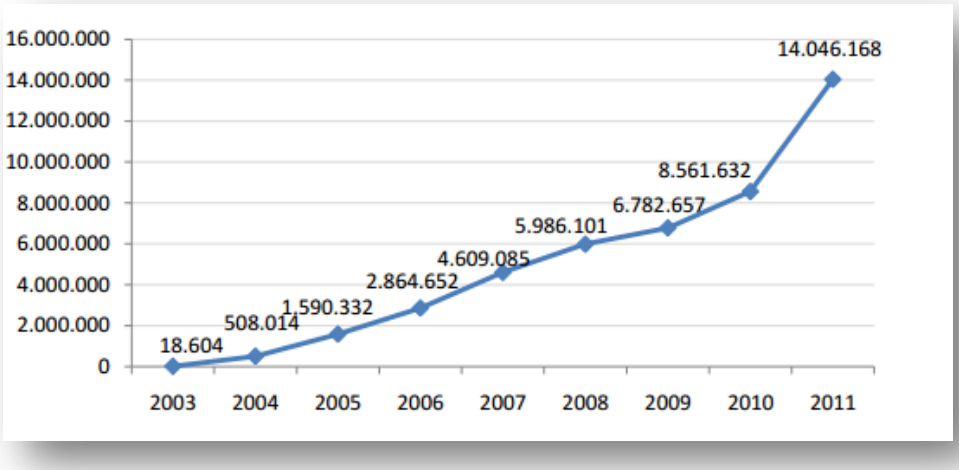
2 Fiche pays : la Turquie

2.1 Infrastructures

2.1.1 La croissance exponentielle du réseau turc

Depuis 10 ans, le réseau Internet turc est en plein croissance. Selon les chiffres publiés par l'Agence Nationale des Technologies d'Informatique et de Communication (ci-après BTK), la Turquie dispose de 14, 11 millions d'abonnés à Internet, dont 14,02 millions bénéficient d'une connexion haut débit ; soit un **taux de pénétration du haut débit par foyer de 39 %**, alors que la moyenne de l'Union Européenne s'élève à 48 %.[45]

Evolution du nombre d'abonnés au haut débit en Turquie



[46]

Source : rapport trimestriel de BTK pour le 4ème trimestre de l'année 2011, page 29

Entre 2003 et 2011, le nombre d'abonnés au haut débit a augmenté de 755 %, passant de 18 604 à plus de 14 millions d'abonnés.

Fin 2011, la Turquie comptait 6,4 millions d'abonnés l'Internet mobile haut débit[47], dont 4,9 millions sont des utilisateurs de *smartphones*. Fin 2010, ils n'étaient que 1,4 millions d'utilisateurs, soit une augmentation annuelle de 345,8 %.[48]

Par ailleurs, le nombre global d'utilisateurs Internet (toutes types de connexions confondues) entre le 4ème trimestre de l'année 2010 et fin 2011 a augmenté de 62,8 %.[49]

---

[45] Voir le rapport annuel de BTK de 2010 http://www.btk.gov.tr/kutuphane_ve_veribankasi/raporlar/faaliyet_raporlari/fr2010tr.pdf

[46] http://www.btk.gov.tr/kutuphane_ve_veribankasi/pazar_verileri/ucaylik11_4.pdf

[47] Connexion mobile haut débit : Une connexion qui utilise des standards équivalents ou supérieurs au 3G.

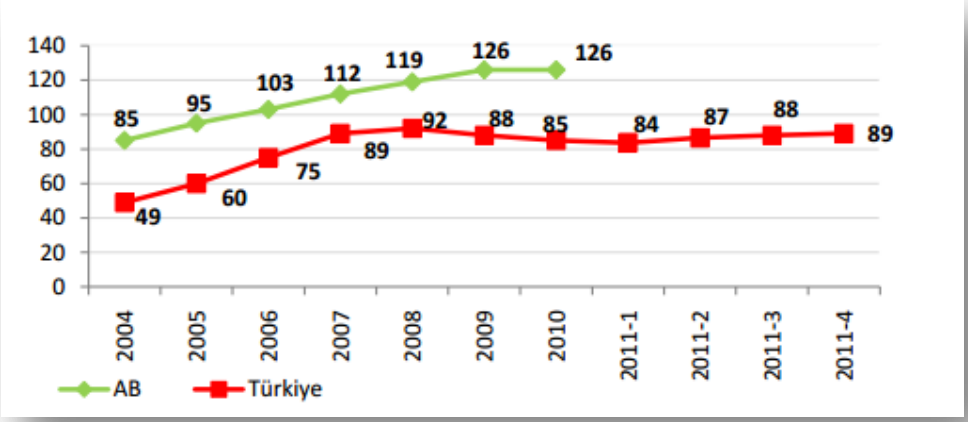
[48] Voir le rapport trimestriel de BTK pour le 4ème trimestre de l'année 2011, page 30
http://www.btk.gov.tr/kutuphane_ve_veribankasi/pazar_verileri/ucaylik11_4.pdf

[49] Idem 4

2.1.2 *Un taux de pénétration de téléphonie mobile important*

Selon les derniers chiffres publiés par le BTK, 65 millions d'abonnements sont enregistrés chez les opérateurs de téléphonie mobile et le taux de pénétration de la téléphonie mobile est estimé à 88,6 %. [50]

Evolution du taux de pénétration de téléphonie mobile



Source : Le rapport trimestriel de BTK pour le 4ème trimestre de l'année 2011, page 44 [51]

Depuis juillet 2009, la Turquie dispose des infrastructures nécessaires à la connexion 3G. Le nombre de téléphones compatibles avec la technologie 3G, 3G+ et 4G est estimé à près de 31 millions.[52]

Trois opérateurs de télécommunication mobile dominent le marché turc : le *leader TURKCELL* (52 % de part de marché), suivi de *VODAFONE* (28 %) et d'AVEA (20 %).[53]

2.1.3 *Le prix moyen de la connexion à Internet*

Le prix moyen de la connexion Internet dans un cybercafé est estimé à 5 *lira*, équivalent de 2,20 euros. Le prix d'abonnement mensuel à l'ADSL moyen en Turquie est de 59 *lira*, soit 26 euros[54].

2.1.4 *Etat des lieux de la connectivité*

La connexion au reste du monde est assurée par deux satellites actifs détenus par l'entreprise publique *TÜRKSAT*[55] et par cinq câbles sous-marins[56]. Ces câbles ont pour points d'entrée les villes suivantes :

---

[50] Pour une population totale de 73 722 988 personnes.

[51] http://www.btk.gov.tr/kutuphane_ve_veribankasi/pazar_verileri/ucaylik11_4.pdf

[52] Voir le rapport trimestriel de BTK pour le 4ème trimestre de l'année 2011, page 30 http://www.btk.gov.tr/kutuphane_ve_veribankasi/pazar_verileri/ucaylik11_4.pdf

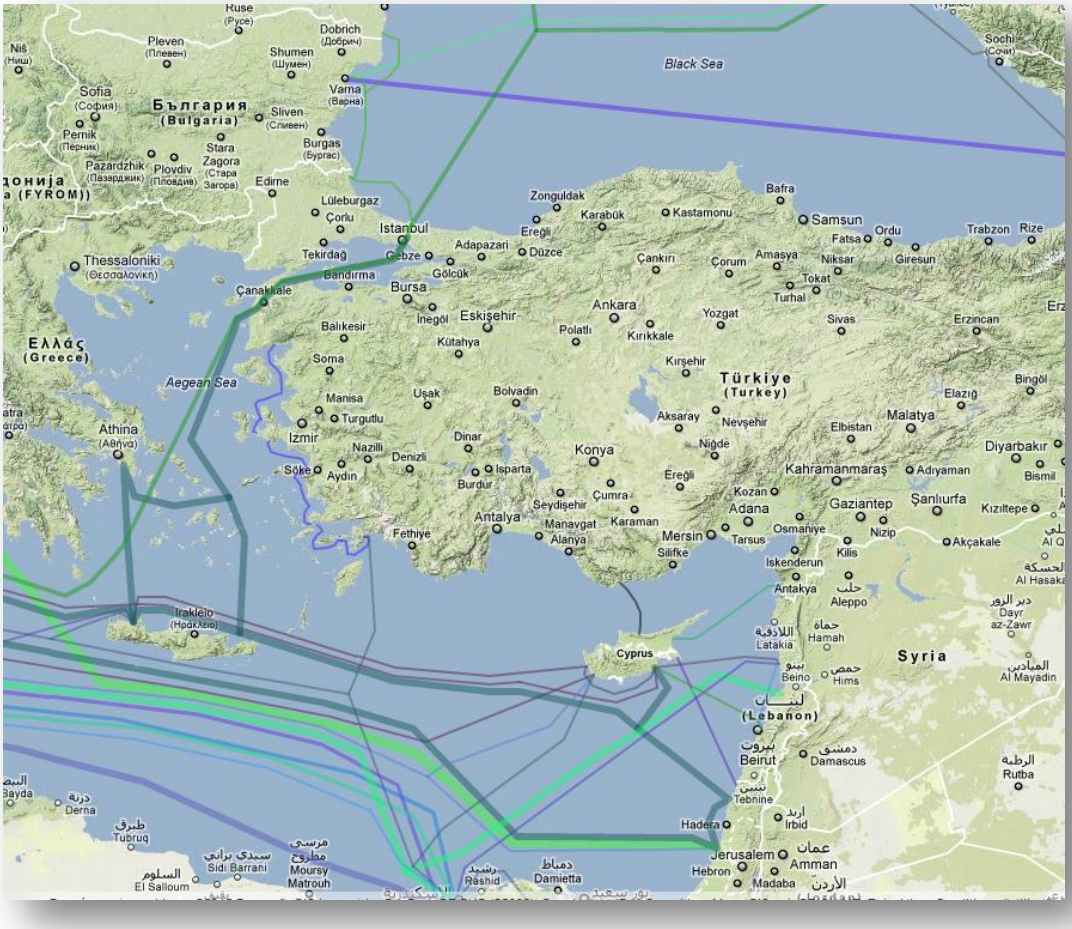
[53] http://www.btk.gov.tr/kutuphane_ve_veribankasi/pazar_verileri/ucaylik11_4.pdf page 50

[54] 80% des abonnés utilisent le tarif illimité avec une vitesse de connexion de 8 Mbits/s. Voir le rapport annuel de BTK pour le 4ème trimestre de l'année 2011, page 34 http://www.btk.gov.tr/kutuphane_ve_veribankasi/pazar_verileri/ucaylik11_4.pdf

[55] Türksat 2A et Türksat 3A http://uydu.turksat.com.tr/uydu-filosu

- Boyazi (via le câble TURCYOS-1) ;
- Samadag (via le câble TURCYOS-2) ;
- Ciftlikkoy, Kucukkuyu, Nergis et Turgutreis (via le câble TURMEOS-1) ;
- Turunc (via le cable SEA-ME-WE 3[57] ou South-East Asia - Middle East - Western Europe) ;
- Istanbul (via les deux câbles MedNautilus[58] et Itur[59]).

Les câbles sous-marins reliant la Turquie à Internet



[56] http://www.iscpc.org/ International Cable Protection Commitee
[57] http://www.smw3.com/

[58] http://www.mednautilus.com/map.asp

[59] http://en.wikipedia.org/wiki/ITUR

Source : cablemap.info

La Turquie dispose de deux points d'échanges internet (IXP) dont l'un est désormais inactif. Le seul point d'échange en fonction, l'*IST-IX* est administré par *TERREMARK WORLDWIDE*. On dénombre par ailleurs trois répliques Domain Name System, ou DNS sur le territoire turc, dont deux à Ankara (I, L) et une à Istanbul (L). [60]

2.1.5 Nombre de datacenters et autonomous systems[61]

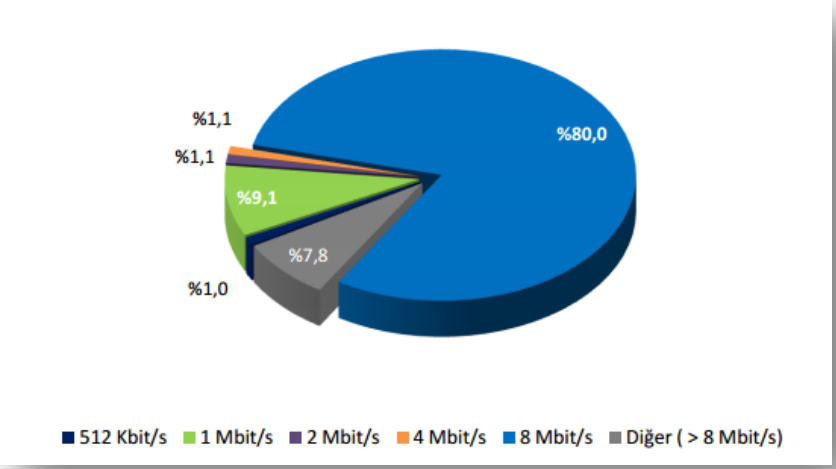
La Turquie possède 20 *datacenters* dont 13 à Istanbul, 3 à Ankara, 2 à Bursa, 1 à Trabzon et 1 à Denizli.[62] Il est estimé qu'un *datacenter* répond aux besoins de 375 000 habitants.

La Turquie possède 197 *autonomous systems* [63] établis sur le territoire, pour une population d'environ 74 000 000 habitants.

2.1.6 La bande passante

Selon les publications de la Banque Mondiale, la bande passante du pays, mesurée en 2008, s'élève à 206 504 Mbps.[64]

Représentation de la topographie de la vitesse de connexion en Turquie



Source : rapport trimestriel de BTK pour le 4ème trimestre de l'année 2011, page 34 [65]

80 % des utilisateurs sont dotés d'une connexion Internet de 8 Mbit/s. Le passage de 1 Mbit/s à 8 Mbit/s s'étant accéléré, la part d'utilisateurs de connexions de 1 Mbit/s est en déclin depuis des

[60] http://www.root-servers.org/
[61] Un Autonomous System, AS, ou Système Autonome, est un ensemble de réseaux informatiques IP intégrés à Internet et dont la politique de routage interne (routes à choisir en priorité, filtrage des annonces) est cohérente. Un AS est généralement sous le contrôle d'une entité unique, typiquement un fournisseur d'accès à Internet.
[62] http://www.datacentermap.com/turkey/
[63] http://as-rank.caida.org/
[64] http://www.tradingeconomics.com/turkey/international-internet-bandwidth-mbps-wb-data.html
[65] http://www.btk.gov.tr/kutuphane_ve_veribankasi/pazar_verileri/ucaylik11_4.pdf

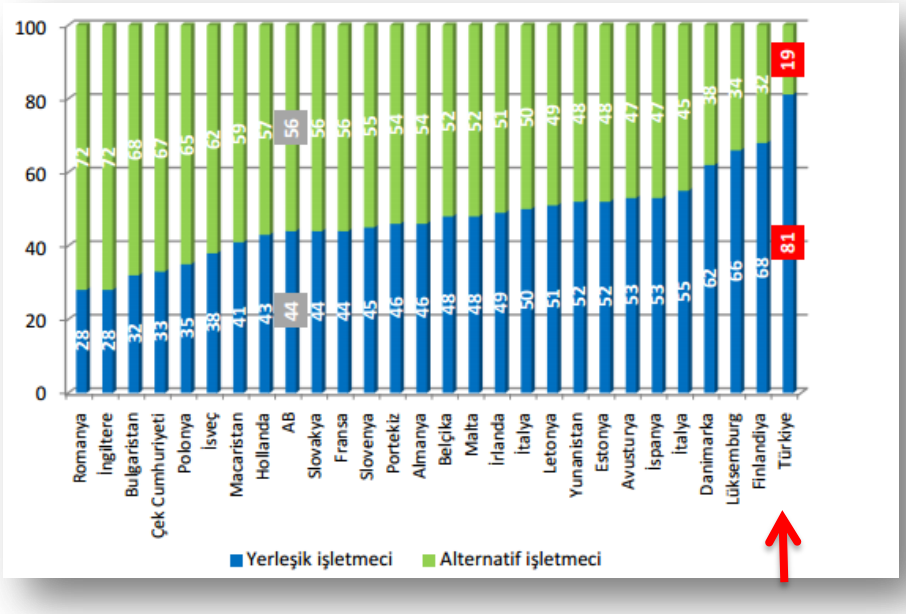
années. Par ailleurs, le nombre d'utilisateurs dotés d'une vitesse supérieure à 8 Mbit/s est estimé à 8 %.

2.1.7 Nombre de Fournisseurs d'Accès à Internet

La Turquie compte aujourd'hui environ 70 fournisseurs d'accès à Internet (FAI) dont le *leader* est *TTNET*, la branche Internet de *Türk Telekom*, l'ancien titulaire du monopole public. La totalité du trafic internet passe par les infrastructures de *Türk Telekom*, les autres FAI fonctionnant sur le réseau de *Türk Telekom* grâce à un système de *leasing*.

TTNET détient désormais 85,84 % du marché. *Superonline*, la branche Internet du plus grand opérateur turque de téléphonie mobile - *TURKCELL*, se place en deuxième position avec 5,60 % de part de marché. Depuis la libéralisation du marché, la part de *TTNET* ne cesse de diminuer, mais elle conserve toujours son rang de *leader* loin devant *Superonline*.

La distribution du capital des FAI des divers pays du monde



Source : Le rapport trimestriel de BTK pour le 4ème trimestre de l'année 2011, page 38[66]

Selon le graphique ci-dessus, malgré la libéralisation des marchés, la part du **capital étranger** dans les entreprises de FAI reste minoritaire avec un taux de 19%. La moyenne européenne dans la même catégorie est estimée à 56%.

2.1.8 Nombre de noms de domaines

Des statistiques datant du 8 mars 2012 montrent que le gTLD[67] turc (.tr) héberge 290 146 noms de domaines.[68]

---

[66] http://www.btk.gov.tr/kutuphane_ve_veribankasi/pazar_verileri/ucaylik11_4.pdf

[67] Generic Top Level Domain, le gTLD turc est .tr

[68] https://www.nic.tr/index.php?USRACTN=STATISTICS&PHPSESSID=133113371580128020390583 6

Le gTLD le plus répandu est « com.tr », suivi de « gen.tr ». Si le gTLD « .com » est très populaire en Turquie, il est impossible de connaître le nombre exact des « .com » turcs. Par ailleurs, le prix d'achat important des *gTLD* turcs, durant les années de la propagation de l'internet dans le pays, a incité des utilisateurs à acheter des gTLD des autres pays.

2.2 Capacités scientifiques et techniques

La Turquie investit largement dans la R&D en matière de nouvelles technologies. Son objectif : rattraper son retard en la matière.

2.2.1 Une main d'œuvre jeune et qualifiée

La structure de la population turque offre un potentiel important de main d'œuvre dans le domaine des TIC. L'âge médian de la population étant de 28,5 ans, 51 % des habitants ont moins de 25 ans et 26 % des habitants se situent dans la tranche d'âge allant de 0 à 14 ans. La population, jeune et dynamique, est donc capable de s'adapter aux nouveautés technologiques.[69] Une affirmation appuyée par l'analyse des profils des ingénieurs informatiques turcs.

Selon la Chambre des Ingénieurs Informatiques Turques (ci-après *BMO*), plus de 30 000 ingénieurs ont fait leur entrée dans le marché du travail depuis 1981. Désormais, les ingénieurs ayant moins de 25 ans représentent 16 % du nombre total d'ingénieurs présents sur le marché, tandis que la part des 25-29 ans et celle des 30-34 ans sont respectivement de 47 % et 22 %.

Ces chiffres seront bientôt revus à la hausse puisque, désormais, les universités turques disposent de 85 formations dans le domaine des TIC (Ingénierie informatique, Ingénierie des systèmes d'information et Ingénierie de logiciels). Surtout, le nombre des nouveaux étudiants inscrits chaque année dans le domaine ne cesse de croître. Cette année, 7479 étudiants se lançaient dans une formation liée aux TIC.

La majorité des diplômés de ces filières se sont ensuite dirigés vers le développement informatique (codes…). Seuls 16 % des diplômés travaillent dans le domaine de cybersécurité.[70]

La Turquie se situe en 12ème place à l'échelle mondiale en matière de main d'œuvre dédiée aux TIC avec un score de 7,032/10. En matière de qualification des ingénieurs informatiques turcs, le pays a obtenu un score de 7,387/10, ce qui place le pays en 13ème position derrière les Etats-Unis et Taiwan.[71]

Le pays a mis en place un projet d'informatisation de l'enseignement public (dit « Projet de FATIH »). Ce projet consiste à distribuer des tablettes tactiles gratuites aux étudiants. Ces tablettes seront dotées d'une connexion Internet et d'un accès illimité aux livres numériques. La tablette sera compatible avec des tableaux électroniques interactifs installés dans les salles d'études. Les étudiants n'utiliseront plus des livres, des cahiers et s'habitueront à travailler dans l'espace numérique connecté.[72]

[69] CIA World Factbook

[70] Le Rapport Annuel de BMO http://www.bmo.org.tr/wp-content/uploads/2011/08/AnketSonucRaporuv2.pdf

[71] World Competitiveness Yearbook, International Institute for management Development, Lausanne Switzerland

[72] http://fatihprojesi.meb.gov.tr/tr/index.php

2.2.2 La Turquie possède plusieurs formations d'excellence

Selon les dernières statistiques du *Times Higher Education Ranking List,* la *Middle Eastern Technical University* (ci-après METU) fait partie de 100 meilleures universités du monde.[73] De son côté, la *Bilkent University* se classe parmi les 200 meilleures universités mondiales en matière de nouvelles technologies.[74]

De nombreux projets de recherche sont conduits et encouragés grâce à la collaboration de l'Organisme National de Recherche Scientifique et Technologique (ci-après *TÜBITAK*), de l'Union Européenne et des universités locales. Plusieurs instituts privés ont également vu le jour depuis début des années 2000 et la part des entités privées dans le secteur des TIC est en croissance depuis la libéralisation et l'ouverture du pays.

2.2.3 Un financement assuré par le secteur privé

Selon les chiffres annoncés par l'Institut National des Statistiques (*TURKSTAT*), le financement des dépenses en matière de recherche et développement est assuré à 45,1 % par le secteur privé, à 30,8 % par le secteur public et à 20 % par les universités.[75] Des chiffres qui traduisent l'engagement du secteur privé au sein de la R&D turque, canalisée par la voie des universités.

En revanche, la part des financements étrangers reste très faible (seulement 1%). La Turquie semble, de ce point de vue, être un pays peu attractif dans le domaine des TIC.

2.3 Base industrielle et technologique

2.3.1 Un marché dominé par les PME

La base industrielle turque dans le domaine informatique demeure relativement faible. Le marché, composé à 96% de PME, est dominé par les micro-entreprises (52 % du marché) et les petites entreprises de 10 à 50 salariés (36% de part de marché). Les entreprises de taille moyenne constituent 10 % du marché et la part des grandes entreprises de plus de 250 salariés ne représentent que 4 %[76].

Les startups peinent à se développer et à embaucher. Selon les estimations de Chambre de l'industrie des logiciels, le secteur ne satisferait que 30% de ses besoins réels en matière de main d'œuvre.

35 % des entreprises se sont installées dans des « Zones de Développement Technologiques »[77]. Le pays compte 43 de ces zones qui ont été créées par un partenariat université /entreprise financé par l'Etat. Objectif : créer de véritables incubateurs afin de concevoir des produits commercialisables bénéficiant d'une forte valeur ajoutée, tout en contribuant à la recherche et développement.

---

[73] 96ème place en 2012 http://www.timeshighereducation.co.uk/world-university-rankings/2011-2012/reputation-rankings.html

[74] Times Higher Education World University Rankings 2010 (ODTU=183ème place, Bilkent 112ème)

[75] Idem 28

[76] Voir la librairie de *TÜBİTAK : http://www.tubitak.gov.tr/*

[77] *TEKNOPARK*

2.3.2 La taille et la structure du marché

Le revenu total généré par le marché des TIC en 2011 est de 31 milliards de dollars. Ce qui représente une croissance de 25,1 % par rapport à l'année 2009 et de 8,8 % par rapport à 2010.[78]

Le marché est structuré en 2 segments : les technologies de l'information (ci-après TI) et les télécommunications. Le segment de la télécommunication couvre 73 % du marché des TIC, et celui des TI, 27 %.

Le chiffre d'affaires de **l'industrie du *hardware*** calculé pour l'année 2011 est estimé à 6,7 milliards de dollars, ce qui représente 22 % du marché global et 72 % du marché des TI. Contrairement à la moyenne mondiale (39 % en 2010), la part de l'industrie turque de *hardware* reste largement majoritaire dans le secteur des TI.[79]

Le chiffre d'affaires de **l'industrie du *software*** pour l'année 2011 est estimé à 2,6 milliards de dollars. Ce secteur est en pleine expansion, avec une croissance d'environ 8 % par an.[80] Il compte près de 1600 entreprises. 87.2 % d'entre elles sont des PME. Parmi ces 1600 sociétés, quelques 100 entreprises exportatrices travaillent avec 50 pays sur 12 zones franches. Leurs exportations s'élèvent à 250 millions de dollars.

D'après les estimations de la banque mondiale, **les importations de biens liés aux TIC** représentent environ 6 % des importations globales. Ce chiffre a atteint un record historique de 12 % en 1999, et est depuis en baisse constante.[81] Les **exportations de biens liés aux TIC** sont quant à elles estimées à 3 % des exportations globales.[82] L'exportation des services liés aux TIC représente enfin 550 millions de dollars, avec une part d'environ 2,1% des exportations globales.[83]

Parmi les **grandes entreprises** dans le domaine des TIC, TURKCELL se démarque avec sa position de *leader* en télécommunications. L'entreprise est présente dans dix pays et est cotée au NASDAQ. Le marché du *hardware* est de son côté dominé par les entreprises INDEKS et ARENA. En matière de sécurité informatique, mises à part quelques entreprises de recherche et développement[84] , le pays est largement dépendant des prestataires étrangers tels qu'IBM, Microsoft, HP ou Kaspersky.

La Turquie est membre de **l'Organisation Internationale de Normalisation**[85] et est présente dans 361 comités techniques.[86]

---

[78] CA total 2009 : 24 570 000 $, CA total 2010 : 28 568 000 $

[79] http://www.interpro.com.tr/?page_id=92

[80] Idem 35

[81] http://www.tradingeconomics.com/turkey/ict-goods-imports-percent-total-goods-imports-wb-data.html

[82] http://www.tradingeconomics.com/turkey/ict-goods-exports-percent-of-total-goods-exports-wb-data.html

[83] http://www.tradingeconomics.com/turkey/ict-service-exports-percent-of-service-exports-bop-wb-data.html

[84] http://signalsec.com/index.php

[85] *ISO*

[86] http://www.iso.org/iso/fr/about/iso_members/iso_member_participation_tc.htm?member_id=2168

2.4 Sécurité et gouvernance des réseaux

2.4.1 Ecosystème cybercriminel et hacktiviste

Comme la plupart des pays émergents ayant développé leur connectivité, la Turquie est fortement exposée aux risques informatiques, les menaces provenant de groupes de *hackers* tel qu'*Anonymous,* et de des groupes locaux empreints de revendications politiques comme *Redhack* (communistes) ou encore *Ayyıldız Tim* (nationalistes).

Carte globale des virus

Source : McAfee [87]

Légende : nombre d'ordinateurs infectés pour un million d'habitant

Selon les estimations de *McAfee,* le pays dénombre plus d'un millier d'ordinateurs infectés pour 1 million d'habitants.

D'après l'étude annuelle de *Kaspersky Lab.,* le *Kaspersky Security Bulletin 2011,* la Turquie se trouve en 18ème position avec 3,1 millions d'attaques vers le reste du monde. Selon la même étude, environ 9 millions d'utilisateurs turcs auraient été visés par des cyberattaques au cours de l'année 2011.[88] Par ailleurs, selon l'étude de *Symantec* sur la sécurité internet pour l'année 2009, le pays se trouvait en 3ème

[87] http://home.mcafee.com/VirusInfo/VirusMap.aspx

[88] http://www.securelist.com/en/analysis/204792216/Kaspersky_Security_Bulletin_Statistics_2011

rang des pays émettant du spam, ceci en raison du nombre important des réseaux « *zombie* » sur son territoire.[89]

En août 2011, des *hackers* ont été arrêtés pour « chantage ». Ils avaient réussi à s'emparer de 400 000 ordinateurs « *zombies* » et les avaient utilisés pour s'attaquer aux sites qui refusaient de payer une rançon. Grâce à ce mode opératoire, les *hackers* auraient collecté 5 millions de *lira*, soit 2,2 millions d'euros.[90]

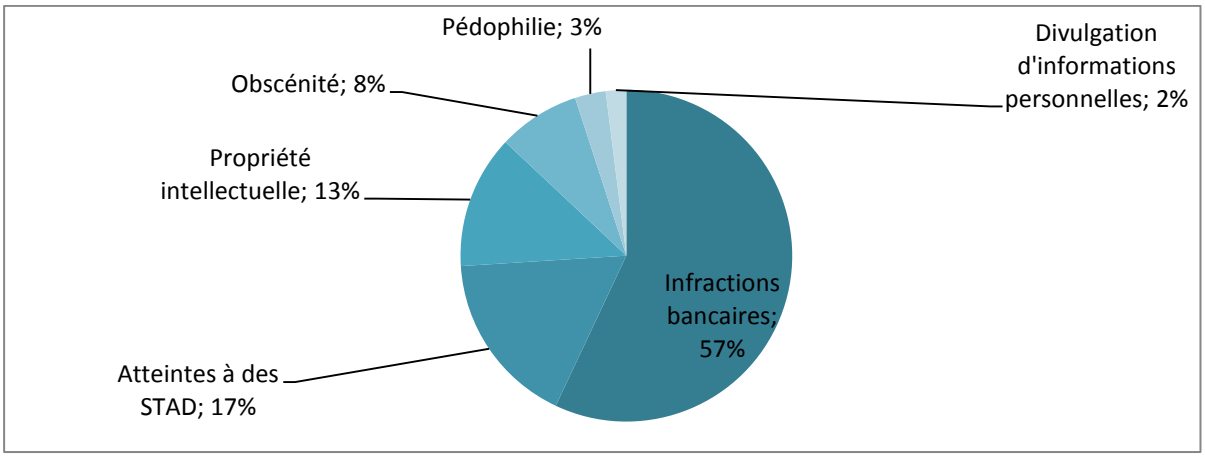
Selon le *Microsoft Security intelligence Report 2011*[91], le taux d'ordinateurs infectés serait en baisse depuis 2009, ce en raison de l'amélioration du niveau de protection des utilisateurs turcs. Ce taux estimé à environ 55 % pour l'année 2009, avoisine aujourd'hui les30 %, inscrivant la Turquie parmi les pays à risque modéré dans le classement mondial.

Une étude intitulée « les cybercrimes en Turquie 1990-2011», présente les résultats suivants (voir schéma ci-contre).[92]

Sur la totalité des actes cybercriminels présentés devant les tribunaux turcs de 1990 à 2011 :

- 57 % de ces actes étaient des piratages de cartes bancaires et des opérations bancaires en lignes.
- 17 % étaient des piratages contre les systèmes d'information.
- 13% concernaient la violation des droits de propriété intellectuelle.

Le reste des délits concernaient « l'obscénité » (8 %), la pédophilie (3%) et la « divulgation d'informations personnelles » (2 %).



La transposition des tensions relatives au génocide arménien dans le cyberespace

[89] Symantec Global Internet Security Threat Report Trends for 2008, Volume XIV, Nisan 2009
[90] http://www.hurriyet.com.tr/gundem/18473643.asp
[91] http://download.microsoft.com/download/1/A/7/1A76A73B-6C5B-41CF-9E8C-33F7709B870F/Microsoft_Security_Intelligence_Report_Special_Edition_10_Year_Review.pdf
[92] http://www.slideshare.net/melihbayramdede/trkiyenin-siber-su-haritas-19902011

Suite à l'adoption d'un texte de loi français réprimant la négation des génocides, dont celui des Arméniens, le site de la députée à l'origine de la loi, Valérie Boyer, a été piraté par des militants pro-Turquie. Un message anonyme à forte connotation politique a été laissé, en turc et en anglais, s'attaquant à la communauté arménienne de France et au gouvernement. L'attaque a été revendiquée par le groupe d'hacktivistes *Akıncılar*.

La décision gouvernementale d'établir des mesures de filtrage d'internet à des fins de protection des mineurs[93] a suscité de vives réactions de la part de plusieurs groupes de *hackers* déterminés à lutter contre « la censure» et à défendre la liberté d'accès à l'information sur l'Internet turc.

La branche turque de l'*Anonymous*, *AnonymousTR* et *Redhack* (les *hackers* rouges, communistes) se sont illustrés dans cette vague de protestation. Ils ont notamment tenté de prendre le contrôle des systèmes de plusieurs entités gouvernementales. La base de données de la « Haute préfecture de la police » a été piratée par *Redhack* et l'intégralité de son contenu a été publiée sur *Anatoleaks*[94]. La branche turque d'*Anonymous* a également lancé une opération contre les serveurs de « l'Agence Nationale des Technologies d'Informatique et de Communication »[95]. Le contenu a ensuite été publié sur Internet afin de protester contre l'interdiction de l'accès à *blogger.com*[96]. Ces *hackers* s'opposent à d'autres groupes, cette fois-ci nationalistes comme *Ayyıldız Tim* ou islamistes comme *Akıncılar* (le groupe qui a revendiqué le piratage du site internet de Charlie Hebdo suite à leur numéro spécial "Charia Hebdo" consacré au prophète Mahomet [97]). Ces derniers, à tendance patriotique, ont pris position contre les *hackers* anarchistes et communistes en ciblant par exemple le site des Anonymous[98] et des divers groupes hacktivistes qu'ils considèrent comme étant des «ennemis du pays ».

2.4.2 Le cadre juridique de la lutte contre la cybercriminalité

2.4.2.1 Les textes

Le processus d'adhésion de la Turquie dans l'Union Européenne et l'obtention du statut officiel du « candidat » a entrainé des transformations importantes du système judiciaire turc. Dans ce contexte, la Turquie a effectué plusieurs réformes en matière de régulation des délits informatiques et de la sécurité sur Internet.

La première loi sur le sujet a été rédigée en 1990. Cette loi faisait référence à des « crimes effectués en utilisant un ordinateur ». Depuis la grande réforme du code pénal turc de 2004, la loi a instauré la notion de « crimes concernant le domaine informatique » et fait directement référence au « système informatique ». Cette appellation englobe tout système informatique ainsi que les outils capables de stocker, traiter, transformer, utiliser et transférer des données. Une définition qui se rapproche du STAD (système de traitement automatisé de données) à la française.

---

[93] http://www.guvenlinet.org/gb/menu/14-The_contents_of_profiles.html
[94] http://anatoleaks.blogspot.com/ (en allusion à *Wikileaks*).
[95] *BTK*
[96] (Opération *DIGITURK*) http://www.ntvmsnbc.com/id/25322201/
[97] http://www.lemonde.fr/actualite-medias/article/2011/11/02/charlie-hebdo-victime-d-une-cyberattaque-turque_1597650_3236.html
[98] http://www.anonnews.org

Les infractions listées dans la loi sont regroupées sous les grands titres suivants :

- Les délits contre les systèmes d'information,
- Les délits concernant la propriété intellectuelle,
- Les délits contre l'ordre et la sécurité nationale,
- Les délits liés à l'e-commerce et aux opérations bancaires en ligne,
- Les délits contre la liberté de communication et la vie privée.[99]

Un projet de loi a également pour ambition de créer un « Droit Informatique » destiné à couvrir tous les délits liés à l'espace virtuel.[100]

Le pays est enfin signataire de la Convention sur la cybercriminalité (Convention de Budapest) depuis le 10 novembre 2011, mais la ratification de la convention par l'Assemblée Nationale a été retardée suite à des problèmes d'interprétation des annexes relatives aux délits liés au racisme et à la xénophobie.[101]

2.4.2.2 L'application de la loi est assurée par deux entités séparées au sein de la police.

Les attaques contre les systèmes d'information, l'infiltration et l'obtention illégale de données, ainsi que les délits liés à l'e-commerce et aux opérations bancaires en ligne relèvent de la Brigade Spéciale d'Informatique de la Préfecture de police.

Tous les autres délits réalisés par ou sur Internet et qui sont contraires à l'ordre public et à la sécurité publique, sont de la compétence de la police criminelle.

2.4.2.3 La gouvernance d'Internet en Turquie

Depuis le 22 août 2011, un système de filtrage généralisé a été mis en place à l'initiative du gouvernement turc afin d'optimiser la sécurité sur Internet et d'assurer la protection des mineurs. Cette initiative du gouvernement exige des utilisateurs qu'ils choisissent un profil d'accès à internet (profil standard, profil familial ou profil enfant), l'accès à certains sites étant restreint selon le profil choisi.[102]

La gouvernance de l'Internet en Turquie relève de la compétence du Ministère de la Communication et du Transport. Au sein du ministère, quatre entités travaillent de concert afin d'assurer la bonne gouvernance des systèmes de communication et d'internet.

- « Le Comité d'Internet » est chargé de suivre l'innovation et le progrès sur Internet, de donner des conseils et de soumettre des projets innovants au ministère.
- « L'Agence Nationale des Technologies d'Informatique et de Communication » (*BTK*) a pour mission d'accorder des licences aux fournisseurs d'accès à internet. Elle assure également le contrôle de la qualité des prestations fournies. Grâce au projet d'anti-spam de *BTK* [103], le pays a réussi à

[99] http://www.tbb.org.tr/Dosyalar/Yayinlar/.../BILISIM_HUKUKU.pdf

[100] http://ekonomi.haberturk.com/teknoloji/haber/712862-siber-tehdit-artik-nukleerden-de-buyuk

[101] Surtout des crimes concernant le mépris des génocides.

[102] Idem 46

[103] http://www.cybersecurity.gov.tr/projects/antispamsms.html

diminuer la quantité d'IP génératrices de spam de 99% et la Turquie ne fait plus partie du « top 10 » des pays à l'origine de pollupostage.

- « Le Comité des Affaires de Télécommunication » (*TIB)* est la seule entité administrative turque ayant une compétence exclusive sur la localisation des signaux téléphoniques, sur le constat, la vérification, l'enregistrement du contenu des échanges effectués via les réseaux de télécommunication.
- Enfin, « le Haut Comité de Radio et Télévision » du Ministère assure un contrôle sur les émissions publiées sur Internet.

L'APSIT[104], ou association des professionnels de la sécurité de l'information de Tunisie, équivalent du CLUSIF français, participe également à la diffusion et la généralisation de la culture de sécurité informatique dans les entreprises.

Pour mieux réagir aux attaques informatiques, le pays dispose d'un CERT (Tr-CERT)[105] et d'un CSIRT (ULAK-CSIRT)[106] qui travaillent tous deux sous la supervision de *TÜBITAK*.

Le Plan Stratégique National 2006-2011 a mis l'accent sur l'identification des « infrastructures critiques ». Selon ce plan, le Ministère de la Justice est compétent pour l'élaboration d'une législation concernant le développement des systèmes nationaux de sécurité informatique et la protection des informations liées la sécurité nationale dans les milieux électroniques. [107] Par ailleurs, les rapports de *BTK*, préparés sur demande du Premier Ministre, accordent une importance particulière à la « sécurité cybernétique » et préconisent l'identification des infrastructures critiques du pays, l'évaluation de leur interconnexion, de leurs niveaux de criticité et de leurs responsables afin de les protéger contre les attaques cybernétiques.[108]

Suite aux déclarations du gouvernement turc sur la question, des ONG ont créé « le Congrès National de Coordination en Cybersécurité »[109]. Cette organisation a pour objectif de réunir experts en cybersécurité, universitaires, représentants des ministères concernés par le sujet et des forces armées, ONG, industriels du secteur informatique, entreprises de télécommunication et divers groupes *hackers* (« blancs » et « noirs »). Chacun contribuera à sa façon : les *hackers* constitueront « une armée » qui sera chargée de défendre les systèmes critiques du pays dans le cas d'une attaque cybernétique, tandis que les experts et les universitaires fourniront des conseils et assisteront à la mise en place d'une stratégie dans le domaine.

Malgré les travaux pertinents effectués par les experts de *TÜBITAK* et de *BTK* sur le sujet, la Turquie reste cependant en retard sur le sujet, surtout au niveau législatif, par rapport au reste du monde.

---

[104] http://www.apsit-tunisie.org/

[105] http://www.bilgiguvenligi.gov.tr/certen/index.php

[106] http://csirt.ulakbim.gov.tr/eng/

[107] Voir le document sur http://www.bilgitoplumu.gov.tr/

[108] http://www.bilgiguvenligi.gov.tr/siber-savunma/iki-kritik-kavram-kritik-altyapilar-ve-kritik-bilgi-altyapilari.html

[109] http://www.bilgiguvenligi.org.tr/bgd.php?id=501013

2.5 Capacité de lutte informatique

2.5.1 Une nouvelle ère pour la stratégie turque

L'année 2013 devrait marquer une nouvelle ère pour la stratégie turque en matière de cybersécurité. Le Ministère de Transport et Communication devrait publier un premier plan stratégique sur la cyberdéfense. Ce plan couvrira les mesures et précautions devant être prises par les institutions gouvernementales afin d'assurer une meilleure protection contre les cyberattaques, tout en veillant à la coordination des divers institutions en cas de cyberattaque[110].

Exposée à un nombre croissant de cyberattaques, la Turquie a décidé de renforcer son système de prévention et de protection.

En tant que membre de l'OTAN, la Turquie suit la stratégie de l'organisation en matière de la cyberdéfense. Les cyberattaques sont donc considérées comme une menace importante pour la sécurité nationale. La volonté de se rapprocher de la stratégie de l'OTAN a été accentuée dans « Le Document sur la Sécurité Nationale »[111], établi par le Conseil National de Sécurité.[112] Dans ce document, les cyberattaques ont été pour la première fois reconnues officiellement. Elles sont définies comme des actions menées par un acteur, étatique ou indépendant, qui visent à pénétrer dans les ordinateurs et les réseaux d'un autre pays afin d'endommager et de perturber ses systèmes informatiques. Le Conseil a notamment mis l'accent sur la nécessité de créer des institutions compétentes en la matière et sur le développement de mesures de prévention et de protection.[113]

2.5.2 Des unités dédiées à la cyberguerre

Un projet de création d'un cyber commandement au sein des forces armées turques, qui serait similaire au *Cyber Command* américain, a été lancé au début des années 2000, mais le projet n'a pas été encore abouti. Selon les termes du projet, ce cyber commandement serait chargé de la défense de toutes les infrastructures du pays, qu'elles soient militaires ou civiles.

En outre, une « unité de base » composée de huit ingénieurs informatique formés dans le domaine par des experts a été établie sous la supervision du chef d'état-major des armées afin de faire face aux cyberattaques potentielles.[114]

2.5.3 L'Exercice national cybernétique

Afin de tester la capacité défensive du pays, un « exercice national cybernétique »[115] a été conduit en Turquie, avec la participation de 41 institutions publiques, privées et militaires en janvier 2011. L'exercice consistait à simuler des situations de crise afin d'évaluer la capacité de réponse, d'organisation et de résilience des institutions. Les résultats de l'exercice ont été peu concluants et ont illustré le retard accumulé par la Turquie en matière de cyberdéfense.

---

[110] http://www.hurriyetdailynews.com/turkeys-cyber-defense-plan-to-be-ready-in-2013.aspx?pageID=238&nid=15054

[111] Appelé le livre rouge, le document établi la stratégie de défense du pays et fait la liste des menaces potentielles à combattre pour assurer l'ordre et la sécurité nationale.

[112] Composé des chefs des états major de diverses armées, du président de la république, le premier ministre et les ministres liés.

[113] http://mobile.defensenews.com/story.php?i=7388376&c=FEA&s=SPE

[114] Idem 68

[115] http://www.cybersecurity.gov.tr/nce.html

Les systèmes informatiques des institutions sont très peu protégés, qu'il s'agisse de sites vitrines ou d'infrastructures critiques. A titre d'exemple, tous les systèmes informatiques et les sites internet des institutions participant à l'exercice de crise ont été infiltrés et maîtrisés par les attaquants, à l'exception du *BTK*, *de TÜBITAK* et des sites internet des forces armées. Notons cependant que, malgré ce résultat, les « *Anonymous* » ont réussi à s'emparer d'un sous-site internet de *BTK,* sorti grand gagnant de l'Exercice de crise national, un mois après la simulation.[116]

2.5.4 Etat des lieux de l'armement informatique turc

En ce qui concerne la conception d'armes et de produits de défense informatiques, les forces armées turques favorisent une approche de partenariat public / privé / université. La coordination entre les organismes partenaires s'effectue par l'intermédiaire du « Sous Secrétariat de l'Industrie de la Défense » (ci-après SSID).[117] Le SSID, supervisé par le ministère de la défense, est chargé de mettre en place des offres publiques d'achat dans le secteur de l'industrie de la défense et de superviser les travaux. Au sein du SSID, des « Réseaux d'Excellence »[118] (ci-après RE) ont été créés : citons le RE de la guerre électronique, le RE de la nanotechnologie, le RE des technologies d'information. Des partenariats s'effectuent au sein des RE avec la participation des divers partenaires cités ci-dessus.

Plusieurs organismes semi-publics, majoritairement détenus par la Fondation des Forces Armées Turques, ont été créés afin de soutenir la recherche et développement, ainsi que la conception de produits à destination militaire et civile pour satisfaire les besoins de l'armée turque. Deux d'entre eux sont spécialisés dans le domaine de l'informatique et l'électronique : *HAVELSAN*[119] et *ASELSAN*[120].

HAVELSAN, crée en 1982, est le fournisseur principal de l'Etat turc en matière de logiciels, de systèmes d'information, de systèmes de simulation, de systèmes de sécurité et d'e-gouvernement. Tous les logiciels et les systèmes de l'Etat sont conçus, administrés et protégés par l'entreprise. *ASELSAN,* créée en 1975, est quant à elle une entreprise semi-publique spécialisée dans la production des systèmes électroniques de défense et dans la conception et le développement de leurs *softwares*.

Les deux entreprises coopèrent avec les universités spécialisées (comme *METU*, *ITU* et *Bilkent University*) et avec *TÜBITAK* en matière de recherche et développement. Elles sont installées dans des « zones de développement technologiques ». Elles coopèrent par ailleurs avec des entreprises privées au niveau local dans la production et l'approvisionnement des produits intermédiaires et des pièces détachées.

La Turquie coopère également avec les entreprises de divers pays membres de l'OTAN sur des projets de défense (Siemens, Stöeger, Selex…). Selon les chiffres publiés par SSID pour l'année 2010, 52,1 % des besoins de l'armée sont satisfaits par les entreprises nationales et les exportations de l'industrie représentent 850 million de dollars.

---

[116] http://www.btk.gov.tr/basin_bultenleri/dosyalar/BTK-saldiri-14-02-2012.pdf

[117] Savunma Sanayii Müsteşarlığı http://www.ssm.gov.tr/anasayfa/Sayfalar/default.aspx

[118] « Mükemmeliyet Ağları » ***http://sanayilesme.ssm.gov.tr/ARGE/MUKNET/Sayfalar/default.aspx***

[119] http://www.havelsan.com.tr/SirketProfili/ENDefault.aspx

[120] http://www.aselsan.com

« Le Document Stratégique de l'Industrie de la Défense 2009-2016 »[121] publié par le SSID, met l'accent sur la nécessité de développer le secteur national des systèmes d'information électroniques tels que la communication, les systèmes de contrôle à distance, les satellites et les simulateurs.

2.5.5 La cyberguerre, un concept encore peu ancré dans le domaine militaire turc

Même si le gouvernement a la volonté de développer les armes et produits de défense informatiques, ces domaines sont toujours perçus comme des domaines accessoires, complémentaires dans la mentalité militaire turque. L'utilisation du concept de « guerre électronique » au lieu de celui de « guerre cybernétique » ou de « cyberguerre » au niveau militaire en est la parfaite illustration.

[121] http://www.ssm.gov.tr/anasayfa/kurumsal/Documents/2009_SSSS.pdf