Business Services

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE LA DÉFENSE

Etude Prospective et Stratégique

Réseau Internet et sécurité : Quel impact du progrès des Technologies de l'information et de la communication (TIC) sur la capacité de l'Etat français, de maîtrise du réseau et de sa sécurité d'ici 15 à 20 ans ?

Version 1.1

Date : 06/01/2015

Orange Consulting
114 rue Marcadet 75018 Paris
Tél. : (33) 1 56 55 45 00
Fax : (33) 1 56 55 45 01

Description du document

Propriétés				
Titre document	Etude Prospective et Stratégique - Etude sécurité Internet 2030			
Version	1.1			
Rédacteur	Orange Consulting (Christophe GUILLOU, Alain MARCAY) - Pole cyberdéfense et confiance numérique			
Statut	❑ En cours	❑ Revue	■ Validé	❑ Approuvé
Date	mardi 6 janvier 2015			

Classification du document

Classification	
Confidentialité	Confidentiel Client

Diffusion du document

Société	Nom	Fonction	Diffusion
Ministère de la Défense DGA/DS/SASF/SDCP	Xavier FAVREAU	Référent de l'étude	Information

Historique des versions

Version	Opération	Nom	Date
0.2	Version intermédiaire	Orange Consulting	05/09/2014
1.0	Version finale provisoire	Orange Consulting	17/12/2014
1.1	Version finale	Orange Consulting	06/01/2015

Table des matières

1. Introduction

Le présent document constitue le rapport de l'étude « Réseau Internet et sécurité : Quel impact du progrès des Technologies de l'information et de la communication (TIC) sur la capacité de l'Etat français, de maîtrise du réseau et de sa sécurité d'ici 15 à 20 ans ? »

L'actualité démontre régulièrement l'importance vitale du réseau Internet suite à des cyber-attaques de grande ampleur avec un impact majeur sur les plans psychologique et économique voire potentiellement une atteinte aux intérêts de l'état français. De manière générale, les réseaux privés étant de moins en moins « fermés », le niveau d'exposition aux cyberattaques va croître[1] dans les années à venir. Internet est également de plus en plus présent au niveau des systèmes industriels (ex : environnements SCADA) ce qui laisse entrevoir des impacts sur la sécurité physique des biens mais aussi des personnes[2].

Cette étude a pour objectif de faire une analyse prospective à l'horizon 2030 de la cybersécurité du réseau Internet civil, principalement sur le plan technique, mais également sociétal, réglementaire, juridique ainsi que sur les usages. A noter que certains sujets de l'étude pourraient être a priori transposables aux réseaux militaires et gouvernementaux français.

Note : cette étude ne prend pas en compte d'éventuels bouleversements géopolitiques majeurs susceptibles de modifier profondément l'équilibre mondial actuel.

Ce document est structuré en 3 grandes parties :

- La première partie porte sur l'évolution du cyberespace (le réseau Internet, les services et les usages, les tendances en termes de performances et sécurité) [chapitre 4]
- La seconde partie est consacrée à l'étude des nouvelles menaces, des nouveaux scénarios de vulnérabilités et de manière plus générale les enjeux de sécurité dans ce futur cyberespace [chapitre 5]
- La troisième partie est consacrée aux futures mesures de sécurité envisageables (techniques, organisationnelles, réglementaires) [chapitre 6]

[1] (DSI : préparez-vous contre les Cyber-attaques, 2014)
[2] (Digital Life in 2025 - Cyber Attacks likely to Increase, 2014)

2. Remerciements

Les auteurs remercient l'ensemble des acteurs qui ont été sollicités pour la réalisation de cette étude. Beaucoup de contributeurs sont internes au groupe Orange, en particulier les responsables de domaine de recherche au sein des équipes Recherche & Développement du groupe Orange (« Orange Labs »). Les contributeurs externes appartiennent à différents organismes : CNIL, ANSSI, Gendarmerie Nationale, Universités.

3. Résumé

La prochaine révolution attendue d'ici à 2030 sera l'Internet des objets, et plus particulièrement le M2M (Machine to Machine). En effet, le réseau Internet ne sera plus uniquement un vecteur de communication entre des individus et des machines, mais entre des machines totalement autonomes et de plus en plus intelligentes. Dans ce nouveau contexte, les usages de services déportés sur Internet (Cloud Computing) devraient exploser et les terminaux mobiles ainsi que les routeurs d'accès abonné (type box opérateur) seront amenés à jouer un rôle primordial sur le plan de la sécurité.

Au niveau des réseaux opérateurs, les changements disruptifs vont concerner la virtualisation des réseaux (SDN, NFV), les réseaux mobiles de cinquième génération (5G), la téléphonie sur internet WebRTC. Les infrastructures supportant Internet seront par conséquent de plus en plus ouvertes et mutualisées, ce qui va accroitre certains risques et en créer de nouveaux. De grands acteurs de l'Internet actuel (Google, Apple, Microsoft) devraient également challenger les opérateurs historiques via le déploiement de solutions d'infrastructures réseau novatrices et « low-cost », en particulier dans les pays en voie de développement, mais aussi dans les grandes agglomérations occidentales, leur conférant ainsi une plus grande autonomie pour la délivrance de leurs services.

Les enjeux de sécurité à appréhender dans ce futur cyberespace sont multiples ; certains étant particulièrement importants en raison des profondes mutations qu'ils pourraient engendrer :

- La principale rupture à anticiper concerne l'impact des cyberattaques. Aujourd'hui limité à des biens matériels et immatériels (ex : financier), ce sont désormais des vies humaines qui pourraient être impactées en raison de la cyberdépendance croissante de plusieurs secteurs d'activité vitaux : industrie énergétique, transports (ex : voiture connectée), la santé ;
- Couplée à des réseaux de plus en plus performants, l'uniformité croissante des matériels et surtout des logiciels, aussi bien dans le domaine professionnel que grand public, va étendre la portée et la gravité des cyberattaques ;
- La protection des données personnelles, initialement pensée avec une préoccupation idéologique, va devenir un pilier de la lutte contre la cybercriminalité et la cyber-insécurité. Les progrès attendus dans les domaines de la géolocalisation et de la reconnaissance faciale vont aussi amplifier le sentiment de surveillance permanente de la population et probablement aggraver certains risques psycho-sociaux ;
- La modèle d'authentification actuel basée essentiellement sur le couple login/mot de passe atteint ses limites et des changements majeurs sont à prévoir d'ici quelques années pour améliorer le niveau de sécurité global, simplifier la vie des usagers et s'adapter aux spécificités de l'Internet des objets (ressources contraintes) ;
- Les protocoles SSL/TLS qui sécurisent la majorité des échanges sur Internet souffrent d'un grave problème de confiance envers les autorités de certification X.509. Cette problématique de confiance sera d'autant plus critique avec le déploiement envisagé de solutions comme DNSSec ou RPKI/BGPSec pour sécuriser le cœur de l'Internet.

La souveraineté, la sécurité nationale et la capacité de défense de l'état français sont également menacées par cette révolution technologique et sociale :

- La France, et dans une plus large mesure l'Europe, est victime d'une perte croissante de souveraineté sur le plan industriel car elle devient de plus dépendante de pays étrangers (matériels, logiciels, services, recherche et développement). Cette perte de souveraineté s'accentue avec la délocalisation des services et des données engendrées par les usages Cloud ;
- Les évolutions technologiques à venir font craindre une perte de maitrise étatique sur les moyens de surveillance (capacité à réaliser des interceptions légales et des réquisitions judiciaires). La généralisation du chiffrement des flux de bout en bout et des terminaux usager va amplifier cette problématique ;
- Le scénario d'une paralysie économique du pays, voire même de certaines infrastructures et services vitaux, devient de plus en plus probable ;
- La stabilité de l'état pourrait être altérée par les nouveaux risques qui vont peser sur les citoyens, notamment ceux pouvant impacter l'intégrité physique des personnes, mais aussi les risques psycho-sociaux ;
- L'accessibilité du cyberespace civil dans les zones de conflits armés pourrait engendrer une réelle problématique de maitrise de l'information sur le plan militaire, notamment à cause des usages personnels : renseignement via la géolocalisation de terminaux et l'interception de communications, altération du commandement, manipulation de l'information.

Le rôle protecteur de l'état, notamment le ministère de la Défense, envers ses citoyens sera donc un enjeu majeur dans les années à venir. Dans un futur proche, certains sujets devront faire l'objet de réflexions au niveau étatique :

- Faut-il créer un Internet de confiance au niveau national ou européen, avec davantage de souveraineté et de maitrise technologique pour les usages critiques et les missions de services publics ? Un enjeu important sera de concilier la souveraineté numérique avec les libertés individuelles et la capacité d'innovation ;
- Doit-on imposer une normalisation de la sécurité plus étendue qu'actuellement au sein du cyberespace ? (certification systématique des produits matériels et logiciels, garanties entendues sur la maintenance et le support) ;
- Faut-il privilégier une action au niveau national ou au niveau Européen, notamment concernant la gouvernance, la réglementation, la pénalisation ?
- Une étude est à mener sur l'intérêt et les dangers des usages personnels, en particulier les terminaux mobiles, au sein des armées.

En conclusion, Internet ne sera plus seulement un moyen de communication, de divertissement, et de commerce. Il deviendra un système critique pour la survie économique des entreprises et pour le fonctionnement des infrastructures vitales (énergie, transport, santé, alimentaire). Il acquiert désormais autant d'importance que l'énergie électrique à la différence près qu'Internet est plus vulnérable et plus critique en terme de disponibilité (pas de moyens de secours). Toutefois, la société évoluant, il faudra probablement apprendre à vivre avec de nouveaux risques « numériques/virtuels » ayant des impacts très graves dans le monde « physique/réel ». Le risque zéro n'existe pas et n'existera pas. Enfin, il faut garder à l'esprit que la sécurité aura toujours un coût financier, qui devra être assumé par tous les acteurs du futur cyberespace.

4. Evolutions du cyberespace

Tout au long de son histoire, le réseau Internet a évolué avec quelques étapes majeures en termes d'usage. L'Internet est ainsi demeuré pendant longtemps un réseau de télécommunication « technique » avec pour principal objectif la mise en relation de ses utilisateurs, d'abord dans le milieu universitaire et industriel, puis dans le domaine grand public. Le début des années 2000 a vu l'explosion des usages domestiques et professionnels et surtout une démocratisation à grande échelle. Des usages innovants tels que les réseaux sociaux, le e-commerce et de manière générale le e-business ont émergés et se développent encore aujourd'hui. La prochaine révolution qui verra le jour d'ici à 2030 sera l'Internet des objets, et plus particulièrement le M2M (Machine to Machine). En effet, le réseau Internet ne sera plus uniquement un vecteur de communication entre des individus et des machines, mais entre des machines totalement autonomes et de plus en plus intelligentes.

Les fondements de l'Internet actuel, en termes d'architecture et de protocoles, ne devraient pas être remis en cause d'ici à 2030. Des évolutions techniques et organisationnelles peuvent apparaitre, pour moderniser et sécuriser le réseau notamment, mais l'hégémonie d'Internet et son universalité sont telles que l'on ne voit pas comment une technologie concurrente pourrait voir le jour d'ici à 2030. A plus long terme, des technologies orientées sur les contenus comme ICN[3] pourraient émerger, mais cela demeure encore extrêmement hypothétique.

Pour appréhender les futurs enjeux de sécurité, il est nécessaire d'identifier (ou d'évaluer) les futures évolutions et usages d'Internet. Ce chapitre a pour but de présenter une synthèse des évolutions à envisager sur le futur cyberespace à horizon 2030 et de réaliser un premier niveau d'analyse des enjeux de sécurité. Il présente également les grandes tendances sur l'évolution à venir du réseau Internet en termes de performances, dimensionnement et cybersécurité. Tous ces éléments permettent de mieux cibler les futures sources de menaces et d'appréhender les surfaces d'attaques.

Cette synthèse a été réalisée sur la base de plusieurs sources :

- le pôle Recherche & Développement du groupe Orange et sa veille technologique ;
- des travaux de recherche documentaire réalisés spécifiquement pour cette étude (articles/ressources Internet principalement) ;
- des études prospectives récentes sur le thème d'Internet, en particulier :
  - « *La dynamique d'Internet - Prospective 2030* »[4] ;
  - « *France numérique 2012-2020 / Bilan et Perspectives* »[5] ;
  - « *L'Internet industriel* »[6].
  - « *Global Trends 2030: Alternative Worlds*»[7]

[3] (Information-Centric Networking Research Group, 2013)
[4] (La dynamique d'internet - Prospective 2030, Télécom ParisTech, 2013)
[5] (France numérique 2012-2020 / Bilan et Perspectives, MINEFI, 2011)
[6] (L'Internet industriel, Pierre BELLANGER, 2013)
[7] (National Intelligence Council : Global Trends 2030: Alternative Worlds - page 86, 2012)

4.1. Vue « usager »

4.1.1. Les usages mobiles

Les usages mobiles vont continuer de croitre d'ici à 2030 avec une montée en puissance remarquable des objets connectés. Le grand gap technologique, prévu entre 2020 et 2025, sera la généralisation des réseaux mobiles de cinquième génération (5G) qui décupleront les débits par rapport aux réseaux 4G (LTE) actuels et optimiseront davantage l'énergie.

Cette augmentation des performances des réseaux mobiles démocratisera certaines applications gourmandes en débit telles que la visioconférence, la TV sur mobile, la vidéosurveillance, la réalité augmentée. Au niveau résidentiel, il est également possible que certains usagers délaissent l'accès traditionnel en filaire (xDSL, FO) pour ne disposer que d'un accès mobile.

Avec l'essor de la géolocalisation et la multiplication des objets connectés de type caméras et capteurs, il faut surtout s'attendre à une généralisation massive des applications de surveillance et de contrôle à distance dans le domaine grand public qui, actuellement, sont plutôt réservées au domaine professionnel ou à des classes sociales aisées. Outre les problématiques de protection de la vie privée et de fraudes, les utilisations malveillantes telles que l'espionnage dans un contexte de guerre économique vont également s'amplifier.

Le smartphone va poursuivre son développement pour intégrer encore davantage de fonctionnalités, en particulier dans le domaine bancaire et médical. Ainsi, le smartphone pourra être utilisé aussi bien pour des achats en ligne que pour des transactions locales (technologie NFC / paiement sans contact). Il pourra également être utilisé comme relais pour des capteurs biométriques surveillant l'état de santé d'un individu. Le smartphone sera donc plus que jamais un concentré de données personnelles. De manière plus générale, le smartphone est voué à jouer un rôle de pivot vis-à-vis des objets connectés rattachés à un individu (capteurs, montre, lunettes…), car ces derniers utiliseront des technologies et des protocoles spécifiques non IP (développés en dehors de toute standardisation à l'inverse du GSM).

D'un point de vue connectivité, l'accès Internet mobile devrait s'étendre dans des lieux mal desservis actuellement tels que les transports en communs, et plus particulièrement les avions via le développement des offres de raccordement par satellite. Thales prévoit ainsi que 70% de la flotte aérienne mondiale sera connectée en 2025[8].

La généralisation de l'accès Internet mobile dans les automobiles est une évolution majeure qui va permettre le développement de nombreuses applications telles que le guidage intelligent, l'aide à la conduite avec la réalité augmentée, l'assistance mécanique, les services de sécurité (lutte contre le vol, communication de type « e-call » avec les services d'urgence) et à plus long terme le pilotage automatique pour lequel les enjeux de sécurité sont évidents.

4.1.2. Le « Cloud »

Les usages cloud, grand public et entreprise, vont se développer et se démocratiser en raison des performances croissantes sur les réseaux (généralisation du raccordement en fibre optique, réseaux mobiles de cinquième génération).

[8] (Thales parie sur l'Internet à bord des avions pour faire décoller son chiffre d'affaires, 2014)

Les terminaux mobiles et les objets connectés seront des gros consommateurs des services de stockage en ligne. Pour les terminaux fixes, les applications en mode SaaS vont se développer, rendant la machine locale de moins en moins intelligente et de moins en moins adhérente aux individus. Dans ce contexte, il probable que l'on assiste à une convergence des terminaux fixes et mobiles en termes d'environnement système et d'applications.

Certains services de sécurité, comme l'antivirus ou le pare-feu, sont susceptibles d'être délocalisés dans le Cloud. C'est un usage minoritaire aujourd'hui, mais qui va probablement se développer dans les années à venir avec toute la problématique de maitrise que cela engendre. Ce déport de fonction de sécurité dans le Cloud, qui peut être restreint au réseau local, constitue aujourd'hui un axe de recherche important pour sécuriser les objets connectés de faible capacité.

4.1.3. L'Internet des Objets (IoT)

Incontestablement, le développement de l'Internet des objets et du M2M, qui caractérise le web3.0, sera l'évolution majeure du cyberespace dans la prochaine décennie. Ces objets seront présents dans tous les domaines de la vie quotidienne ainsi que dans l'industrie, la grande distribution, l'assurance, la santé, les systèmes industriels ainsi que dans les transports mais aussi dans le domaine de la défense et du renseignement. Les applications sont vastes : médical (capteurs biométriques, pilulier, injecteurs), transport (voiture connectée, sondes de trafic, éléments de signalisation, antivol), eau et énergie (sondes, compteurs, actionneurs), agroalimentaire (outils connectés, collier animaux, capteurs), domotique (serrures connectées, multimédia, électroménager, alarmes intrusion), armement (smartgun[9]).

Ces objets pourront être très adhérents aux individus via le développement des interfaces bio-interactives : capteurs biométriques, appareils médicaux (exemple : pompe à insuline, pacemaker), interfaces bioniques. L'Internet des objets sera également le fondement de la maison intelligente (domotique 2.0) et de la ville intelligente (smart-city) qui immergera en permanence les individus et leur environnement dans le cyberespace.

Bien que les chiffres exacts divergent entre cabinets spécialisés comme IDC, Gartner ou encore IDate, ils convergent tous sur un point : à horizon 2020 il y aura des dizaines de milliards d'objets connectés au réseau Internet. Les prévisions les plus optimistes prévoient 80 milliards d'objets connectés d'ici à 2020[10] (contre 15 milliards actuellement) ; ce chiffre est probablement très sous-estimé si l'on considère les objets indirectement connectés, notamment par l'intermédiaire des smartphones et des box.

L'explosion du nombre d'objets connectés devrait s'accélérer dans les années à venir avec la miniaturisation croissante des composants électroniques associée à une baisse de leurs coûts. Les jeunes sociétés innovantes sont au cœur de cette révolution annoncée qu'est l'Internet des objets : les grands groupes industriels historiques, challengés par ce nouveau domaine qu'ils ne maitrisent pas et dont leurs clients sont friands, s'appuient sur ces jeunes sociétés innovantes pour accélérer la transformation de leurs produits et services. Avec des prévisions de chiffre d'affaire de l'ordre de 300 Milliards $, le marché des objets connectés est vu comme un nouvel eldorado par les acteurs du domaine numérique.

[9] (Des armes à feu compatibles avec les Google Glass, 2014)
[10] (80 milliards d'objets connectés en 2020, 2013)

Les décennies à venir verront le développement d'une catégorie particulière d'objets connectés que sont les robots. Ils seront de plus en plus intelligents et autonomes et utiliseront le réseau Internet pour communiquer, avec des machines ou des individus. Les applications robotiques se situent dans le domaine du transport (avion, bus, train, voiture autoguidés), dans le domaine agricole (robot-tracteur), mais aussi au niveau domestique (robots ménagers, robots de surveillance, robots d'aide aux personnes âgées ou handicapées). D'un point de vue sécurité, une caractéristique commune de ces robots connectés sera le risque d'atteinte à l'intégrité physique des personnes.

Des progrès majeurs sont également à prévoir dans le domaine des interfaces « bio-interactives », support de nombreux objets connectés. Les domaines d'applications sont variés : identification/authentification biométrique, interfaces bioniques et neuronales, interaction holographique, interfaces sensorielles pour les jeux vidéo et les réseaux sociaux, applications médicales.

Il faut aussi s'attendre à une explosion des performances et des utilisations de la reconnaissance faciale. D'abord utilisée à des fins d'authentification, elle se généralisera probablement à d'autres usages tels que la publicité, la surveillance, voire des applications plus sujettes à polémique comme la détection des émotions. La problématique de protection de la vie privée sera évidemment un enjeu de sécurité majeur.

4.2. Vue « opérateur »

Côté opérateur, il faut s'attendre à plusieurs évolutions majeures à horizon 2030 : la généralisation du protocole IPv6 ; la virtualisation des applications réseaux (NFV et SDN) ; les réseaux mobiles de cinquième génération (5G) ; la montée en puissance des réseaux de contenus (CDN) ; l'ouverture de la téléphonie (WebRTC); l'émergence de nouveaux types d'infrastructures réseau. Ces évolutions auront des conséquences importantes en termes de sécurité.

Le protocole IPv6 qui peine à s'imposer aujourd'hui devrait probablement se généraliser d'ici à 2030, notamment en raison de la pénurie des adresses IPv4 et la multiplication des terminaux et objets connectés. Le trafic IPv6, actuellement de 3%, est en croissance constante ; il devrait atteindre 10% en 2015 [source : mesures internes Orange]. La période de cohabitation IPv4/IPv6 va perdurer pendant encore au moins 20 ans, amplifiant ainsi les sources de menaces et la surface d'attaque (doubles piles protocolaires, protocoles de translation, complexité de gestion). A noter que l'administration française a pour ambition de généraliser IPv6 pour l'ensemble de ses services Internet à l'horizon 2015 ; la même cible est souhaitée pour les entreprises d'ici à 2020[11].

La virtualisation des réseaux, qui repose sur les modèles NFV et SDN, a pour finalité l'automatisation et la fourniture d'interfaces externes pour la programmation des réseaux. Les bénéfices escomptés sont notamment la réduction du temps de déploiement de nouveaux services réseau, une plus grande flexibilité en terme d'utilisation des ressources réseau et des gains en matière de coûts opérationnels et d'investissement sur le matériel réseau. NFV et SDN ne sont pas aujourd'hui standardisés et font l'objet de travaux de recherche. Au niveau français,

[11] (France numérique 2012-2020 / Bilan et Perspectives, MINEFI, 2011)

un projet de recherche ANR traitant NFV et SDN associe Orange, Thales, 6Wind, l'Université Pierre et Marie Curie, l'Institut Telecom-ParisTech Normale Sup' Lyon et L'INRIA. A noter qu'Orange prévoit les premières implémentations opérationnelles de SDN sur ses réseaux WAN courant 2017/2018.

NFV[12] (Network Functions Virtualization) est un ISG de l'ETSI qui pour principal objectif la mise en œuvre de fonctions logicielles réseau sur des serveurs banalisés dans une architecture cloud. Cela permet aussi de programmer le chaînage de fonction réseaux pour personnaliser des services finaux pour des clients. NFV peut prendre appui sur SDN pour assurer la connectivité entre machines virtuelles localisées dans des POP (ou data centers) différents.

SDN[13] (Software Defined Networking), projet initialisé par l'ONF (Open Networking Foundation) et considéré par l'IETF et l'ITU-T, définit une architecture de gestion et de commande des ressources réseaux en fonction d'objectifs de services. L'architecture pour le SDN est structurée en trois couches :

- les ressources réseau constituées par l'ensemble des éléments de réseaux physiques ou virtuels (routeurs et commutateurs)
- une couche de contrôle contenant des fonctions d'abstraction et de programmation des ressources réseau sous-jacentes et offrant un ensemble de gestionnaires de service de base comme la gestion des nœuds et des liens associés
- une couche de services applicatifs réseau, tels que des applicatifs de gestion de VPN à la demande, des services de connectivité cloud Network as a Service (NaaS). Les trois couches de l'architecture SDN sont séparées au moyen de deux types d'interfaces dites « Application-control » et « Resource-control ».

La virtualisation va bien évidement faire apparaitre de nouvelles problématiques de sécurité du fait notamment de la mutualisation des ressources et l'ouverture d'interfaces de gestion à des tiers.

Les réseaux mobiles de cinquième génération seront normalisés à partir de 2020 et généralisés en termes de déploiement à horizon 2030 ; ils sont en cours de définition et de normalisation au niveau européen dans le cadre du PPP-5G[14]. La 5G (LTE-B) constituera une transition technologique majeure et globale par rapport aux réseaux mobiles actuels, notamment 4G/LTE. La refonte concernera non seulement la gestion du spectre et les protocoles radios, mais également le cœur de réseau (IMS) et surtout la sécurité. Il fait aussi s'attendre à une généralisation de la voix sur LTE (VoLTE[15]). A plus longue échéance, les réseaux 6G sont déjà évoqués, mais cela demeure encore trop abstrait.

A horizon 2030, Internet devrait évoluer depuis un modèle fournissant de la connectivité réseau vers un modèle fournissant des services, des données et des contenus. Cette tendance est actuellement observée avec la montée en puissance des CDN, générant ainsi des tensions économiques entre les fournisseurs de contenus de type OTT et les opérateurs, voire avec les états (fiscalité, financement culturel, mise en valeur des contenus nationaux). En terme d'architecture, l'IETF envisage même que les terminaisons abonnés puissent évoluer vers des interfaces « Full CDN », avec un adressage basé sur DNS et faisant abstraction des couches IP

[12] (Premiers livrables ETSI concernant la virtualisation de fonctions réseau, 2014)
[13] (Première norme sur la softwarization du réseau 'SDN' et la connectivité à la demande, 2014)
[14] (5G PPP, 2014)
[15] (VoLTE : des appels via 4G améliorés, le point chez les 4 opérateurs, 2014)

et donc sans communication IP de bout en bout (les couches IP seraient réservées au cœur de réseau).

De manière plus globale, les opérateurs risquent de perdre la maitrise de certains services historiques comme la téléphonie (cf. WebRTC) ou la vidéo (ex : OTT Netflix), notamment au niveau des réseaux mobiles. Le WebRTC, qui est une forme de Skype normalisé fonctionnant dans un navigateur web, pourrait ainsi échapper totalement aux opérateurs et potentiellement remettre en cause certains principes de surveillance et de réquisition judiciaire par les états, notamment en raison du chiffrement quasi-systématique des flux. A noter que la technologie WebRTC pourrait également ouvrir la porte à la convergence fixe/mobile qui fait parfois défaut aujourd'hui.

En termes d'infrastructure, de nouveaux types de réseaux devraient voir le jour ou prendre de l'ampleur, court-circuitant ainsi les opérateurs historiques. Il faut notamment s'attendre à une montée en puissance des réseaux communautaires de type had-doc qui sont, pour le moment, plutôt réservés aux pays en voie de développement pauvres en infrastructures. Ces réseaux had-hoc peuvent s'appuyer sur le wifi, voire le LTE sur des bandes de fréquences non-officielles mais sous-utilisées (White-Spaces[16]). Des modèles d'infrastructures réseaux low-cost sont d'ores et déjà testés en Afrique par Google[17] et pourraient très bien s'exporter dans des pays comme la France à moyen terme. Les grands acteurs du net comme Google ou Facebook ne cachent pas leurs ambitions de fournir des solutions d'accès Internet à grande échelle (réseau de satellites ou de drones), leur procurant ainsi une totale maitrise de bout en bout. Une éventuelle perte de maitrise des opérateurs historiques aurait des répercussions majeures sur l'économie nationale et la souveraineté de l'état Français.

4.3. Tendances / Dimensionnement

Même s'il est difficile de réaliser de façon globale et avec précision une projection de ce que sera le dimensionnement d'Internet en 2030 d'un point de vue quantitatif, en particulier à partir des données en notre possession actuellement, nous pouvons appréhender plus facilement l'évolution qualitative de celles-ci et tenter de corréler le tout avec les évolutions technologiques probables.

4.3.1. Evolution du trafic

Ce sous-chapitre décrit l'évolution du trafic Internet résidentiel fixe et mobile depuis une dizaine d'années et propose quelques tendances pour les années à venir. Elle se base principalement sur des mesures réalisées sur les réseaux d'Orange en France et diverses autres études.

- Trafic résidentiel fixe

  En France comme dans la majorité des pays, le trafic Internet résidentiel fixe croit fortement depuis l'introduction des technologies d'accès haut débit, ADSL (à partir de fin 1999) puis FTTH (introduction progressive à partir de 2008).

[16] (4G white-spaces, 2014)

[17] (Google veut amener le wifi en Afrique subsaharienne avec des ballons dirigeables, 2014)

La première composante de cette croissance est celle du nombre de clients. Celle-ci a été forte jusque vers 2010, elle est maintenant très mesurée le marché étant maintenant mature.

La seconde composante de cette croissance est une augmentation toujours soutenue du trafic par client aussi bien en volume (octets échangés par les clients) qu'en débit (qui sert à dimensionner les réseaux), les deux variables étant évidemment corrélées.

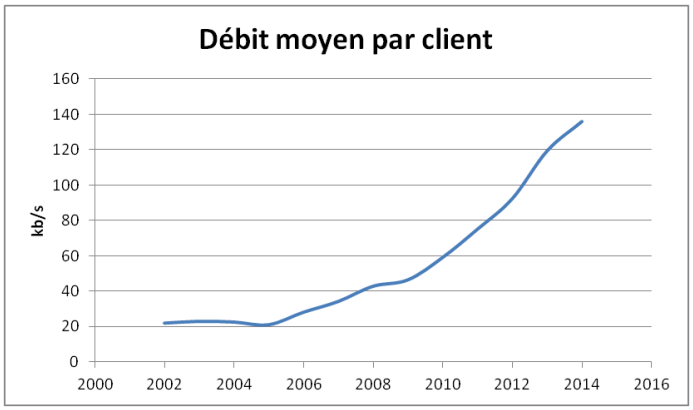

Figure 1 – évolution du débit moyen par client (réseau résidentiel fixe Orange France)

Cette croissance soutenue du trafic est liée en premier lieu aux usages d'Internet, usages qui ont beaucoup évolué depuis 10 ans. La première période (2002-2005) est caractérisée par un usage relativement faible des clients, une connexion au réseau à la demande (en opposition avec la connexion toujours active qui est devenue la norme) et bien sûr un catalogue d'applications réduit. En 2004 les usages sont tirés par l'échange de fichiers en P2P. Débuté avec Napster, cet usage va se développer avec des applications phares comme eMule, BitTorrent. Puis après 2007, le streaming et le téléchargement vont progressivement prendre de l'importance pour supplanter le P2P après 2010. Aujourd'hui le streaming est largement dominant avec des services comme YouTube qui concentre une part très importante du trafic (environ 15% à lui seul).

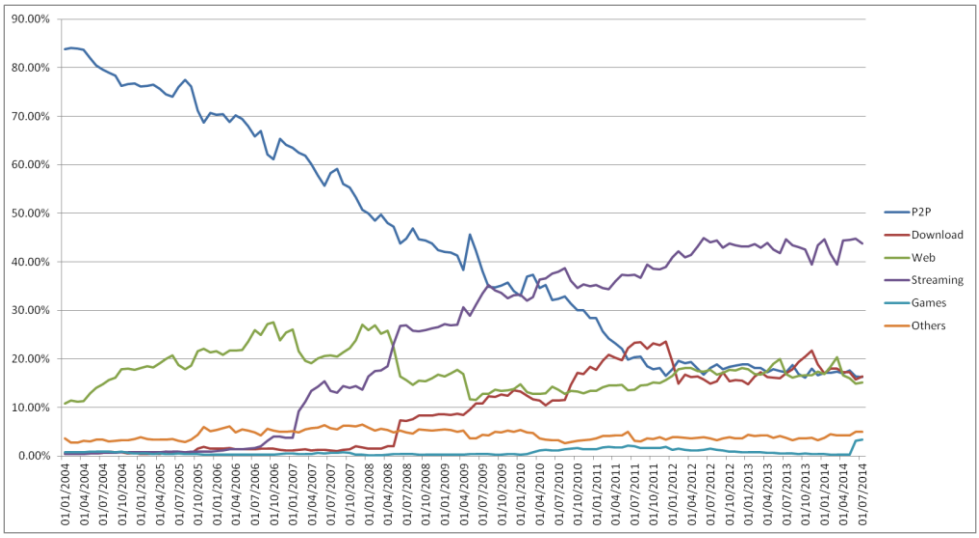

Figure 2 – évolution de la répartition du trafic (réseau résidentiel fixe Orange France)

Les usages se sont également modifiés avec la multiplication des terminaux connectés. Il est aujourd'hui courant d'avoir plusieurs ordinateurs ainsi que des smart phones, tablettes, consoles de jeux et télévisions connectés. L'usage des télévisions connectées reste marginal aujourd'hui (au moins sur Internet, les opérateurs ayant mis en place des services de VoD spécifiques séparés de l'Internet général). Par contre les smart phones et autres tablettes ont tiré les usages depuis ces dernières années pour représenter plus de 25% du trafic global aujourd'hui sur réseau fixe.

Les usages varient également en fonction du type d'accès (ADSL ou FTTH). Sans surprise, les clients FTTH ont des usages plus importants avec environ 50% de volume en plus dans le sens réseau vers client et plus 4 fois plus dans le sens client vers réseau. Les clients tirent manifestement parti du débit remontant beaucoup plus important des accès fibre. Cet usage remontant est majoritairement de l'échange de fichiers en P2P (environ 75%) et concentré sur un petit nombre de très gros utilisateurs.

Au cours des dernières années et en lien avec les usages, il y a eu également une évolution importante de la provenance du trafic. Dans les années 2004/2005, avec une très forte proportion de P2P, le trafic était majoritairement national, la plupart des contenus étant échangés entre internautes français (au moins pour les films et séries qui représentent le gros du trafic). Avec l'arrivée des services de streaming ou de téléchargement, généralement localisés hors de France, le trafic a progressivement basculé vers l'étranger. Puis récemment, avec la multiplication des CDN les sources de trafic sont assez majoritairement revenues sur le territoire français, même si ce 'n'est que via des copies locales de contenus déposées dans des caches.

- Trafic résidentiel mobile

Le trafic Internet mobile a clairement décollé à partir de 2008 et l'arrivée des smartphones, iPhone en tête. La disponibilité de terminaux à l'ergonomie bien étudiée et la disponibilité de nombreux services très pratiques ont fait exploser les usages. La croissance est liée à l'augmentation des smart phones, et à l'augmentation des usages de chaque terminal en lien avec la richesse toujours plus grande des services disponibles et à l'augmentation de capacité des terminaux. Le lancement de la 4G en 2013 a fait repartir à la hausse le taux de croissance du trafic. La croissance est supérieure à 80% par an.

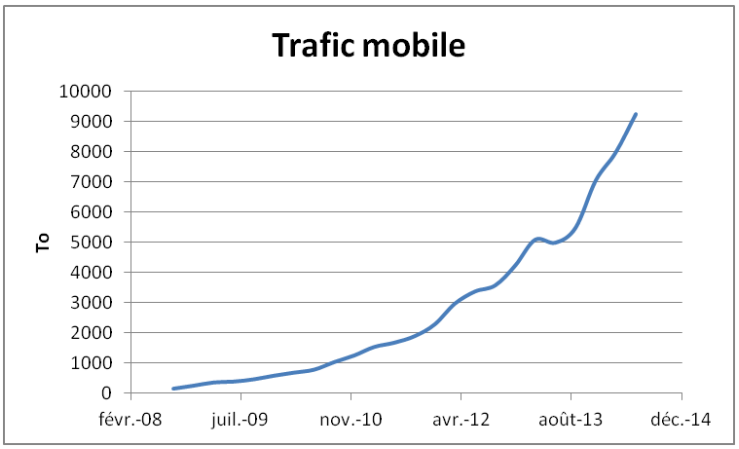

Figure 3 – évolution du trafic mobile (réseau mobile Orange France)

Comme indiqué dans le paragraphe sur le trafic fixe, une partie seulement du trafic des smartphones s'effectue sur le réseau mobile, la partie en fait la plus importante passe par le réseau fixe via la connexion en WiFi sur les passerelles domestiques (Box opérateur) quand les utilisateurs sont à leur domicile. Il est d'ailleurs intéressant de noter que les pics de trafic du réseau mobile ont souvent lieu pendant la pause-déjeuner, en semaine alors que ceux du réseau fixe ont plutôt lieu les dimanches en soirée.

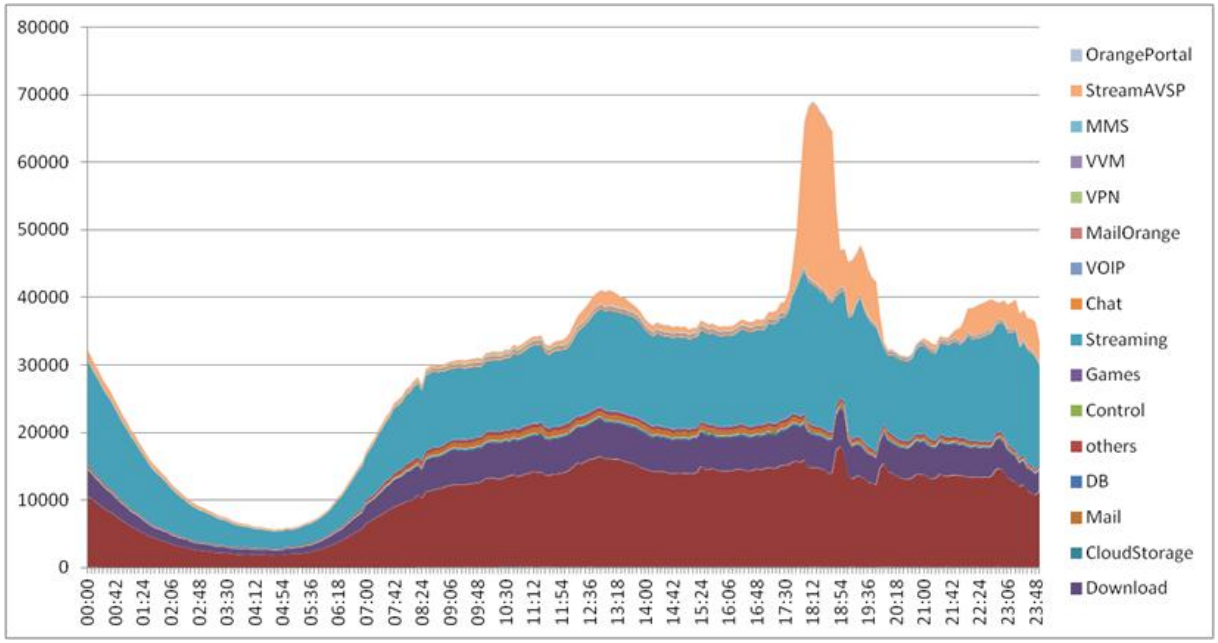

Figure 4 - mesures de trafic en Gb/sur une journée (réseau mobile Orange France)

Le trafic du réseau mobile est relativement faible par rapport à celui du réseau fixe (moins de 10%), il est également plus sensible aux événements exceptionnels. Par exemple, lors du la coupe du monde de football 2014, les matches de l'équipe de France ont provoqué des pics de trafic très importants. Le nouveau record établi en Juin 2014 est de 85 Gb/s, et c'est plus du double du précédent record qui datait de Mai 2014. Ceci n'a été possible que grâce à la capacité importante déployée via les cellules 4G.

Les usages sur réseau mobile sont légèrement différents de ceux sur réseau fixe. Ceci est lié d'une part à la capacité généralement plus faible des accès mobile (sauf en 4G) mais surtout aux types de terminaux. En effet, en France au moins le trafic vient très majoritairement des smartphones (plus de 90%). De plus certains usages comme le P2P sont interdits sur les réseaux mobiles.

Le streaming reste majoritaire, mais on constate des usages Web plus importants, liés au fait que la plus grande partie des applications mobiles (consultations météo, informations…) utilisent des services Web.

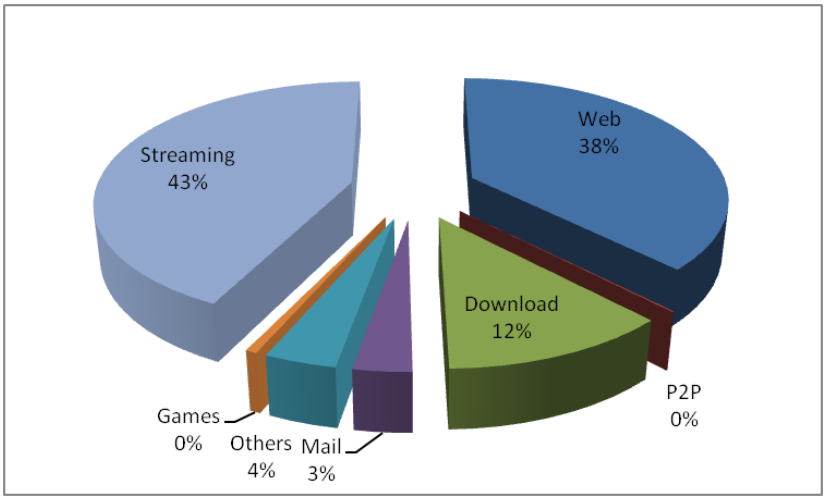

Figure 5 – répartition du trafic mobile en 2014 (réseau mobile Orange France)

- Et dans le futur ?

La prévision de trafic est un exercice difficile, surtout dans un environnement très volatile comme les usages Internet. La plupart des services les plus populaires n'ont que quelques années d'existence, et il est très probable que de nouveaux services à forte audience naissent dans un futur proche.

A l'échelle internationale, suivant que l'on considère une évolution prudente ou optimiste des usages et données véhiculées sur Internet, en extrapolant à partir d'études disponibles actuellement[18], on peut anticiper un volume de données produit compris entre 22 zettaoctets[19] (projection pessimiste) et plus de 80 zettaoctets (projection plus réaliste). L'inflexion vers l'une ou l'autre des tendances va en partie dépendre de la possibilité des gouvernements et des entreprises à relier les populations non encore raccordées à Internet : une étude[20] de l'union internationale des télécommunications (UIT) prévoit de passer la barre des 3 milliards d'internautes à la fin de l'année 2014. Il reste donc un potentiel de 4,3 milliards d'habitants non encore connectés, principalement en Afrique (81%), en Asie/Pacifique (68%) et au Moyen-Orient (59%).

Compte-tenu des spécificités géographiques, des difficultés propres à ces régions et des investissements nécessaires, il est probable que l'accès à Internet dans le futur, notamment pour les populations citées précédemment, sera fera principalement à travers l'Internet Mobile, c'est-à-dire à l'aide d'infrastructures sans fil, depuis un ordiphone/smartphone.

Les volumes de données en jeu, et leur traitement, relève de technologies et de compétences qui relève des mégadonnées (« Big Data »), voire ce que l'on anticipe déjà sous le nom de « Massive Data » ou « Mega Data ».

Dans le futur, comme aujourd'hui, seule une partie infime des données produites seront analysées. Avec la montée en volume globale des données produites, et plus particulièrement avec l'augmentation des données dites « non structurées », comme les

[18] (The Digital Universe in 2020 : BigData, Bigger Digital Shadows and Biggest Growth in the Far East - United States, 2012)
[19] 1 zettaoctet = 1000 exaoctets = 1 milliard de teraoctets
[20] (The World in 2014 : ICT Facts and Figures 2014, 2014)

vidéos ou le trafic M2M, la tâche d'analyse de ce type de données, notamment d'un point de vue sécurité, se heurtera à des plafonds de complexité technique et surtout de rentabilité financière.

Dans le futur, et encore bien d'avantage qu'aujourd'hui, il sera impossible à une entité quelconque, au niveau global mais aussi au niveau régional voire national, d'indexer, de contrôler, de filtrer et surtout de stocker l'intégralité des données produites sur Internet.

Le trafic M2M va continuer se développer avec la montée en puissance des applications de l'Internet des objets. Même si ce trafic restera limité par rapport au trafic global dans un futur proche, sa croissance pourrait être significative au regard des contraintes imposées par des applications faisant de plus en plus appel à l'usage de vidéo (par exemple, télésurveillance, télémédecine, voire navigation).

Dans les mois et les années à venir, l'arrivée de services de vidéo de type Netflix pourrait changer assez fortement les usages par rapport à aujourd'hui. Si l'offre a du succès elle pourrait assez rapidement faire croitre le trafic 10 à 15% (c'est-à-dire la moitié de la croissance annuelle sur les réseaux fixes). Toujours sur les réseaux fixes, l'arrivée de services faciles d'emploi sur télévision connectée pourrait également provoquer une forte augmentation de trafic, les débits de codage nécessaires pour obtenir une bonne qualité d'image sur un écran de télévision étant beaucoup plus élevés que sur une tablette. Cette tendance sera sans doute facilitée par la puissance informatique disponible dans le cloud toujours plus importante. En effet des serveurs à haut débit réclament une capacité de calcul très importante ainsi qu'une très bonne connectivité réseau, ce qui est le cas dans les gros data centres.

Les études prospectives affichent une croissance soutenue du trafic au moins jusqu'en 2020, en particulier pour le trafic mobile dont la croissance annuelle serait supérieure à 60%. De même, le trafic de contenu resterait prédominant. Au final, l'Europe verrait également une croissance du trafic relativement modeste par rapport aux autres régions du globe telles que l'Asie ou l'Amérique du Nord.

- Pour aller plus loin

Le travail présenté par M. Feknous lors du congrès IEEE ISCC 2014 "Internet Traffic Analysis : A Case Study From Two Major European Operators »[21] analyse et compare les usages dans deux pays européens (France et Espagne).

Quelques équipementiers présents dans le domaine de l'analyse du trafic (Cisco[22], Sandvine[23]) publient régulièrement des rapports donnant des projections sur le trafic internet au niveau mondial.

4.3.2. Evolution des infrastructures

L'augmentation continue des volumes de données transportés, traités et stockés n'ira pas sans poser de problèmes, technologiques dans un premier temps, et financiers dans un second.

[21] (IEEE ISCC 2014 "Internet Traffic Analysis : A Case Study From Two Major European Operators, 2014)
[22] (Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013–2018, 2014)
[23] (Global Internet Phenomena Report, 2014)

D'un point de vue technologique, les challenges à relever seront liés à :

- L'évolution des performances

Que ce soit pour le transport de données (avec principalement les fibres optiques et les liaisons sans fil), que ce soit pour le stockage de celles-ci (avec les disques durs et la mémoire vive des équipements), ou que ce soit pour la puissance de traitement nécessaire, aucune des technologies utilisées actuellement n'offre suffisamment de possibilités de scalabilité pour accompagner de façon continue les anticipations de volume et de débit annoncées. Une ou plusieurs ruptures technologiques seront sans doute nécessaires, et des investissements importants en Recherche & Développement indispensables : la 5G et la généralisation de la fibre optique en sont deux exemples d'axes prioritaires.

D'un point de vue plus technique, le protocole IP, élément fondateur d'Internet sera acculé dans ses derniers retranchements. Le besoin d'identifier de façon unique chaque équipement sur Internet et le besoin d'acheminer les données entre chaque entité sur Internet va enterrer progressivement la version actuelle du protocole (IPv4) au profit de la nouvelle version (IPv6). De par sa conception, IPv6 est capable de gérer de façon satisfaisante l'augmentation exponentielle du nombre d'équipements, y compris à l'horizon 2030.

Par contre, les protocoles de routage associés (notamment BGP) devront être en mesure d'accompagner la multiplication du nombre de terminaux, la multiplication du nombre d'acteurs et de leurs réseaux, et au final la multiplication du nombre de routes sur Internet. Ce qui ne se fait pas sans mal aujourd'hui. Pour rappel, malgré toutes les précautions prises par les opérateurs de télécommunications, le 12 aout 2014, la limite théorique de 512000 routes publiques sur Internet (appelés « prefix ») a été dépassée, rendant certaines portions d'Internet injoignables[24]. Des équipements de routage un peu anciens n'ont plus été en mesure de traiter l'intégralité des routes publiques d'Internet. Des investissements seront nécessaires pour mettre à jour ces nœuds clés du réseau des réseaux.

Pour soutenir la croissance de l'internet fixe vers le haut, voire le très haut débit, la solution la plus réaliste et la plus souvent envisagée est la généralisation de la fibre optique : d'un débit descendant partagé 2,5Gb/s (technologie GPON), il est envisager d'évoluer vers un débit descendant partagé de 10Gb/s (horizon 2018-2019), puis vers le standard NGPON2 (débit descendant partagé sera à 40Gb/s) à l'horizon 2025.

- L'évolution des types de flux

Lors du symposium NOMS 2014[25], les tendances en matière d'usages ont été dressées.

Conjointement à l'évolution des volumétries de données, des changements dans la typologie de flux échangés est également prévisible.

La montée en puissance des échanges de flux vidéos en haute (HD), et à terme en ultra haute (UHD) définition va augmenter de façon sensible la sollicitation des infrastructures de transports et de stockage des acteurs de l'Internet (notamment chez les opérateurs globaux, régionaux, transnationaux, nationaux et locaux).

A terme, et à condition de régler d'ici là les problèmes de confiance des utilisateurs, l'augmentation prévisible de la dématérialisation et du stockage des données en ligne

[24] (Devenu trop grand, Internet a subi des perturbations, 2014)
[25] (NOMS 2014 - IEEE Network Operations and Management Symposium – Cracovie /Pologne, 2014)

(Cloud Computing) va apporter aux utilisateurs d'indéniables bienfaits (notamment en termes de simplification des usages et de facilité d'accès). A contrario, cela va encore plus solliciter les infrastructures de stockage et de transport des acteurs de l'Internet.

Que ce soit pour une utilisation « grand public » ou pour un usage professionnel, les échanges M2M, notamment lié à l'Internet des objets (IoT), vont croire de façon importante dans les prochaines années, et pour à terme probablement dépasser les autres formes d'utilisations (C2C, B2C, B2B). Il est notable que les données de l'Internet des Objets auront probablement moins d'impacts sur les volumes transportés que sur les volumes stockés (sur la durée).

- L'évolution des terminaux

Compte-tenu de la miniaturisation, de l'augmentation de la puissance et de l'augmentation des fonctionnalités, dans le futur, l'accès à Internet se fera très probablement à partir des terminaux mobiles, à travers des liaisons sans-fil à haut (4G) et très haut (5G) débit.

Si l'on considère le taux de pénétration très important du téléphone mobile dans les pays développés (121% en moyenne, 117,1% en France en décembre 2013), les deux principales marges de progression sont liées à l'augmentation (continue) des débits, et à l'élargissement des usages (notamment les objets connectés).

A l'inverse, il reste des axes importants de progression dans les pays en voie de développement. Dans la même étude et à la même époque, il a été constaté que le taux de pénétration du portable n'était que de 69% en Afrique et 89% en région Asie Pacifique. De plus, dans ces mêmes régions le haut débit mobile représente moins de 25% de l'ensemble.

D'un point de vue financier, pour pouvoir accompagner les évolutions identifiées précédemment, et pour pouvoir financer les infrastructures susceptibles de supporter les besoins associés (volumétrie, débit, latence) ces acteurs vont devoir investir massivement et sur la durée, avec un modèle économique et un retour sur investissement non encore identifié.

4.3.3. Cybersécurité

Parallèlement à l'évolution des technologies et des usages, les menaces informatiques ont également évoluées depuis le début de l'Internet.

Une évolution des motivations

Au commencement de l'Internet civil (nous ne traitons pas de son ancêtre militaire - Arpanet), l'interconnexion au réseau des réseaux était principalement réservé aux universitaires, aux chercheurs et aux grandes entreprises. L'objectif premier (quasiment utopique aujourd'hui) était l'amélioration de la recherche scientifique par la collaboration entre différentes équipes distantes et in fine la propagation du savoir.

Les premiers actes d'incivilité sur le réseau avaient uniquement pour but l'amusement et la démonstration des capacités techniques. On peut à ce propos citer la création du ver Morris en 1988, ou les premiers livres sur la virologie informatique[26].

[26] (The Little Black Book of Computer Viruses - Mark A. Ludwig, 1991)

Avec la création du World Wide Web (et les technologies sous-jacentes que sont le langage HTML et le protocole HTTP), la mise à disposition d'informations a été simplifiée, le nombre de sites Web a augmenté, le prix des services d'accès à diminué au fil du temps, le nombre d'internautes a cru, bref l'accès Internet s'est démocratisé. Selon le site Internet Worls Stats[27], le nombre d'internautes est passé de moins d'un million en 1990 à plus de 100 millions en 1998 et à plus d'un milliard aujourd'hui.

Les sociétés commerciales ont voulu profiter du nouveau média pour, dans un premier temps s'offrir une visibilité sur ce potentiel de visiteurs, et dans un second temps, profiter de la réduction des coûts d'infrastructure et de télécommunication pour les échanges mondiaux. La création du commerce électronique (et son potentiel fabuleux) viendront plus tard.

Avec l'accroissement des enjeux financiers (commerce électronique, jeux en ligne, etc.) et l'accroissement du nombre d'internautes (donc potentiellement de victimes), les menaces et les motivations liées à la cybersécurité ont radicalement changées : aujourd'hui, Internet est devenu une manne financière pour un ensemble d'organisations et d'individus, certes compétents, mais surtout peu scrupuleux.

Même si les études à disposition sont souvent imprécises et contestables, la tendance du nombre d'incidents de sécurité, d'attaques, voire d'intrusions ne laisse aucun doute. Depuis la fin des années 90, le nombre d'attaques sur Internet augmente de façon exponentielle[28]. A noter que ces dernière années, les attaques en déni de service sont en forte progression.

De même, du fait de ses ramifications profondes avec de nombreux pans de l'économie dans la majorité des pays du globe, le cyberespace est devenu un enjeu de souveraineté pour les pays les plus développés et à l'inverse un moyen de déstabilisation (voire de cyber-conflit) pour d'autres.

Un dernier type de motivation prend également de plus en plus d'ampleur sur Internet : l'« hacktivisme », c'est-à-dire la perpétration d'actes plus ou moins illicites pour faire entendre un message idéologique, politique, environnemental, religieux ou sectaire. Devant la faiblesse des coûts d'une attaque informatique, et les retombées médiatiques parfois importantes qu'elles peuvent engendrer, de plus en plus d'organisations se tournent vers ce type de « communication ».

Une évolution des cibles

Si au début d'Internet les cibles visées l'étaient principalement pour des raisons symboliques (serveurs de la NASA, serveurs de l'armée américaine, serveurs du Pentagone), la recherche de la maximisation du profit (de façon illicite) fait qu'aujourd'hui toute entité connectée à Internet peut être la victime d'actes frauduleux, voire d'attaques délibérées.

Les particuliers intéressent les cyber-attaquants pour leurs données personnelles (données bancaires, informations personnelles, photos, vidéos, etc.) qui seront revendues aux plus offrants, et pour leur connectivité Internet : les ordinateurs infectés par des logiciels malveillants (dès lors appelés « zombies » ou « bots ») seront mis en réseau (appelé « botnet ») pour coordonner diverses activités illicites (attaques, dénis de service, partage de fichiers sans licences) ou fortement encadrées (émission de message électroniques commerciaux par exemple).

[27] (Internet World Stats, 2014)
[28] (Verizon - 2014 Data breach investigations report, 2014)

Les entreprises intéressent les cyber-attaquants pour leurs données professionnelles sensibles (propriété intellectuelle, données financières et bancaires, messages électroniques, comptes utilisateurs) qu'elles hébergent en leur nom propre ou pour des clients. Les sociétés de stockage en ligne, d'hébergement et les prestataires de service « dans le Cloud » sont particulièrement visées.

« Les organisations ont continué à faire face à des attaques ciblées visant parfois directement les secteurs de l'énergie, de la finance, de la santé, de la grande distribution ou encore des infrastructures sensibles », explique JD Sherry, Vice-President of Technology and Solutions chez Trend Micro. « Un choix logique pour les cybercriminels : des cibles stratégiques, sources de gains colossaux, ont été attaquées avec succès, malgré tous les efforts des entreprises pour protéger leurs informations critiques.

Que ce soit pour des particuliers ou des entreprises, des campagnes de rackettage sont également menées régulièrement à travers Internet, notamment à l'aide de rançongiciels (« ransomwares »). A l'aide de logiciels malveillants, les attaquants chiffrent les données sensibles des particuliers ou des entreprises, et les prennent en otage. Le versement d'une rançon est demandé en échange de la clé de déchiffrement des données, de façon à permettre à son propriétaire de recouvrer les données rendues inaccessibles.

Aujourd'hui, dans la mesure où la plupart des attaques sont automatisées, aucune personne, aucune entité ou aucune machine interconnectée à Internet n'est à l'abri.

Une évolution des menaces

En développement croissant ces dernières années, la cybercriminalité est la nouvelle bête noire des gouvernements : usurpation d'identité, vol de données (entreprises et particuliers), malware, phishing (ou hameçonnage), etc. les autorités font face à pléthore d'inventions que les nouvelles technologies ne cessent de rendre possible.

Depuis le début, en 2004, de l'étude annuelle sur les intrusions réalisée par Verizon[29], on constate des évolutions au niveau de la typologie des menaces depuis les débuts de l'informatique, et de l'Internet en particulier.

Si auparavant les attaques étaient principalement opportunistes (les cibles faciles étaient principalement ciblées et attaquées), les attaques actuelles sont de plus en plus ciblées, souvent automatisées (notamment par l'utilisation de maliciels), dotées de mécanismes de protection (anti-détection et anti-analyse[30]) et elles utilisent de nouveaux vecteurs d'attaque, tel que les équipements mobiles (smartphones) ou les terminaux de paiement.

L'utilisation croissante d'outils cryptographiques (actuellement et encore plus dans le futur) par les logiciels malveillants montre une volonté de contourner les mécanismes actuels de protection (comme les anti-virus et les outils de détection d'intrusion). Ces mécanismes complexifient également la tâche d'analyse post-incident (en particulier la rétro-ingénierie) et rendent difficiles les investigations pour essayer de remonter aux sources de l'attaque.

Des techniciens de haut vol, financés par ceux qui ont les plus gros moyens (majoritairement des États, des multinationales et des organisations criminelles), forgent des attaques informatiques très complexes, des Blended Threats, appelées APT (Advanced Persistent Threats), ou encore, par certains, AVT (Advanced Volatile Threats), qui permettent au pirate de

[29] (Verizon - 2014 Data breach investigations report, 2014)

[30] (F-Secure - Malwares analysis Report - Regin, 2014)

cibler une organisation, de tromper toutes les défenses installées (pare-feu, antivirus, IDS/IPS) et de dissimuler des boites à outils complètes dans la machine de l'attaqué.

Les cas de piratage de terminaux de paiement rapportés aux États-Unis, notamment dans les secteurs de la grande distribution et de l'hôtellerie (Target par exemple), ou encore les attaques menées de l'intérieur ayant touché des sociétés de cartes de crédit Sud-Coréennes, démontrent l'urgence de déployer des stratégies de défense sur-mesure.

5. Evolutions des menaces et nouveaux enjeux de sécurité

Ce chapitre a pour but de présenter les nouveaux enjeux de sécurité dans le futur cyberespace en focalisant sur l'évolution des menaces et les scénarios de vulnérabilités. Le domaine de couverture est principalement technique, mais également social et juridique.

Les informations présentées sont basées sur plusieurs sources :

- Le pôle Recherche&Développement du groupe Orange et sa veille technologique, notamment en matière de sécurité
- La communauté expert sécurité du groupe Orange qui associe le pôle R&D et les équipes opérationnelles du groupe
- Des travaux de recherche documentaire spécifiques (articles/ressources Internet principalement)

Cette étude des futurs enjeux de sécurité s'appuie sur les évolutions et tendances présentées dans le chapitre 4. Elle est organisée selon différentes thématiques majeures qui sont présentées dans les sous-chapitres ci-après.

5.1. Une menace à l'échelle mondiale

Le réseau Internet a déjà été le support de quelques attaques ou pannes informatiques de grande ampleur. Les impacts sont, pour le moment, demeurés localisés à un domaine d'activité (ex : DRAGONFLY en 2014[31]), une zone géographique ou un pays (ex : La Georgie en 2008[32]).

A horizon 2030, il faut s'attendre à une menace beaucoup plus étendue ; certains analystes allant jusqu'à évoquer la possibilité d'un krach mondial (« cybergeddon »[33] qui impacterait la totalité du cyberespace (réseau Internet, serveurs, terminaux, objets…). Un tel scénario peut aboutir à des pertes massives de données et interrompre des services pendant une très longue durée. Les conséquences humaines, industrielles, économiques et sociales pourraient donc s'avérer dramatiques comme lors de toute crise majeure.

Une étude menée début 2014 par le groupe Zurich, en partenariat avec le cabinet de conseil Atlantic Council, identifie ainsi sept cyberattaques type, dont le cumul pourrait provoquer un choc mondial à l'image de celui de la crise financière survenue en 2008[34].

Des secteurs d'activité particuliers, comme le secteur bancaire ou le commerce, sont particulièrement sensibles, avec un impact possible au niveau national, voire au niveau mondial. Un fait récent donne une idée de l'impact financier qui peut être atteint (exemple : la perte de 1 milliard de dollar par la société américaine de grande distribution TARGET suite à une cyberattaque[35].

[31] (Dragonfly : après Stuxnet, nouvelle attaque réussie contre les systèmes Scada, 2014)
[32] (Attaques en DDoS : De l'Estonie à la Géorgie, 2008)
[33] (Les risques pour le monde en 2014 : Le cybergeddon, 2014)
[34] (Les risques cyber pourraient provoquer un choc mondial (étude Zurich) , 2014)
[35] (Target : un sinistre cyber américain estimé à plus de 1Md$, 2014)

Les facteurs qui accréditent la possibilité d'un cybergeddon sont multiples :

1) L'universalité croissante des technologies et des produits au sein du cyberespace. La normalisation se retrouve dans les protocoles, mais également de plus en plus dans les produits et les services. A titre d'exemple, des acteurs comme Google deviennent de plus en plus incontournables pour le fonctionnement de l'Internet, surtout dans le domaine de l'Internet mobile avec son OS Android.

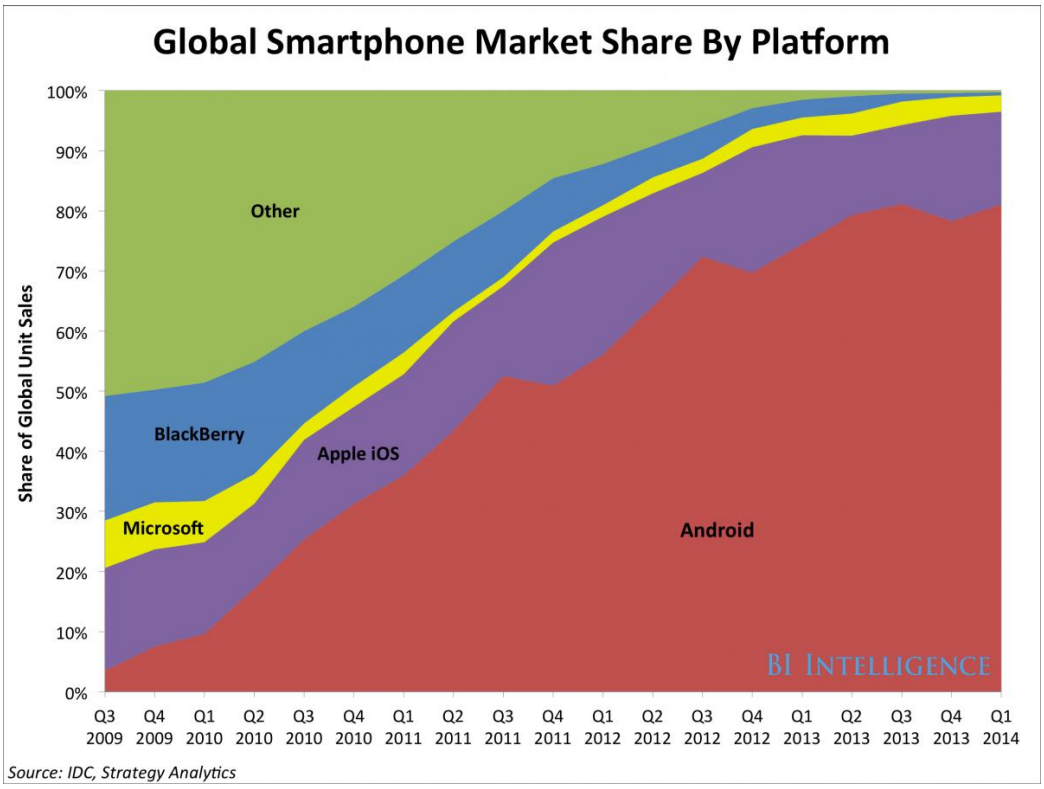

Figure 6 - répartition des OS mobiles (source : IDC, Strategy analytics)

Ce contexte favorise le ciblage et augmente considérablement la surface d'attaque. Le domaine du logiciel libre est globalement problématique : certes, il permet une visibilité sur le code, mais en contrepartie, ce code peut être étudié par des entités malveillantes. En outre, du fait de leur gratuité et de leurs performances, ces logiciels ont tendance à se répandre de manière unique dans le cyberespace et, par conséquent, à augmenter la surface d'attaque. Deux exemples récent de failles de sécurité en sont les parfaites illustrations : sur le protocole OpenSSL (Faille Heartbleed[36]) et sur l'interpréteur de commande Bash (Faille Shellshock[37]). Une problématique majeure est que le code open-source est parfois utilisé dans des composants de sécurité, notamment dans le domaine militaire. A l'avenir, il faut s'attendre à ce que les produits open-source soient davantage ciblés qu'actuellement (exemple : introduction de « backdoor » dans des patchs correctifs)

[36] (Une nouvelle faille découverte dans OpenSSL, 2014)
[37] (Shellshock, la nouvelle faille qui inquiète Internet, 2014)

2) La dépendance par rapport au cyberespace. Outre l'usage du réseau comme vecteur de communication, les usages Cloud (exemples : Office 365, Salesforce, SAP) vont continuer de croître que ce soit au niveau des entreprises, des administrations qu'au niveau du grand public.

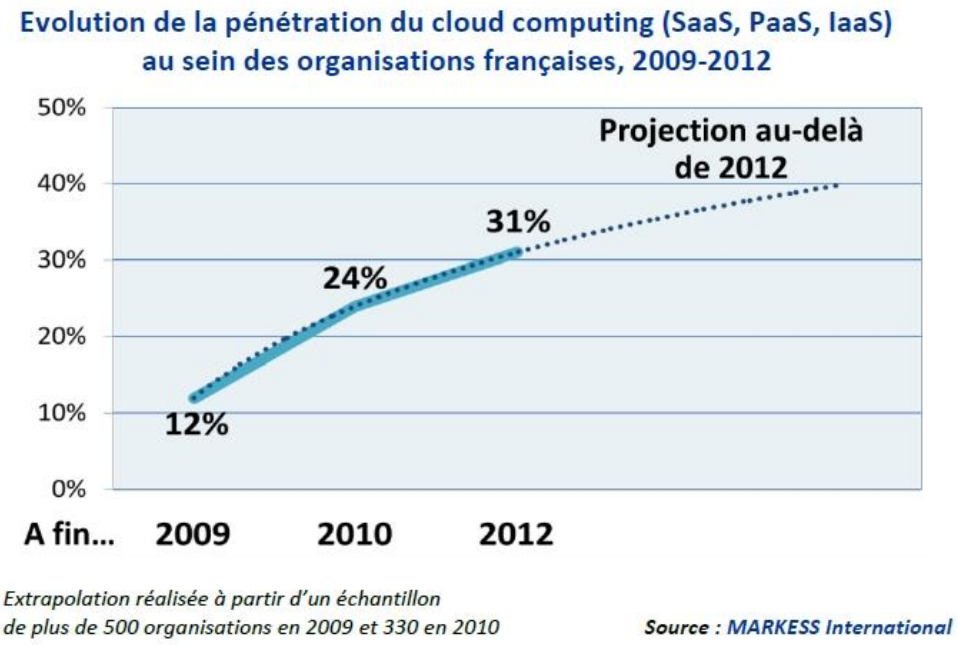

Figure 7 - Taux de pénétration du Cloud en France (source : Markess International)

Une indisponibilité du réseau Internet aboutira logiquement à une incapacité à accéder aux services et aux données. Cette dépendance peut être étendue au fonctionnement même des terminaux dans la mesure la diffusion des logiciels et des mises à jour se réalisent uniquement via le réseau (exemple : Google Play, AppStore, Windows update). Ce concept de diffusion logicielle via le réseau apporte un pouvoir important aux acteurs de l'Internet qui les fournissent. Il est aujourd'hui très focalisé sur les terminaux mobiles, mais sera de plus en plus présent au niveau résidentiel et au sein des entreprises (activation de licences à la demande par exemple). Cette nouvelle manière de « consommer » du logiciel progresse en raison de la simplicité d'installation, de gestion et d'utilisation, mais cela ne doit pas occulter l'extrême dépendance par rapport à ces fournisseurs de services.

3) La réactivité de l'Internet pour véhiculer l'information. En raison des progrès technologiques, notamment sur les réseaux mobiles, l'information circule de plus en plus rapidement. Les systèmes et applications étant de plus en plus homogènes (mêmes OS, mêmes applications, mêmes versions), les futures cyberattaques seront inéluctablement plus rapides et plus destructrices en volume.

4) La multiplicité des interconnexions, en nombre et en type de technologie, notamment avec l'essor des objets connectés. Cela accroit la surface des attaques, mais aussi la source des attaques (DDOS par exemple).

5) L'intelligence des machines de plus en plus prépondérante dans le fonctionnement même du cyberespace. L'automatisation grandissante dans la gestion des réseaux et

des services (exemple : le SDN) peut aboutir à des réactions en chaines avec une perte de contrôle par l'humain. Un phénomène comparable s'est déjà produit dans les réseaux boursiers, par exemple lors du krach boursier de 1987[38].

6) Le développement d'une cybercriminalité « organisée » et des organisations gouvernementales. L'actualité le démontre régulièrement ; la montée en puissance de ces organisations à but offensif va se poursuivre. (cf. §5.2). Ces organisations ont les moyens de mener des cyberattaques multiples, combinées ou parallélisées.

Exemple de scénario d'exploitation de vulnérabilité : compromission du service GooglePlay aboutissant à la diffusion d'une mise à jour corrompue (malware) sur les terminaux Android. L'impact pourraient concerner un parc très important de terminaux (mobiles et tablettes notamment) et porter atteinte à la confidentialité ou à la disponibilité des données (exemple : attaque massive en DDOS vers des tiers). L'exemple récent de la cyberattaque DRAGONFLY dans le domaine des systèmes industriel illustre ce genre de scénario dans un secteur d'activité particulier.

La source des menaces peut être d'origine malveillante (cyber-attaque), mais des scénarios de panne à grande échelle ne sont pas à exclure, notamment en raison de l'universalité accrue des protocoles et des produits (OS, logiciels, services web) et en particulier les produits de sécurité. Un simple bug peut involontairement provoquer une panne à grande échelle. Cela s'est déjà produit, à plus petite échelle, dans le domaine de la téléphonie mobile (cf. bug dans le logiciel HLR ayant abouti à une panne majeure du réseau mobile Orange en 2012[39]. Le scénario d'une tempête solaire impactant les réseaux électriques et de télécommunication à grande échelle est également à prendre en compte. Selon le physicien Pete Riley, ce type d'évènement aurait une probabilité d'occurrence de 12% dans la prochaine décennie[40].

Enfin, certains états comme la France, ne sont aujourd'hui probablement pas suffisamment préparés pour faire face à une telle menace, notamment par l'absence de plans de crise à grande échelle prenant en compte la population. Dans cette optique, il faudrait envisager des plans de crise à l'échelle nationale, mais également internationale. Une démarche comparable existe aujourd'hui dans le domaine de la santé par exemple, avec différents plans de crise permettant de faire face à une pandémie.

5.2. Cyberguerre, cyberterrorisme et cyberdéfense

Nous sommes passés d'un monde constitués de blocs opposés idéologiquement forts (l'utopie motrice de la société, fédératrice), composé de territoires bien repérés dans l'espace (les frontières) qui s'affrontaient via des médias lents et localisés portés par des intellectuels instruits, à une toile reliant des gens différemment matérialistes (la technologie devenant la motrice), dispersés, isolés dans l'espace mais ultra-connectés, pas forcément instruits mais surinformés, prolixes et prolifiques, réunis en tribus réactives. Conçu selon l'esprit du Premier amendement de la Constitution des Etats-Unis, l'Internet est un encore un espace de liberté où

[38] (Krach d'octobre 1987, 2014)
[39] (Panne géante d'Orange : les dessous techniques de l'incident, 2012)
[40] (Une tempête solaire a frôlé la Terre en 2012, 2014)

il est difficile de légiférer au-delà de l'espace National. De plus, les dérives actuelles observées sur l'Internet, sont autant de preuves qu'en l'absence de législation, ce n'est pas par son surmoi que l'homme, cachés derrière proxies et botnets, brille.

Nous pouvons tenter de qualifier le monde grâce à nos sciences humaines, de quantifier les comportements de groupes… l'influence reste toutefois LE facteur majeur de la structuration de nos sociétés, que celle-ci soit le fait de lobbyistes, des gens de la mercatique ou de ceux de la communication : combien de personnages publiques, de marques, de particuliers en ont été victimes.

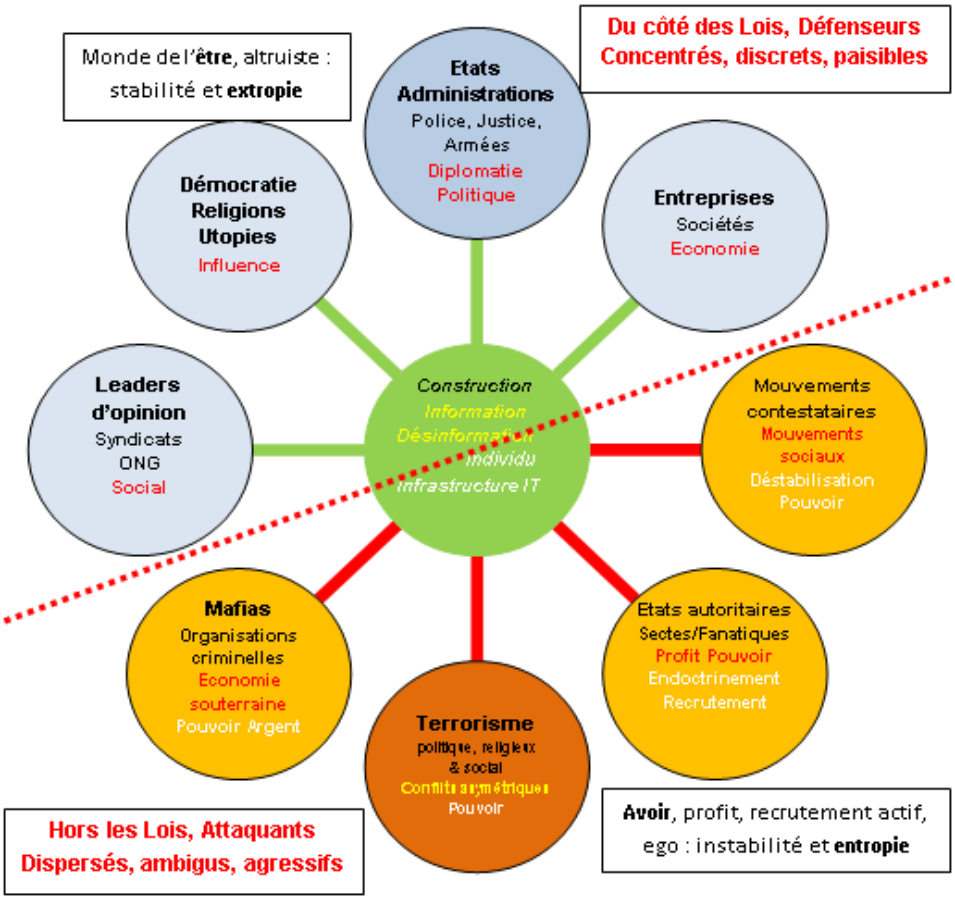

Figure 8 - Le monde de l'Internet

A chaque sphère du monde institutionnel (ici en bleue) s'oppose une sphère (en orange ou marron) diamétralement opposée, principale source ces prochaines années de la cybercriminalité ; l'argent (qui donne le pouvoir) reste la motivation première de ces gourous. Sous couvert d'idéologies, et grâce à l'Internet, des gens exilés, dispersés dans l'espace, réussissent à créer des groupes d'intérêts communs ; dans un monde confus, au nom de nouvelles utopies certains tentent de recruter des disciples pour de conquérir les espaces perdus de nos républiques. Dans un contexte d'adversité, difficile pour des adolescents attardés de distinguer le vrai du faux, le bien du mal.

Si nous parlons aujourd'hui de cyberdéfense, c'est bien parce qu'il y a des cyberattaques : la cyberguerre a commencée depuis déjà longtemps, c'est une guerre économique entre des états concurrents, les pays les plus développés technologiquement. Dans ce contexte troublé,

la montée de groupuscules agressifs provoquera une recrudescence des conflits asymétriques, ce qui obligera les Etats à des actions d'infiltration, des ripostes nombreuses mais ponctuelles et ciblées : sur l'échiquier international, la meilleure défense reste encore l'attaque : avoir toujours un coup d'avance (spécialité états-unienne, évidence depuis déjà longtemps pour les « buzz-marketeurs »).

Un autre phénomène à prendre en compte est la créativité des internautes : en effet, avec une imprimante 3D achetée d'occasion sur un site d'objets d'occasion et un logiciel trouvé sur l'Internet on peut aujourd'hui reproduire des armes à feu indétectables aux portiques de sécurité conventionnels ; nous pouvons aussi viser une cible grâce à nos Google Glass… cette innovation sauvage doit faire l'objet d'une veille permanente de la part des différents services qui sont chargés de protéger nos citoyens.

Pour une Nation, maîtriser les technologies que tous utilisent est essentiel, et, parce que nous sommes tout le temps potentiellement dans une gestion de crise, il est principal d'avoir le contrôle total de ses communications. La professionnalisation de la menace oblige tous les corps de l'état à procéder à une veille en temps réel mais surtout à posséder la plus forte expertise globale possible de ce monde complexe. »

Ces prochaines années, nous risquons d'assister à la multiplication des conflits asymétriques, des actes de cyber-terrorisme ou de cyber-activisme, qui pourront tout aussi bien dissimuler des actes de cyberguerre de la part d'Etats impérialistes, attaques qui viseront à déstabiliser les Etats, à voler des données industrielles ou clients, ou à saboter les moyens de production, les infrastructures, les OIV. Il sera de plus en plus complexe de distinguer une agression due à un groupe criminel d'une attaque due à un Etat. Les moyens qui sont à disposition de ceux qui commettent des forfaits sont tous les mêmes : proxies (Tor), BotNets (machines zombies), techniques… Une recrudescence de la saturation des bandes passantes est à prévoir.

Internet devient un espace pour des guerres qui agissent aujourd'hui sur le plan économique et social, mais qui à terme, pourraient atteindre l'intégrité physique des personnes … Les cyber attaques dirigées contre un état peuvent ainsi désormais être considérées comme des actes de guerre par L'OTAN[41] ; elles tombent sous le coup de l'article 5 du traité de l'OTAN, article qui prévoit la solidarité entre les membres en cas d'agression de l'un d'eux.

La cyberdéfense consistera à répondre en temps réel, et de la manière la plus proportionnée possible, à toute cyber-agression, notamment avec une approche plus offensive de la sécurité. L'art de défendre pourra alors s'appuyer sur des renseignements sûrs qui nous autoriseront à faire feu les premiers. Cette guerre préventive risque d'être au cœur des cyber-conflits futurs.

5.3. Gouvernance du cyberespace

L'Internet est aujourd'hui largement gouverné par les Etats-Unis : innovation technologique et technique, électronique, matériels, logiciels, ils sont devenus leaders pour dominer le cybermonde. Nos alliés anglo-saxons utilisent les renseignements ainsi obtenus à des fins de domination économique ; toutefois, ils sont en train de payer les très nombreux transferts de

[41] (L'OTAN prévoit une réaction militaire contre les cyberattaques, 2014)

technologies effectués dans le cadre de ces années prospères de sous-traitance chinoise. En effet, la Chine ébranle, dans quasiment tous les domaines, la suprématie américaine, menaçant du même pas leur capacité de renseignement électronique (brillant exemple : Huawei contre Cisco). La Chine, qui, rappelons-le, possèdent ¼ des travailleurs mondiaux, fait preuve d'une hostilité systématique sans commune mesure avec ce que font les autres Etats.

Si la Chine, la Russie ou la Corée-du-Nord possèdent encore des réseaux cloisonnés hérités des années du communisme, les pays de l'Union Européenne sont totalement dépendants des technologies et techniques de leur principal partenaire économique et allié. Dans ce contexte de récession économique, aucun des pays de l'Union ne pourrait aujourd'hui envisager la construction de matériels, réseaux, OS, logiciels qui seraient véritablement indépendants, donc maîtrisés[42]. Nous ne pouvons que tenter de protéger nos communications et nos données, de repenser les périmètres et de chiffrer fortement (ce qui reste un problème sur le sol américain), avec nos propres algorithmes.

L'obligation récente imposée aux OIV, auxquelles l'ANSSI demande une obligation de résultat quant à leur résilience, procède d'un profond changement de paradigme : avant c'était la coutume et l'usage qui faisaient Loi. Aujourd'hui c'est l'occurrence du risque qui pousse l'Etat à légiférer. Ce que les Etats-Unis, l'Allemagne et maintenant la France s'imposent, devrait être exigé des autres pays d'Europe, puisqu'il s'agirait d'une Union, certes bien disparate en terme de préoccupations et de maturité des SI La qualité des enseignements dispensés dans les grandes écoles et universités françaises nous permet de posséder une grande expertise en termes de recherche (en cryptologie) et dans le domaine du conseil : c'est à ce titre que nous devons continuer à être prescripteurs pour l'Europe, pour nos partenaires économiques étrangers, et, qu'à l'image de la démocratie, nous devons défendre avec vigueur nos convictions éclairantes.

Lorsque structurer de simples accords bilatéraux s'avère être déjà une épreuve, un accord global sur la gouvernance de l'Internet semble relever de l'utopie, d'autant plus qu'un désaccord profond sur les questions de contenu / contenant subsiste entre Occidentaux et anciens pays communistes, ces derniers considérant que la machine et les données sont une seule et même chose. Pour qu'un accord multipartite puisse engager plusieurs gouvernements dont certains ne seraient pas démocratiques autour d'un acceptable et d'un inacceptable, il faudrait que tous s'accordent sur une approche commune qui se conformerait aux différentes cultures, aux mœurs, aux croyances, aux sensibilités : cela supposerait que l'Internet dût être apolitique, areligieux et familial, qu'il procédât plus d'une envie de valoriser l'humanité, de produire des choses intelligentes ou bienveillantes (scientifiques, culturelles, artistiques… ce pour quoi il fut d'ailleurs créé), plutôt que de tout mystifier, vilipender ou détruire. A cette époque de l'épuisement des ressources et du développement durable, le retour à des collaborations de proximité pourrait-être une solution. Une entente avec l'Allemagne serait souhaitable pour la France, à condition bien sûr, que l'Union Européenne puisse un jour bénéficier, à l'image de ce qui est fait aux Etats-Unis d'Amérique, d'un pouvoir supranational qui consisterait en l'arbitrage des intérêts économiques particuliers des différents Etats membres.

[42] (La cybersécurité est une question de souveraineté, selon Guillaume Poupard, 2014)

En nous appuyant sur notre « French Echelon » (possible compte tenu de la dispersion de nos territoires), et en nous alliant à des pays forts et pareillement développés en terme de SI, nous pourrions espérer conserver notre relativement indépendance, être toujours compétitifs, dans un monde que nous avons voulu ouvert. La volonté forte et apparente qu'ont les états de devenir des acteurs majeurs de la gouvernance de l'Internet relève plus d'une volonté d'y participer, d'un besoin de considération, que d'une opportunité effective. S'allier à certains de ces grands pays industriels parait à terme obligatoire : l'anthropologie culturelle, la géopolitique, la diplomatie devant en devenir les garde-fous.

5.4. Souveraineté et territorialité

La problématique de souveraineté nationale est un sujet d'actualité majeur. Au quotidien, la France reste innovante au niveau des services et des usages au sein du cyberespace. En revanche, elle est aujourd'hui entièrement dépendante de tiers étranger sur les plans technologiques et économiques, notamment dans les domaines suivants :

- Les composants matériels utilisés en micro-électronique [hormis pour quelques besoins spécifiques militaires ou gouvernementaux ainsi que dans le domaine des cartes à puces]
- Les équipements cœurs de réseau et sécurité (en particulier les produits Firewall, les IDS/IPS), les serveurs, les terminaux … A noter que certains équipementiers étrangers disposent également d'une contrôle total sur leurs équipements par délégation des opérateurs et des fournisseurs de services (infogérance, maintenance)
- Les principaux systèmes d'exploitation, notamment MS Windows, Google Android, Apple IOS
- Une grande partie des middlewares et applications, pour les entreprises et le grand public
- L'Open source (fort soutien des Etats-Unis)
- Les services, notamment de type Cloud, fournis par les gros acteurs du net tels que Google, Amazon, Apple, Microsoft, Facebook, les OTT pour la vidéo et la musique …

Cette dépendance est aujourd'hui acceptée par la France car elle accorde une certaine confiance envers les Etats-Unis qui est le principal fournisseur de solutions matérielles et logicielles à l'heure actuelle. A noter que les états ont également une maitrise très importante du réseau Internet global (plages d'adresses, BGP, DNS).

A horizon 2030, si aucune mesure n'est prise, cette dépendance va perdurer et même s'amplifier. L'hégémonie américaine pourrait être remise en cause par de nouveaux acteurs, comme la Chine[43] par exemple, notamment par le développement de technologies innovantes dans le domaine de la fibre optique. La marque Huawei est aussi en progression constante au niveau de ses parts de marché et se diversifie (équipements réseau et télécom, terminaux mobiles) ; elle dispose en outre d'une force de R&D de plus en plus importante.

Actuellement, aucune initiative sérieuse au niveau national et même européen n'existe pour rétablir une forme de souveraineté dans le domaine des TIC et assurer une certaine

[43] (L'actuelle bataille des câbles préfigure-t-elle le cyberespace de 2030 ? , 2014)

indépendance dans la maitrise du cyberespace[44]. Cette perte de souveraineté pourrait s'amplifier avec l'avènement du SDN engendrant une perte de maitrise absolue sur les cœurs de réseau des opérateurs.

Outre la souveraineté, se pose également un problème majeur de territorialité qui devrait s'amplifier dans la prochaine décennie. En effet, par nature, le réseau Internet est mondial et ne connait pas de frontières (à l'exception de quelques pays qui appliquent un cloisonnement, comme la Chine ou la Corée du nord). Le modèle de fonctionnement en Cloud (stockage en ligne, applications SaaS) et la localisation de nombreux serveurs à l'étranger engendrent une forme de délocalisation numérique qui rend de plus de plus difficile l'application d'une réglementation nationale, en particulier sur le plan de la fiscalité. D'ici à 2030, il faut s'attendre à une exportation massive des données des individus et des entreprises françaises vers l'étranger. Les grands acteurs américains déploient des efforts considérables pour collecter de manière confidentielle ces données dans une optique Big Data. Certes, une réglementation peut exister et être appliquée en France, mais au niveau international, cette réglementation est aujourd'hui complètement caduque. D'autre part, la tendance croissance à généraliser le chiffrement des flux va rendre de plus en plus difficile les contrôles et les éventuelles interceptions étatiques, faute d'une législation spécifique (obligation de fournir les clefs à un organisme étatique par exemple). Le modèle règlementaire actuel pourrait rapidement s'avérer inefficace s'il n'existe pas de frontières numériques, à l'échelle nationale ou européenne, pour être en mesure d'imposer et de contrôler cette réglementation.

Ce problème de territorialité génère déjà des conséquences importantes, par exemple :

- incapacité à mener des enquêtes judiciaires sur des données stockées dans des Cloud étrangers (refus de la perquisition possible par le fournisseur, durée de rétention des données et des traces non assurée)
- incapacité d'organismes tels que le CSA à contrôler les contenus vidéo
- difficulté à faire respecter les droits d'auteur (la loi Hadopi est facilement contournable)
- incapacité de l'état à protéger efficacement les mineurs vis-à-vis de la pornographie ou des jeux en ligne
- incapacité de l'état à interdire les paris en ligne prohibés
- accès à des sondages interdits lors des campagnes électorales

A plus long terme, avec l'ouverture de la téléphonie sur Internet, la convergence fixe-mobile et la montée en puissance des OTT diffuseurs de contenus vidéo et audio, il faut s'attendre à une perte de contrôle encore plus importante de l'état en matière de censure, de respect réglementaire, et de possibilité d'investigation et de perquisition.

Ce problème de territorialité peut poser des problèmes plus sournois. Par exemple, un individu peut avoir fait valoir son droit à l'oubli auprès de Google en Europe (notamment en France), mais une société d'assurance ou un responsable RH qui cherche des informations sur cet individu peut facilement contacter un homologue étranger pour obtenir les informations censées avoir été effacées. Le développement du Big Data, notamment à l'étranger, pourrait aboutir à une explosion de ce type de pratiques et donner lieu à une véritable industrie du renseignement à usage commercial. Des applications existent également pour les particuliers (situation de

[44] (L'Internet industriel, Pierre BELLANGER, 2013)

divorce par exemple ou l'ex-conjoint chercherait des preuves d'infidélité), mais aussi pour les entreprises (carnets d'adresses client, chiffres commerciaux).

5.5. Les impacts d'Internet sur la défense nationale

Le cyberespace peut avoir des effets directs ou indirects sur la capacité opérationnelle militaire de la France. L'analyse ci-après ne couvre pas la dépendance technique ; il est fait l'hypothèse que les systèmes militaires critiques nationaux et multinationaux, notamment OTAN, sont conçus de manière à être décorrélés et indépendants du cyberespace public. L'analyse ne traite pas non plus la problématique d'interopérabilité entre les systèmes militaires et les réseaux publics qui fait l'objet d'expertises spécifiques en fonction des besoins de sécurité et du système concerné.

Les impacts sont actuellement relativement limités ; ils se cantonnent principalement à des problématiques sociales de par le niveau d'information que les militaires peuvent obtenir en dehors des canaux conventionnels de communications militaires. En effet, l'essor des réseaux publiques Internet et mobiles à travers le monde, et en particulier sur les champs de bataille, offre aux militaires la possibilité d'avoir rapidement accès à des informations non vérifiées et non censurées via des canaux de communications non surveillés et difficilement maitrisables. Les militaires sur le champ bataille ont également de plus en plus la possibilité de transmettre des informations potentiellement interdites vers leurs proches ou les médias, notamment via les réseaux sociaux. A horizon 2030, cette problématique va être fortement amplifiée, notamment par les performances accrues des réseaux ; avec des conséquences classiques : impact sur le moral des troupes, désobéissance, désertion, mutinerie, manipulation de l'opinion publique. La maitrise de l'information sur les réseaux publics au niveau des champs de bataille sera un enjeu majeur, notamment au regard des risques de manipulation de l'information et de l'instantanéité du futur cyberespace (exemple : informations « personnelles » pouvant démotiver le soldat). Une communication avec l'ennemi, court-circuitant la hiérarchie est également à envisager (contacts directs avec les soldats ennemis par exemple).

Sur un plan strictement militaire, toute l'attention des armées devra donc se concentrer sur les risques liés aux usages personnels, tout particulièrement quant à l'utilisation des terminaux mobiles sur le théâtre d'opérations. A noter que les terminaux mobiles peuvent également offrir également des possibilités de géolocalisation et d'interception de trafic à l'ennemi.

La capacité opérationnelle de la France est également conditionnée au bon fonctionnement de ses infrastructures. Or ces infrastructures sont de plus en dépendantes du cyberespace pour fonctionner correctement. Des mesures de protection sont actuellement prises pour pallier les pannes (groupes électrogènes, réserves de nourriture, réserves de carburant, régiments du génie …). Il faut toutefois noter que toutes les mesures de protection sont prévues pour une durée limitée et il n'est pas certain que cela puisse permettre de faire face à un sinistre pendant une longue période dans le cas où la panne est consécutive à une cyberattaque.

Il convient également d'anticiper des évènements indirects tels que l'indisponibilité des infrastructures de transport, de par leur dépendance croissante au monde numérique et au cyberespace.

Concernant le réseau routier, différents scénarios peuvent aboutir à sa paralysie[45], notamment en raison de l'encombrement par des véhicules civils (attaque sur les systèmes de signalisation et de contrôle, indisponibilité des systèmes de géolocalisation et de navigation, scénarios de vulnérabilités avec les voitures connectées notamment sur les fonctions antivol, génération de phénomènes de panique). L'impact principal peut être de ralentir, voire empêcher le transport de troupes et de matériels, notamment en zone urbaine. Cela peut aussi impacter les personnels qui opèrent les infrastructures critiques du pays.

La problématique existe également, mais dans une moindre mesure, pour les transports en communs (Trains, Bus, Métro) ainsi que dans les systèmes de navigation ou de contrôle aérien, pour lequel l'effet est principalement de provoquer un ralentissement de la capacité opérationnelle.

Enfin, un scénario susceptible d'impacter la capacité opérationnelle de la France est le risque d'émeutes et de troubles graves en cas de cyberattaque majeure. En effet, les modes actuels de distribution et consommation sont de plus en plus dépendant du cyberespace. A horizon 2030, des besoins primaires tels que boire et manger par exemple pourraient poser problème en cas d'indisponibilité du cyberespace. Des besoins secondaires, néanmoins importants tels que l'accès à l'énergie, aux carburants, à l'eau potable viendront amplifier ce phénomène si cela se produit. Il s'agit là de certains symptômes d'un état de guerre avec un ralentissement de l'activité globale, notamment au niveau de l'industrie agro-alimentaire.

Plus simplement, les citoyens français, fortement dépendants du cyberespace, pourraient subir des actions malveillantes, notamment de la manipulation d'information et de la propagande, uniquement dans le but de générer une réaction sociale contre l'Etat.

5.6. Essor de la cybercriminalité

La cybercriminalité tends vers une véritable industrie, de mieux en mieux organisée, dont le cout mondial est actuellement estimé à plus de 400 milliards de dollars selon une étude menée par MCAfee et le CSIS (Center for Strategic and International Studies), dépassant ainsi les revenus estimés du trafic de drogue au niveau mondial[46]. L'organisation de la cybercriminalité ne suit pas un modèle mafieux (hiérarchique), mais plutôt un modèle communautaire coordonnant des groupes d'individus relativement autonomes et de taille modeste ; les compétences et les ressources faisant l'objet d'un marchandage à l'échelle mondiale. L'organisme européen EC3 (Europol's European Cybercrime Centre), entretient un référentiel des menaces en matière de cybercriminalité : iOCTA[47] (Internet Organised Crime Threat Assessment).

La cybercriminalité inclut la cyber-délinquance, qui concerne des délits relativement bénins, mais dont les acteurs sont potentiellement très nombreux, notamment en raison du risque pénal peu élevé, mais surtout en raison du fait que ces acteurs ne sont pas forcément conscients du caractère illégal de leurs activités (exemple : non-respect des droits d'auteur). Dans ce contexte, le risque d'une cyber-délinquance généralisée est plus que jamais à considérer dans les années à venir.

[45] (Le piratage des voitures autonomes pourrait mener... au chaos routier, 2014)
[46] (Net Losses : Estimating the Global Cost of Cybercrime, 2014)
[47] (EC3 : the 2014 Internet Organised Crime Threat Assessment (iOCTA), 2014)

La lutte contre la cybercriminalité sera un enjeu majeur de la prochaine décennie, notamment par l'établissement d'une réglementation internationale, à défaut européenne, plus efficace qu'aujourd'hui. Les principales problématiques actuelles pour lesquelles il faudra trouver des contre-mesures d'ici à 2030 sont notamment :

- l'essor incontrôlé des monnaies virtuelles qui sont le support de transactions illégales (trafic de drogue, trafic d'armes, trafic humains). L'absence d'identification des utilisateurs génère un anonymat préjudiciable à la traçabilité des transactions ;
- l'incapacité à contrôler les réseaux privés d'échanges comme le Darknet (réseaux TOR), support de choix pour de nombreuses activités criminelles (trafic de drogue, trafic d'armes, proxénétisme, pédophilie) ;
- la prolifération des botnets, support à de nombreuses pratiques illégales comme les escroqueries via phishing par exemple ;
- la difficulté à protéger les données personnelles à l'échelle mondiale, notamment par le fait que ces informations sont exportées à l'étranger et donc hors de contrôle de la réglementation française (les données personnelles peuvent être utilisées à des fins criminelles telles que l'usurpation d'identité ; elles sont aussi utilisées pour réaliser de l'ingénierie sociale) ;
- le laxisme de certains pays en matière de cybercriminalité, notamment Africains ou Est-européens (exemple : la Roumanie), source de nombreux délits actuellement ;
- le développement des techniques « anti-forensique » permettant d'effacer les traces/preuves des délits ;
- la généralisation des techniques de chiffrement maitrisées par l'utilisateur final qui rendent de plus en plus difficiles les activités forensiques dans le cadre des enquêtes judiciaires ;
- l'impunité souvent constatée pour les auteurs de chantages et demandes de rançons, envers les entreprises, mais également de plus en plus les particuliers, principalement en raison du fait que ces auteurs agissent depuis l'étranger. A noter que les « ransomwares », en particulier ceux mettant en œuvre du chiffrement, constituent une problématique majeure. Les attaques ciblées initialement vers les entreprises ont tendance à se généraliser massivement vers les citoyens via des outils automatiques ;
- l'utilisation d'imprimantes 3D pour fabriquer des objets illégaux comme des armes à partir de fichiers téléchargés via Internet. (une problématique similaire existe déjà avec les plans et les recettes pour fabriquer des engins explosifs par exemple) ;
- le vol des terminaux mobiles (actuellement en pleine expansion), compte-tenu du rôle de plus en plus important et central de ces terminaux (paiement, données de santé, source d'authentification...). La lutte contre le vol et indirectement la protection des informations contenues dans ces terminaux vont constituer un enjeu majeur.

A horizon 2030, il faut s'attendre à une cybercriminalité de mieux en mieux structurée (crime organisé), rapide, évasive et pouvant provoquer des cyber-attaques massives. Certains délits vont particulièrement marquer la prochaine décennie :

- l'usurpation d'identité, dont les conséquences seront croissantes en raison de la numérisation massive des actes administratifs notamment. Le développement hétérogène de la délégation d'authentification par des grands acteurs du net (ex : Facebook, Google, Twitter, Microsoft …) va faire évoluer le risque actuel ;
- la fraude bancaire en raison de l'essor des transactions en ligne et des nouveaux moyens de paiement (paiement avec le terminal mobile, monnaies virtuelles) ;

- les jeux d'argent et les paris en ligne prohibés ;
- le rapt de données personnelles pouvant faire l'objet d'un véritable marchandage à grande échelle ;
- chantage et/ou demande de rançon envers des particuliers par rapports à leurs données personnelles et de plus en plus leur écosystème numérique. (exemple : paralysie d'une voiture connectée avec demande de rançon pour la débloquer) ;
- chantage et/ou demande de rançon envers les entreprises par rapport à leurs données et outils professionnels ;
- l'espionnage industriel, l'usurpation de propriétés intellectuelles (brevets).

Enfin, avec le développement de la e-sante, il est également possible d'imaginer des scénarios beaucoup plus graves comme une prise d'otage, ciblée ou massive, par rapport à la prise de contrôle à distance d'objets médicaux connectés[48] tels que des pompes à insuline, des pacemakers. Des scénarios similaires aussi graves, car impactant l'intégrité des personnes, ne sont pas non plus à exclure dans le domaine des transports (ex : voiture autoguidée, avions), des infrastructures industrielles (barrages, centrales nucléaires, usines chimiques …), notamment dans un contexte terroriste.

5.7. Atteinte aux personnes

En termes de sécurité, la différence fondamentale entre le cyberespace actuel et celui à horizon 2030 est l'impact sur les personnes. En effet, nous allons passer d'un monde ou les incidents de sécurité ont des impacts essentiellement économiques, sociaux, matériels à des impacts pouvant porter atteinte l'intégrité physique des personnes[49]. Cela sera en grande partie dû à la progression de l'Internet des objets dans des domaines d'activité critiques tels que la santé, l'énergie, les transports, l'industrie. La perte croissante du contrôle humain dans la maitrise des systèmes, catalysé par les solutions M2M, est également une nouvelle dimension majeure à prendre en compte.

Certaines applications seront particulièrement susceptibles d'être à l'origine d'atteinte grave aux personnes :

- les objets connectés « actifs » dans le domaine médical
- les voitures connectés et autoguidées (utilisable comme arme par destination)
- les moyens et les infrastructures de transport (avion, train)
- les industries SEVESO (chimie, nucléaire …)
- les fournisseurs d'énergie (gaz, électricité), notamment en période hivernale
- Les systèmes d'armes militaires

Des scénarios de prise d'otage et de provocation de panique à grande échelle ne sont pas exclure, par exemple des fausses alertes depuis des objets connectés, qui sollicitent les services de secours ou les forces de l'ordre (cambriolage, accident, incident médical…). Ce risque de phénomène de panique à grande échelle est réel car les informations sont véhiculées

[48] (Europol prédit une vague de cybercrimes par objets connectés, 2014)

[49] (Les spécialistes s'inquiètent sur la sécurité d'Internet: D'ici 2025, une cyber-attaque pourrait provoquer des morts, 2014)

de plus en plus rapidement et par forcement par des humains. En effet, les robots via le M2M prendront des décisions de plus en plus importantes.

5.8. Les enjeux de sécurité pour l'Internet des objets

Certains acteurs industriels historiques ressentent l'arrivée des objets connectés comme une source de risques car ils seront confrontés à une évolution rapide et soudaine des comportements de la part des usagers ainsi qu'à l'apparition de nouveaux compétiteurs adoptant des stratégies disruptives. Le domaine de la santé, ou plus globalement celui du bien-être, pourrait être cité comme exemple avancé des changements à venir. L'arrivée sur le marché de capteurs de données biométriques (physiologiques, médicales) à des prix particulièrement accessibles provoque des changements dans le comportement des personnes elles-mêmes mais aussi l'arrivée de nouveaux acteurs économiques jusqu'alors absents dans le domaine (exemple : Arrivée récente d'Apple dans le domaine du médical avec son application « Health » et sa plateforme « HealthKit »).

Sur le plan de la sécurité, les objets connectés ont aujourd'hui mauvaise presse[50] ; plusieurs raisons peuvent l'expliquer :

1) leur cycle de vie peut être très court et dans une logique économique ou la primeur est un enjeu marketing, la sécurité est souvent négligée ;
2) Certains objets, notamment grand public, doivent avoir un cout de fabrication extrêmement faible. En outre, ils doivent également être optimisés d'un point de vue performances et consommation énergétique. Les fonctions de sécurité, notamment basée sur la cryptographie, peuvent constituer un surcout important. Le développement de solutions de chiffrement optimisées pour le domaine de l'embarqué va constituer un enjeu important dans les années à venir[51]. La cryptographie asymétrique fondée sur les courbes elliptiques [52] (ECC : Elliptic Curve Cryptography) est particulièrement intéressante dans ce contexte au regard des avantages qu'elle présente d'un point de vue performances.

A plus long terme, les objets connectés vont poser des enjeux de sécurité majeurs, qui vont s'amplifier avec leur expansion :

1) Cela va accroitre les sources d'informations contenant des données personnelles, comme la géolocalisation ou les données biométriques par exemple.
2) Les objets connectés seront de plus en plus nombreux et potentiellement mal sécurisés, ce qui en fait une cible idéale pour mener des attaques par rebond, notamment de type DDOS par exemple.
3) La multitude d'objets connectés va poser des problèmes d'échelle :
    - il sera difficile pour chaque propriétaire de maitriser le parc d'objets sous sa responsabilité et de contrôler l'activité de ces objets. Cette problématique sera amplifiée par la miniaturisation de ces objets du fait des progrès à venir dans les domaines de l'intégration micro-électronique et de l'optimisation des batteries.

[50] (Les objets connectés, future cible des hackers, 2014)
[51] (Cryptographie et objets connectés font ils bon ménage ? , 2014)
[52] (Courbes elliptiques : un nouveau virage pour le chiffrement, 2011)

- l'identification et les solutions d'authentification actuelles seront probablement inadaptées (gestion des identifiants et des certificats, limitations technologiques, gestion des pannes, pertes et vols). Est que des dizaines de milliards d'objets vont devoir/pouvoir s'authentifier à horizon 2030 ?

4) Le besoin de partage pour l'accès aux objets (gestion des droits). Par exemple, un extincteur connecté doit être accessible par les équipes de maintenance, mais aussi potentiellement par tout individu pour son déclenchement.
5) La communication directe entre les machines induite par le M2M va engendrer une perte du contrôle humain.

En l'état actuel de la technologie et de l'absence ou de l'extrême jeunesse des standards dans le domaine, la sécurité des systèmes informatiques chargés de la collecte, du traitement et des communications au cœur des objets connectés est un challenge qui reste à adresser. En effet, les composants et systèmes mis en œuvre dans les objets connectés doivent être à la fois très peu couteux à produire et à maintenir tout en étant particulièrement économes en consommation énergétique. Cet environnement contraint en termes de ressources (puissance de calcul, mémoire et énergie très limitées) rends inadaptées un large éventail de mesures de sécurité communément utilisées par ailleurs dans le domaine des technologies de l'information. Les objets seront connectés directement ou de manière indirecte via le smartphone ou la Box Internet (« agrégateur d'objet »), ce qui déportera certaines problématiques de sécurité au niveau de ces équipements. Outre ces challenges liés à la nature même des systèmes informatiques présents dans les objets connectés, leur maintenance et leur supervision sont aussi des questions pour lesquelles les réponses restent à trouver.

5.9. La sécurité des systèmes industriels

A l'horizon 2030, les systèmes industriels de production (ou systèmes « SCADA »), déjà en voie de sortie de leur isolement, vont poursuivre leur intégration avec les SI d'entreprises, et devenir des cibles privilégiées des pirates : déni de service (arrêt ou dysfonctionnement de la production), extorsion, mais aussi subversion (par exemple : infection par un virus de produits électroniques grand public avant même leur commercialisation) deviendront des incidents courants.

Les milieux industriels ont intégré l'informatique moderne tardivement: ce n'est qu'en 1980 que les équipementiers industriels, accompagnés de la « society of Manufacturing Engineers » ont conçu le modèle CIM. Ce modèle en 5 couches décrit les fonctionnalités apportées par l'informatique depuis les capteurs/actionneurs, jusqu'à la planification globale de la production en passant par la supervision des chaines et ateliers de production.

Des initiatives plus récentes démontrent l'intérêt grandissant de l'informatique dans les environnements industriels. AT&T, Cisco, GE, IBM et Intel se sont associés pour créer un consortium dédié à ce que l'on appelle désormais l'Internet industriel[53] et qui vise à renforcer l'intégration entre les mondes physiques et virtuels. Aucun industriel européen n'est représenté dans ce nouveau consortium baptisé « Industrial Internet Consortium » (IIC). Certes, il s'agit là d'un consortium de plus dont on ne sait pas trop quel sera l'importance, mais c'est néanmoins le signe d'une évolution majeure. Fin 2013, GE avait lancé une première salve en annonçant 14

[53] (General Electric : INDUSTRIAL INTERNET - A European Perspective - Pushing the Boundaries of Minds and Machines, 2013)

nouvelles technologies « Predictivity » basées sur l'analytique et applicables aux secteurs de l'aéronautique, de l'industrie du pétrole et du gaz, des transports, de la santé et de l'énergie (GE lance une grande offensive dans le Big Data industriel). L'idée est simple : tous les équipements existants ou à venir dotés de capteurs pourront produire des données et seront source d'améliorations considérables dans de nombreux domaines.

De façon connexe, la sécurité informatique de ces systèmes a été tardivement prise en compte et les systèmes industriels présentent actuellement un très haut niveau de risque. Trois facteurs expliquent cette situation :

- la probabilité de réalisation d'une attaque est forte étant donné la faible culture sécurité et le fort degré de vulnérabilité de ces systèmes. Les industriels éprouvent actuellement de nombreuses difficultés pour mettre en œuvre des mesures efficaces et pérennes. Sur les années à venir, c'est tout le schéma de conception et d'exploitation des SI industriels qu'il faudra repenser pour aboutir sur des SI industriels sécurisés de manière efficace. En opposition aux SI de l'informatique de gestion, les SI industriels sont très fortement dépendants des matériels qu'ils pilotent et sont conçus pour des cycles de vie de longue durée (10 ans, 15 ans voir 25 ans et plus pour une centrale nucléaire par exemple). Cette approche implique des difficultés de maintenance car il est difficile d'assurer la pérennité des développements et des éditeurs de logiciel sur cette durée. De plus, la nécessaire conduite du changement permettant de faire évoluer les SI pour prendre en compte les mises à jour de sécurité est également complexe à mettre en œuvre car il s'agit bien souvent de systèmes de production continue avec des fenêtres de maintenance étroites et difficiles à planifier ;
- en face de ces systèmes vulnérables, les attaques deviennent de plus en plus sophistiquées. Elles ne sont plus le fait d'amateurs à la recherche de gloire, mais sont le fait de professionnels, qui agissent dans le but de s'élever contre des cibles politiques ou commerciales, sous la forme d'activisme, d'espionnage ou d'attaque gouvernementale. Les menaces persistantes avancées sont passées à un nouveau niveau d'attaques furtives et complexes, difficiles à détecter et encore moins faciles à bloquer. La pression économique actuelle et la forte concurrence menée entre industriels ne fera qu'accroitre cette tendance dans les années à venir.
- l'impact en cas d'attaque peut s'avérer dévastateur. Il s'agit en effet de systèmes en charge d'approvisionner les villes en énergie ou encore de gérer le transport routier, ferroviaire et naval. L'atteinte de ces systèmes est susceptible de causer des dommages environnementaux irréversibles, de paralyser complétement un pays et de porter directement atteinte à l'intégrité physique des personnes.

Deux exemples révélateurs permettent d'illustrer ces enjeux de sécurité :

- Sur le segment spécifique de l'automobile, le développement de la voiture connectée doit notamment permettre de réduire les couts de maintenance, de mieux gérer les parcs de véhicules des entreprises et d'améliorer la sécurité des biens et des personnes. C'est également un formidable espoir pour améliorer le trafic urbain avec l'avènement du V2I (Véhicule To Infrastructure). Un des buts de cette technologie vise à réduire les embouteillages des villes dont le cout actuel est estimé à plusieurs milliards d'euros de perte par an en France. Le V2V (Véhicule To Véhicule) est une autre technologie permettant la communication entre véhicules afin de signaler et d'anticiper, par exemple, un freinage d'urgence. On le voit ces technologies sont à la recherche de dispositifs améliorant la sécurité des personnes. Il serait dommage qu'un défaut de

sécurité informatique remette en cause les véritables progrès dans ce secteur. Pour ce faire, il faudra trouver des solutions de sécurité car les évènements de sécurité redoutés sont nombreux. Les plus basiques touchent l'image de marque des industriels en cas de dysfonctionnement d'un dispositif de sécurité local au véhicule (exemple : un virus se propage sur le système de divertissement embarqué). A une autre échelle ; les industriels redoutent également des attaques de cybercriminalité de grandes ampleurs qui pourraient par exemple immobiliser une série entière de véhicule. En face de ces enjeux, les investissements des constructeurs sur la sécurité informatique ne semblent actuellement pas à la hauteur. Dans un domaine hyperconcurrentiel, ils ne représentent aujourd'hui qu'un très faible pourcentage du cout de production d'un véhicule car ce type de préoccupation est pour le moment assez éloigné des clients finaux. Ceux-ci sont peu sensibilisés et seule une prise de conscience collective permettra d'améliorer durablement les choses.

- le secteur de l'énergie est également en pleine mutation. La transition énergétique actuelle s'appuie notamment sur la gestion des énergies renouvelables, la maitrise des consommations, la construction de bâtiments à énergie positive et sur bien d'autres sous-systèmes réputés comme étant intelligents. Le passage d'un système hyper centralisé à un système complétement distribué sur le territoire s'appuiera avant tout sur l'intelligence des nœuds du réseau. En outre, cette révolution implique une explosion des échanges de données afin de coordonner et d'autoréguler la production et la consommation. Les problématiques sous-jacentes sont multiples: comment garantir la confidentialité des données personnelles induites (ex : relevé de comptage) ? comment assurer l'intégrité, la robustesse et la résilience des compteurs, capteurs et nœuds de communication ? comment se prémunir d'une attaque sur un nœud de communication desservant tout un quartier ou région ?

En réaction aux difficultés rencontrées par les SI industriels, une première prise de conscience a d'abord été observée aux USA avec le NIST et la DHS par la mise en place d'initiatives pour lutter contre le risque systémique suite aux évènements du 11 septembre 2001. Des initiatives ont également été lancées en Europe par l'ANSSI en France, le BSI en Allemagne ou le CNPI au Royaume-Uni. Les initiatives européennes et outre-Atlantique sont une première réponse mais ces approches se focalisent avant tout sur les services essentiels de l'état en impliquant notamment les Opérateurs d'Infrastructure Vitale afin de prévenir les attaques de grande ampleur au niveau national. Au-delà de ces approches étatiques, les industriels commencent également à s'organiser dans une approche sectorielle avec la publication de référentiels de sécurité adaptés à des contextes précis. Dans le domaine des SmartGrid, on observe une approche verticale par domaine d'activité au niveau européen. Les électriciens sont les plus avancés, notamment sur les initiatives de compteurs électriques communicants, devant le secteur du gaz et eau plus en retard. Bien que la majeure partie des problématiques soit équivalente, les groupes de travail sont indépendants. Cette segmentation est déplorable, car une approche plus concertée permettrait de mieux optimiser les budgets alloués à ce domaine.

5.10. Limites des solutions de sécurité actuelles

5.10.1. Problématiques d'identification

Si les fournisseurs de services en ligne sont aujourd'hui confrontés à un problème de garantie de l'identité de leurs utilisateurs, leur crainte est que celui-ci se globalise en même temps que les objets connectés et les services en ligne, privés ou administratifs, se multiplient. Cette crainte se retrouve également du côté des utilisateurs : selon une étude du CSA[54], près des deux tiers (63%) des français pensent que le risque de criminalité identitaire est élevé. De la prise en compte de cette problématique au plus tôt dépend donc la confiance numérique accordée aux technologies de l'information à venir, et par conséquent leur essor.

L'obtention d'une confiance numérique suffisante pour permettre le maintien de la croissance de ce secteur nécessite la mise en œuvre et l'acceptation d'une autorité de confiance de l'identité, en charge d'appliquer les fonctions de sécurité fondamentales à l'ensemble des échanges électroniques : authentification, chiffrement, horodatage et signature. De plus, la multiplication des données d'identification, actuellement majoritairement un couple identifiant / mot de passe par service est de moins en moins gérable pour les utilisateurs, qui doivent de surcroît s'authentifier sur les objets connectés (domotique, « wearable-tech ») de plus en plus présents, renforçant le besoin de centralisation de la gestion de l'identité auprès d'une autorité.

La nature que doit avoir cette autorité demeure cependant difficile à discerner aujourd'hui. Elle peut être étatique : des certificats personnels sont gérés et distribués aux citoyens, par exemple à travers la Carte Nationale d'Identité Electronique (CNIE). Utilisés pour sécuriser les accès aux services publics dématérialisés et, potentiellement, le vote électronique, ces certificats peuvent également être exploités pas des services privés, l'état se portant alors garant de l'identité numérique des français. Cette vision étatique ne permet cependant pas de répondre de manière satisfaisante à l'ensemble des risques de fraude : le vol de certificat et la contrainte ne sont notamment pas adressés. Dans un tel scénario, les fournisseurs de service privés devront compléter l'authentification par des mécanismes de ré-identification : déployer des dispositifs d'analyse comportementale de leurs utilisateurs en exploitant les données dont ils disposent, sur le principe des faisceaux d'indices. Un comportement déviant des habitudes de l'utilisateur nécessitera une confirmation de l'identité, et pourra générer une alerte de risque de fraude ; une personne avec le terminal mobile d'un autre sera immédiatement détectée, tant seront nombreuses les anomalies avec son historique de données.

Le développement de méthodes d'analyse comportementale poussées permet d'imaginer un autre type d'autorité : l'autorité privée d'identité. En effet, la qualité du faisceau d'indices dépend essentiellement du type de données dont dispose le fournisseur, et en quelle quantité. Une exploitation pertinente de ces données par un acteur qui, par ses activités, en dispose en grand nombre et de toutes sortes, pourrait permettre de détecter de nombreux cas de fraude, dont l'usurpation d'identité, jusqu'à offrir un niveau de détection inégalable pour toute autre entité ne disposant pas de ces données. Les « résogiciels »[55], futures entreprises dominantes de notre système économique contrôlant en un système unifié les services, les réseaux et les terminaux, sont bien sûr les candidats privilégiés au statut d'autorité privée d'identité. Tout autre acteur pourra alors implémenter des mécanismes de ré-identification en exploitant les API publiées par l'autorité privée.

[54] (CSA - Les Français et la criminalité identitaire, 2012)
[55] (L'Internet industriel, Pierre BELLANGER, 2013)

Enfin, face à la possibilité d'une autorité étatique, qui ne peut pas garantir un niveau de sécurité optimal par manque de données et dont la portée est uniquement nationale (voire européenne), ou à la possibilité d'une autorité privée, très probablement de nationalité étrangère, une autorité souveraine peut trouver sa place. L'autorité souveraine, entreprise privée, nationale et partenaire de l'état, peut exploiter les données dont elle dispose à travers la commercialisation de ses services pour des mécanismes de ré-identification, qui pourront être proposés aux autres entités, l'état en particulier, à travers la publication d'API. L'autorité étant souveraine, nationale et agissant en partenariat avec l'état, le niveau de confiance numérique peut alors atteindre les exigences des utilisateurs comme des fournisseurs de services.

5.10.2. Cryptographie

Les progrès constants en matière de puissance de calcul (processeurs, calcul distribué) et l'efficacité des techniques de cryptanalyse ne sont pour l'heure pas de nature à remettre en cause les principes cryptographiques actuels. Les algorithmes utilisés sont en effet jugés comme très robustes vis-à-vis des attaques, qu'elles soient en cryptanalyse ou dites de « force brute », et ces algorithmes seront raisonnablement toujours fiables d'ici à 2030. Les faiblesses liées à l'utilisation des moyens de chiffrement cryptographique résident davantage dans les implémentations de ces algorithmes ainsi que leur cadre d'utilisation. Ainsi, les exploits qui auraient pu être réalisés par des organisations telles que la NSA américaine sont souvent issus de piégeage au niveau de l'implémentation logicielle des algorithmes cryptographiques[56], voir du contrôle d'organismes de certification X.509.

Pour garantir l'efficacité de la cryptographie, il est primordial de veiller à utiliser des clefs de taille suffisantes : post-2020, l'ANSSI recommande dans le cadre du RGS 2014[57], des tailles de clefs minimales : 128bits pour les algorithmes de chiffrement symétriques tels que AES, 2048bits pour les algorithmes de chiffrement asymétriques tels que RSA.

Le RGS 2014 de l'ANSSI présente également quelques projections temporelles qui évaluent les performances des méthodes de chiffrement symétriques et asymétriques à horizon 2050, en fonction des prévisions de croissance sur la puissance de calcul des machines (Loi de Moore) [La courbe rouge doit être prise en considération]:

[56] (Espionnage : pour casser les clefs de chiffrement, la NSA a dû "tricher", 2013)

[57] (ANSSI - Référentiel Général de Sécurité v2.0 - Annexe B1 - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, 2014)

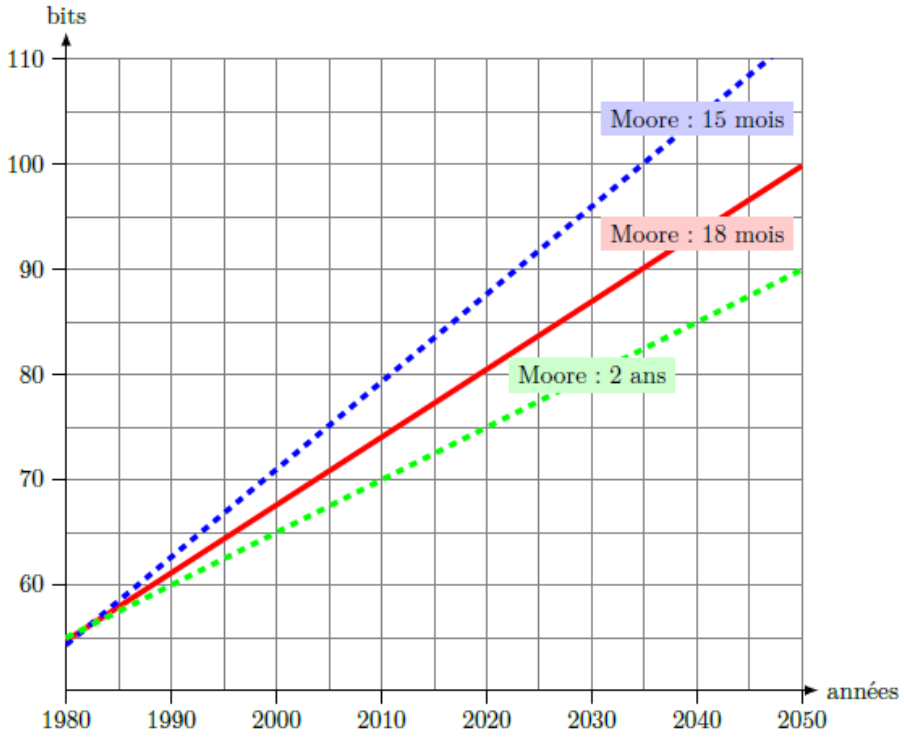

Figure 9 : Évolution des tailles de clés symétriques (source : RGS ANSSI 2014)

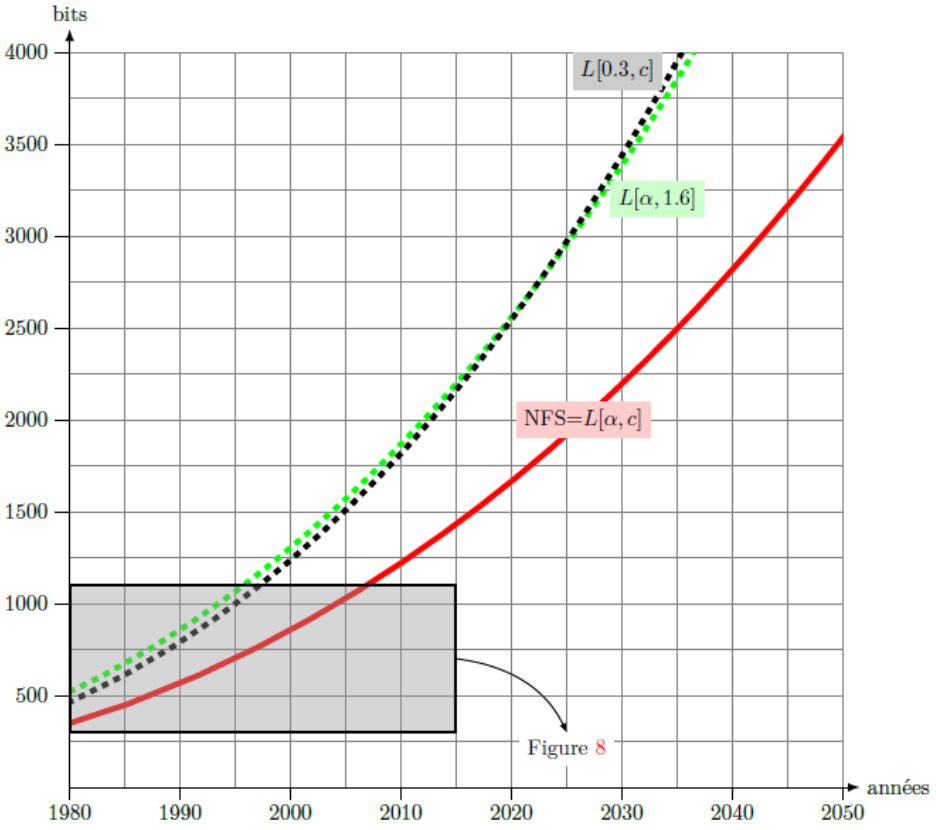

Figure 10 - Évolution des tailles de clés asymétriques (source : RGS ANSSI 2014)

Malgré quelques annonces médiatiques, notamment sur les capacités de la NSA[58], le calcul quantique[59] n'est aujourd'hui pas suffisamment mature ni performant pour remettre en cause l'efficacité de la cryptographie asymétrique actuelle. Toutefois, la recherche académique envisage déjà cette possibilité et travaille sur les algorithmes de chiffrement du futur sous le terme « Post-quantum cryptography »[60].

En matière de cryptographie, la qualité des générateurs d'aléas est également primordiale. Or, aujourd'hui, les générateurs utilisés pour les applications grand public n'offrent peut être pas toutes les garanties suffisantes. En effet, les industriels ne donnent pas beaucoup de détails sur les implémentations et les performances des générateurs qu'ils utilisent ou commercialisent.

5.10.3. Les autorités de certification (PKIX)

La sécurité des échanges sur Internet repose en grande partie sur la confiance accordée envers les autorités de certification X.509 (modèle PKIX). Ce modèle présente un gros défaut : le niveau de sécurité dépend de la capacité des utilisateurs à interpréter correctement les erreurs de certificats. Or une grande partie des utilisateurs d'Internet ne comprend pas le principe de certification et n'est pas conscient des risques que cela peut engendrer d'un point de vue sécurité.

D'autre part, ces dernières années, une crise de confiance est apparue envers les autorités de certification. En effet, la dynamique « low-cost » engagée pour fournir des certificats X.509 a abouti à une multiplication anarchique des AC rendant difficile, pour ne pas dire impossible, leur maitrise. Les navigateurs web actuels intègrent par défaut plusieurs centaines de certificats d'AC racine[61] (exemple : près de 1500 AC pour Firefox). Le principal risque est qu'une AC soit compromise[62] et de faire croire à tort aux utilisateurs que leur connexion est sécurisée. Plusieurs faits récents, avec des attaques de type MITM ont mis en évidence cette faiblesse du modèle PKIX :

- Attaques sur Windows Update, Yahoo, Skype, Facebook, Twitter en 2011 suite à la compromission de l'AC DigiNotar[63] ;
- Attaques sur Yahoo Mail, Hotmail, Gmail, Skype en 2011 suite à la compromission de l'AC Comodo[64].

Plusieurs améliorations ont été proposées pour réduire le risque de compromission de certificats : certificats à Validation Etendue (« EV certificate »), Public Key Pinning Extension for HTTP (draft IETF)[65], Trust on First Use (ToFU), Certificate Transparency (RFC6962), Certificate Authentication and Authorization (RFC5755). Toutefois le modèle demeure fragile car, outre l'hétérogénéité des solutions et le fait que leur efficacité technique reste à démontrer, la sécurité dépend de la vigilance des utilisateurs. La solution la plus efficace sera probablement la généralisation du mécanisme DANE (cf. §6.1.1).

[58] (La NSA veut créer un ordinateur quantique pour pouvoir tout décrypter, 2014)
[59] (Wikipedia - Calculateur quantique, 2014)
[60] (Wikipedia - Post-quantum cryptography, 2014)
[61] (AFNIC - Sécuriser les communications sur Internet de bout-en-bout avec le protocole DANE, 2013)
[62] (Certificats SSL frauduleux et piratage d'autorités de certification : décryptage, 2011)
[63] (Plus de 500 certificats SSL dérobés à une autorité de certification, 2011)
[64] (Des certificats SSL frauduleux de Comodo autorisent des attaques contre les Webmails, 2011)
[65] (Université Amsterdam - Public Key Pinning for TLS Using a Trust on First Use Model, 2013)

5.10.4. Les antivirus

Les antivirus sont de moins en moins performants pour détecter les menaces. En effet, plusieurs études récentes[66] montrent que l'efficacité des antivirus est en baisse constante, notamment face à des attaques de type APT ou AVT. Un dirigeant de Symantec pense même que les antivirus ne sont plus efficaces que contre 45% des menaces[67].

De manière plus générale, bien que son utilité ne soit totalement pas à remettre en cause d'ici à 2030, le principe de l'antivirus se heurte à certaines contraintes :

- cela nécessite une surveillance et une maintenance constante (moteur d'analyse, bases virales, traitement des alertes)
- un antivirus consomme des ressources, notamment dans les phases de mise à jour, ce qui le rend difficilement compatible avec certains objets connectés
- ils sont inefficaces sur des données chiffrées

Enfin, en raison des privilèges système dont ils disposent, les antivirus sont également ciblés par les malwares[68] afin d'outrepasser les droits d'accès au système censé être protégé.

5.10.5. Des protocoles obsolètes

Internet s'appuie aujourd'hui sur certains protocoles plutôt anciens (plus de 20 ans) et qui n'ont pas été conçus à l'origine pour assurer un niveau de sécurité en phase avec les enjeux actuels et futurs. Même si quelques évolutions ont été apportées pour améliorer la fiabilité et la sécurité de ces protocoles, ils seront probablement obsolètes à horizon 2030. Les principaux protocoles concernés sont :

- BGP4 (routage entre ISP) : détaillé au §5.12.4 ;
- DNS (résolution de noms de domaine) : détaillé au §5.12.5 ;
- NTP (synchronisation horaire) : notamment utilisé pour réaliser des attaques DDOS par amplification[69] ;
- SMTP (relais de mail) : encore utilisé à grande échelle, ce protocole véhicule les messages en clair. L'usage de l'extension STARTTLS[70] devrait être généralisé pour sécuriser les échanges de mails.

5.11. Essor des attaques ciblées

Le terme « attaque ciblée », aussi dénommé APT (Advanced Persistent Threat), désigne une forme particulière de menace informatique, dans laquelle l'attaquant cherche à pénétrer une cible en particulier (par opposition aux attaques massives et opportunistes), suivant des motivations spécifiques à sa cible – souvent, il s'agit d'espionnage – et disposant de moyens et de temps en conséquence.

En 2030, plusieurs tendances de l'informatique vont fortement influencer les attaques ciblées, en particulier :

[66] (L'antivirus, technologie à bout de souffle ?, 2012)
[67] (L'antivirus est mort, dit Symantec, 2014)
[68] (Des trous de sécurité trouvés dans 14 antivirus, 2014)
[69] (Attaque DDoS de 400 Gbits/s avec amplification NTP : terrifiante de simplicité, 2014)
[70] (IETF - SMTP Service Extension for Secure SMTP over Transport Layer Security , 2002)

- la généralisation des systèmes de fédération d'identité, un tiers de confiance devenant garant de l'identité de ses clients auprès de services tiers (sites web, e-marchands, voire entreprises), ces derniers renonçant à capter par leurs propres moyens l'identité de leurs utilisateurs ;
- l'informatisation quasi-totale des services (administrations, transports, santé…) et outils quotidiens (voitures, dispositifs médicaux personnels, lunettes, lentilles de contact, domotique, …) ;

Ces deux tendances combinées vont déplacer les attaques ciblées vers le vol d'identité ciblé : d'une part les tiers de confiance vont recevoir quantité de nouvelles attaques du fait de leur nouveau poids dans l'économie numérique ; et d'autre part, par rebond, les attaquants vont ainsi profiter des ressources affectées aux individus dont l'identité a été usurpée, y compris chez leur employeur.

Avec la révolution à venir de l'informatique quantique, portée notamment par les procédés de téléportation de l'information à l'aide de photons intriqués (procédé expérimenté par de nombreux établissements de recherche à l'heure actuelle, et en passe de devenir industrialisable), de nouvelles formes de portes dérobées verront le jour. A l'heure actuelle, les portes dérobées matérielles, permettant d'espionner à distance un équipement ou un ordinateur, requièrent toutes une connexion sortante afin de permettre une communication avec le malfaiteur : cette connexion est typiquement réalisée par voie réseau classique, sur le réseau de l'organisation affectée ; ou bien par voie radio, de sorte de pouvoir espionner un équipement ne disposant d'aucune connexion réseau. La détection et le blocage de ces « backdoors » sont certes difficiles, mais possibles (par examen du trafic réseau, par installation d'une cage de Faraday, …) ; mais l'informatique quantique va rendre quasi-impossible cette détection : en effet, aucun transfert de matière n'étant désormais nécessaire pour transmettre une information sur une longue distance, il ne sera plus pertinent d'observer les entrées-sorties électromagnétiques d'un système, et il va devenir impossible de garantir que ce système est réellement isolé et n'est pas en communication avec un autre système à l'autre bout du monde. Les portes dérobées quantiques ne pourront être décelées que grâce à un examen physique minutieux des composants électroniques de l'équipement avant son installation, capacité très coûteuse dont trop peu d'acteurs disposent.

5.12. Enjeux pour les opérateurs

Les opérateurs vont être confrontés à des enjeux de sécurité importants, notamment sur les thématiques suivantes :

- la transition IPv6
- les nouvelles menaces engendrées par la virtualisation des réseaux (NFV) et l'automatisation associée (SDN)
- le nouveau paysage de la téléphonie (fixe et mobile)
- les relations entre opérateurs et acteurs du net

5.12.1. Transition IPv6

La pénurie d'adresses globales IPv4 est devenue une réalité. La plupart des opérateurs ont dévoilé leur stratégie de migration vers IPv6, qui constitue la seule réponse durable à la pénurie d'adresses IPv4. Mais la migration vers IPv6 ne se fera pas en un jour, et la période de

transition caractéristique de la cohabitation des mondes IPv4 et IPv6 s'étalera vraisemblablement sur plusieurs décennies.

Du point de vue de la sécurité des infrastructures de communication, l'introduction progressive d'IPv6 dans les réseaux et services exploités et fournis par les opérateurs est de nature à amplifier les risques de failles sécuritaires ([RFC-4942], [RFC-6980]). En particulier :

- La capacité des composantes élémentaires d'une chaîne de service de communication (du terminal au serveur Web, en passant par les routeurs du réseau, le système d'information, les plates-formes de service, etc.) de traiter indifféremment le trafic IPv4 et le trafic IPv6 selon la nature du contenu auquel l'utilisateur souhaite accéder (architecture « double pile »), est de nature à accroître la surface d'attaque et à augmenter le nombre de failles de sécurité potentielles. De plus, comme le nombre d'adresses IPv6 pour un seul lien réseau est potentiellement plus important que pour IPv4, les sources de stockage nécessaires au bon fonctionnement d'IPv6 (e.g., caches) doivent impérativement avoir une taille adaptée et potentiellement des mécanismes de protection contre les attaques de type «cache flooding» [RFC6583]
- La généralisation d'ingénieries spécifiques destinées à garantir la continuité de services IPv4, c'est-à-dire la capacité à accéder à un contenu uniquement accessible en IPv4 depuis un terminal qui ne dispose que d'un préfixe IPv6), qui constituent autant de cibles supplémentaires.

Toutefois, la mise en place d'une politique de sécurité IPv6 n'est pas fonctionnellement différente de la mise en place d'une politique de sécurité IPv4. Il s'agit en substance :

- De *protéger les ressources réseaux* (routeurs) impliquées dans l'acheminement de trafic IPv6. Cela repose sur la mise en place de filtres adaptés à ce type de trafic, mais qui restent comparables aux filtres mis en place par des routeurs IPv4.
- De *protéger les sites des utilisateurs finaux* et les terminaux qu'ils utilisent pour accéder à Internet. Cela repose sur la mise en place de pare-feux IPv6 fonctionnellement comparables aux pare-feux IPv4. De même, la protection de sites hébergeant des Data Centers IPv6 repose notamment sur la mise en place de pare-feux et de zones démilitarisées (DMZ) adaptés aux caractéristiques du protocole IPv6.
- De *préserver tout ou partie de la confidentialité du trafic IPv6* susceptible d'être acheminé sur Internet. Cela repose notamment sur l'utilisation de techniques de chiffrement telles que celles mises en œuvre par la suite de protocoles IPSec (IP Secure) qui, en IPv6, fait l'objet d'un en-tête d'extension particulier et optionnel.
- *D'identifier, voire d'authentifier de manière fiable les interlocuteurs IPv6*, que ce soient les routeurs d'un réseau tiers avec lesquels des routes IPv6 sont échangées ou les utilisateurs d'un service fourni par l'opérateur (par exemple un service d'accès à Internet ou un service de réseau privé virtuel). Là encore, des techniques telles que la signature numérique de connexions TCP ou l'utilisation d'une mécanique AAA classique capable d'intégrer des informations d'identification caractéristiques du protocole IPv6 (par exemple, les attributs IPv6 utilisés par le protocole RADIUS, (RFC-6911) peuvent être mises en œuvre pour répondre à ce genre de besoin.

Le protocole IPv6 comporte néanmoins certaines fonctions spécifiques (auto-configuration, notamment) susceptibles d'être utilisées comme vecteurs d'attaque. Le protocole ICMPv6 ([RFC-4443]) définit une bibliothèque de messages particuliers qui impose des règles de filtrage adaptées : blocage des messages ICMPv6 identifiés par des Types non alloués ou

expérimentaux, restriction de la diffusion de certains messages ICMPv6 à l'environnement LAN du client (échanges des messages Neighbor Solmicitation et Neighbor Advertisement, *etc*.).

Le protocole IPv6 dispose également d'outils capables de fournir des garanties strictes quant à l'identifiant (e.g., adresse IPv6) d'un interlocuteur avec lequel un terminal est susceptible de dialoguer. C'est l'objet du protocole SeND (Secure Neighbor Discovery protocol, [RFC-3971]), qui repose sur l'utilisation d'adresses IPv6 générées crytographiquement [RFC-3972] et de certificats X.509 [RFC-6494], ces derniers étant compatibles et potentiellement liés avec une RPKI (cf. §6.1.2).

D'une façon générale, le protocole IPv6 dispose d'ores et déjà des outils adéquats pour mettre en place des politiques de sécurité adaptés aux besoins et aux environnements d'opérateurs. La période de transition introduit en effet des risques supplémentaires et notamment liés à la capacité d'utiliser le trafic IPv6 comme un vecteur d'attaque de terminaux IPv4, mais des solutions existent pour minimiser ces risques.

L'expérience opérationnelle acquise après les premières années d'exploitation de réseaux et services IPv6 par de nombreux opérateurs constitue en outre un atout majeur pour optimiser la gestion des failles sécuritaires caractéristiques de la période de transition.

A noter qu'IPv6 devrait simplifier la traçabilité des connexions par rapport à IPv4, en raison de la disparition de la translation d'adresse (NAT).

5.12.2. Virtualisation des réseaux (NFV et SDN)

La virtualisation et l'automatisation vont constituer une évolution majeure des réseaux opérateurs dans les années à venir, notamment en raison du niveau d'ouverture des fonctions de signalisation et de contrôle. Les deux grandes thématiques qui vont engendrer des enjeux de sécurité majeurs sont NFV et SDN.

Le NFV (Network Functions Virtualization) consiste à virtualiser les fonctions réseaux (et sécurité) sur des bases matérielles génériques. Des problèmes similaires à ceux existants dans le domaine de la virtualisation des serveurs sont à appréhender, en particulier :

- garantir le cloisonnement entre les différentes instances virtuelles de fonctions implantées sur une même base matérielle, en termes de confidentialité et d'intégrité. Une sécurisation de la couche de virtualisation préservant les performances, constituera un défi majeur dans les années à venir.
- garantir les performances de chaque instance et plus globalement la disponibilité dans un contexte de traitement en temps réel. Cette problématique de disponibilité est aujourd'hui un sujet de recherche important notamment pour les fonctions cœur de réseau (la virtualisation n'atteint pas les performances d'un matériel dédié basé sur des ASIC matériels).

Le SDN (Software-Defined Networking) a pour objectif de simplifier et d'automatiser la mise en œuvre et la gestion opérationnelle des réseaux pour les rendre plus dynamiques et évolutifs, notamment dans la gestion de la qualité de service. SDN sera notamment une pierre angulaire des futurs réseaux 5G.

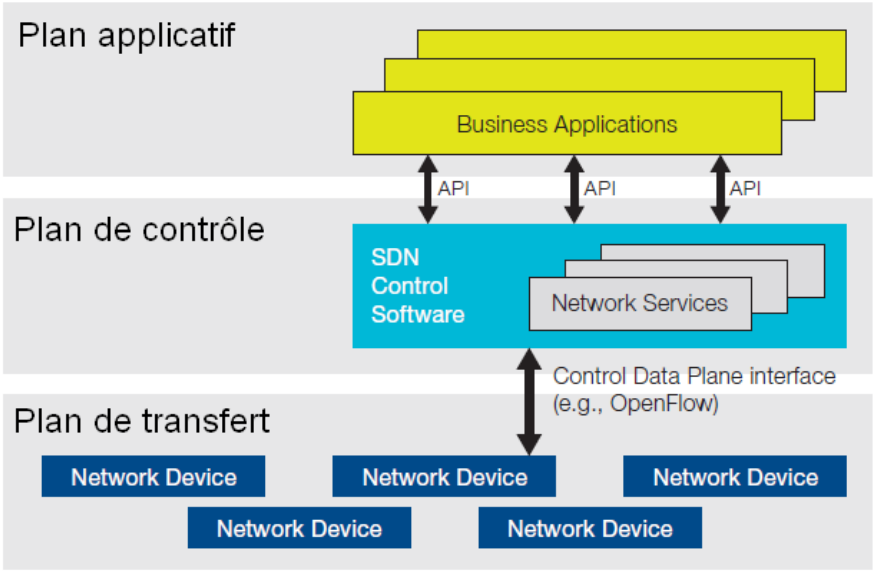

Figure 11 - modèle d'architecture SDN (approche initiale)

Dans le modèle SDN, les couches de contrôle et de gestion sont bien distinctes de la couche de transfert de données, ce qui est plutôt une bonne chose d'un point de vue sécurité. Toutefois, le protocole de communication entre ces deux couches (exemple : OpenFlow, NETCONF, I2RS) devient critique en termes de sécurité dans la mesure où il véhicule toute la configuration et toute l'intelligence du réseau. A l'heure actuelle, il est prévu de sécuriser ces échanges avec SSL/TLS. La disponibilité est aussi une problématique importante dans la mesure où ces échanges peuvent transiter avec les flux de trafic (in-band).

Un des objectifs du SDN est également l'ouverture d'interfaces (type API) vers des tiers externes pour la programmation dynamique du réseau, ce qui constitue un enjeu important en termes de sécurité ; surtout qu'à plus long terme, la finalité est d'obtenir une automatisation complète de bout-en-bout avec un concept de SDDC "Software Defined Data Center" mutualisant l'automatisation des fonctions réseaux et serveurs. La délivrance de la chaine de service va donc désormais reposer sur de multiples acteurs, créant des problématiques de définition des périmètres de responsabilité, de gestion des droits et d'établissement de processus. De manière générale, l'ouverture de la programmation/contrôle du réseau vers des partenaires (exemple : les opérateurs virtuels) va inévitablement engendrer des risques nouveaux.

Enfin, un des plus gros enjeux de sécurité de SDN sera probablement les garde-fous qu'il faudra mettre en place pour restreindre toute possibilité d'attaque massive sur les réseaux. En effet, l'automatisation et la centralisation simplifient et accélèrent la gestion au quotidien, mais en cas de compromission, cela décuple la puissance d'une cyberattaque avec une surface d'attaque qui n'aura d'égale que sa rapidité. D'autre part, il ne faut pas occulter le risque d'erreur humaine ou de panne, qui comme pour tout système virtualisé et automatisé, peut être à l'origine de disfonctionnements de grande ampleur. Dans ce contexte d'architecture centralisée et très « logicielle », les processus de mises à jour devront faire l'objet d'une attention toute particulière en raison des impacts potentiellement très graves.

A plus long terme, notamment à horizon 2030, le SDN va devenir de plus en plus intelligent et autonome ; cela va notamment ouvrir la porte à de nouvelles réponses en matière de sécurité en agissant directement au niveau des ressources réseaux. Le revers de la médaille à cette intelligence accrue, notamment en raison des évolutions à venir dans le domaine de l'intelligence artificielle, est le risque de perte de contrôle humain sur le réseau.

En termes de standardisation, il faut souligner l'initiative open source « opendaylight »[71] qui est soutenue par de nombreux équipementiers, malgré la réticence de certains leaders comme Cisco ou Huawei qui souhaitent conserver une maitrise du plan de contrôle dans leurs équipements. Toutefois, pour des raisons historiques et stratégiques, les standards de l'écosystème SDN/NFV demeurent très diversifiés. Les multiples implémentations des équipementiers sont pas conséquent plus difficile à maitriser sur le plan de la sécurité. Enfin, force est de constater que la sécurité n'est aujourd'hui pas une préoccupation majeure ; comme bien souvent, la priorité est davantage portée sur le fonctionnel et le positionnement stratégique sur le marché. Pour résumer, la virtualisation des réseaux est actuellement jugée immature sur le plan de la sécurité[72].

D'un point de vue global, la virtualisation des réseaux va poser des questions de fond qui ne sont pas que techniques:

- Quel sera le niveau de confiance accordé dans les équipements qui réalisent le traitement dans le plan de transfert/transport ? En effet, il y a des chances pour que les équipementiers historiques se concentrent sur les fonctions de contrôle (logiciel) et que les fonctions de traitement (cf. matériel) soient réalisées sur la base de composants génériques peu maitrisés sur le plan de la sécurité (matériels ODM en marque blanche) ;
- Quel sera le degré d'adhérence avec les équipementiers et fournisseurs ? Afin de pouvoir assurer une qualité de service et un contrôle des licences, il est fort probable que les modules logiciels et matériels en fonctionnement opérationnel soient de plus en plus interconnectés avec les plateformes des équipementiers ;
- Quel sera le rôle des états et des autorités gouvernementales sur le plan de la réglementation ? Aujourd'hui, les opérateurs de communications électroniques sont soumis à une réglementation spécifique[73], notamment concernant la confidentialité des communications. Une obligation de certification de certains composants employés dans une solution SDN/NFV (hyperviseurs, orchestrateurs) doit être envisagée.

Sur le plan de la recherche, il est intéressant de citer l'existence du projet REFLEXION (REsilient and FLEXible Infrastructure for Open Networking) mené par l'ANR. Il s'agit d'un projet industriel qui vise à étudier d'une part la robustesse et la flexibilité des architectures SDN et NFV, en particulier pour assurer les services critiques, et d'autre part la dynamique et l'efficacité des solutions d'exécution des fonctions réseaux virtualisées. Ce projet implique des acteurs majeurs du secteur des télécoms : Orange, Thales, 6Wind, L'Université Pierre et Marie Curie, l'Institut Telecom-ParisTech Normale Sup' Lyon et INRIA. Il a été labellisé début juillet 2014 pour une durée de 2 ans.

[71] (Opendaylight project, 2014)
[72] (Gartner - pour le SDN, la sécurité n'est pas prête, 2014)
[73] (Legifrance - Obligations des opérateurs, 2014)

Sur le premier axe, le projet REFLEXION considère les questions de diagnostic et de gestion de fautes pour NFV de manière à ce que les services restent assurées de manière sans couture et envisage des techniques de répartition afin d'accroitre la robustesse des plans de commande et de transport dans NFV. Le projet fournira également des méthodes de conception de services virtuels robustes prenant en compte des menaces dans l'architecture mise en place.

REFLEXION proposera des méthodes de métrologie nouvelles pour contrôler les fonctions réseaux virtualisées. Des techniques d'optimisation seront mises en œuvre pour réallouer des fonctions réseaux virtuelles de manière à satisfaire les contraintes de performance et de qualité d'expérience.

REFLEXION est un projet orienté NFV qui pourrait avoir un impact sur les normes en vigueur (ETSI NFV, ONF et IETF) ainsi que sur l'écosystème scientifique dans le domaine des réseaux du futur.

5.12.3. Réseaux mobiles 5G

Les réseaux mobiles actuels sont très hétérogènes tant au niveau des infrastructures que des terminaux. La tendance, amorcée avec les réseaux 4G, est de migrer vers des architectures « full-IP », notamment au niveau du cœur de réseau (architecture IMS[74]). Par nature, ce type d'architecture faisant appel à des protocoles ouverts (ex : SIP) est plus vulnérable en comparaison avec les architectures précédentes plus spécifiques et propriétaires (équipements, protocoles/infrastructures de transport type TDM ou ATM, compétences métiers). La connexion des contrôleurs radios LTE au cœur de réseaux est particulièrement critique et il faudra mettre en œuvre des solutions de sécurisation performantes avec le recours à de l'authentification forte par certificat (de tels standards existent déjà mais ne sont pas implémentés par les équipementiers). Il faudra également appréhender la phase de cohabitation et de transition entre les réseaux téléphoniques dédiés (c'est encore le cas avec la 4G qui se replie sur la 3G pour le service de téléphonie via le mécanisme « CS Fall Back ») et les futures architectures « full-IP » basée notamment sur la téléphonie VoLTE.

Sur le plan de la sécurité, l'accès au réseau mobile peut être considéré comme correctement sécurisé depuis le déploiement de la 3G (authentification mutuelle entre le terminal mobile et le réseau opérateur, chiffrement des flux de signalisation). La protection des flux de trafic (communications) est en revanche plus problématique sur le segment radio en raison de la disparité des normes et des produits. Le constat est qu'il existe de multiples algorithmes de chiffrement liés à l'évolution des technologies radio (A5/x, GEAx, UEAx, EEAx[75]) et qu'ils ne sont pas imposés par les normes. Les réseaux opérateurs proposent globalement des possibilités de chiffrement à l'état de l'art ; une négociation avec le terminal mobile permet de sélectionner un algorithme. Le problème est que le parc de terminaux mobiles est hétérogène pour des raisons historiques et économiques (effet achat « SIM only » avec terminal non fourni par l'opérateur) ; certains terminaux proposent des algorithmes connus comme étant vulnérables (ex : A5/1), voire parfois aucun algorithme de chiffrement, même en 4G ! (cf. note de l'ANSSI C&ESAR 2014)[76]. Il est important de noter qu'aujourd'hui, les capacités de chiffrement des communications ne constituent pas un critère de choix pour un terminal mobile et qu'en

[74] (Wikipedia - IP Multimedia Subsystem, 2013)
[75] (ETSI - Cellular encryption algorithms, 2014)
[76] (ANSSI - Analyse de la sécurité des modems des terminaux mobiles, 2014)

termes d'IHM, le niveau de sécurité des communications n'est pas affiché à l'utilisateur (bien que son affichage soit standardisé voir 3GPP TS 22.101).

Un enjeu majeur de la 5G va donc être de normaliser au niveau international, en particulier dans le domaine de la sécurité sur les fonctions d'authentification et de chiffrement sur le canal radio. Dans ce contexte, le chiffrement des communications VoLTE de bout en bout, est un axe d'étude important. Une des difficultés de la 5G sera d'assurer une rétrocompatibilité avec le parc de terminaux existants. Les enjeux de santé publique seront également à prendre en compte ; des pistes techniques sont ainsi actuellement étudiées pour limiter l'exposition et la consommation énergétique (principe de faisceau directif basé sur le retournement temporel par exemple). L'optimisation de l'énergie est un enjeu important de la 5G, notamment au regard de l'application aux objets connectés. A noter que cette technologie présenterait un intérêt dans le domaine militaire (augmentation de l'autonomie, discrétion radio).

Les objets connectés, notamment de type M2M, sont également à l'origine d'une évolution majeure qui pourrait avoir des répercussions importantes en matière de sécurité : le principe de SIM générique intégrée (« Embedded-SIM[77] ») configurable via le réseau radio par les opérateurs. La carte SIM pourra ainsi être activée à distance en OTA (« Over The Air »)[78] avec le profil d'abonnement de l'opérateur. Bien évidemment, cela pose la question de la sécurisation de cette activation à distance. A plus long terme, le concept de carte SIM virtuelle « Soft SIM »[79] est également envisagé. Une « soft SIM » est purement logicielle et ne repose sur aucun matériel dédié, ce qui laisse envisager des problématiques majeures notamment concernant l'intégrité des fonctions de sécurité. Ces évolutions à venir dans la gestion des abonnements mobiles font craindre une perte de contrôle partielle des opérateurs historiques via l'apparition d'opérateurs virtuels, notamment des nouveaux acteurs comme Apple ou Samsung. Ces opérateurs virtuels, potentiellement localisés à l'étranger, pourraient poser des soucis en termes de souveraineté, en particulier concernant les possibilités d'interception légale. Dans ce nouveau contexte, il faudra aussi veiller à ce que la fourniture d'un abonnement mobile respecte un processus qui garantit et répertorie l'identité des détenteurs, comme c'est déjà le cas avec les cartes SIM/USIM actuelles.

Plus globalement, l'écosystème relativement clos des réseaux mobiles va évoluer vers un écosystème ouvert avec deux tendances majeures (du fait de la guerre des prix) qui seront impactantes sur le plan de la sécurité :

- *La mutualisation des ressources en cœur de réseau* : les réseaux ne seront plus sous la gouvernance exclusive d'un opérateur. Le développement des opérateurs virtuels va engendrer de nouveaux processus et des problématiques de responsabilité.
- *L'externalisation voir la délocalisation de certaines activités* : cette tendance est déjà amorcée et elle va se renforcer, notamment pour des raisons économiques. Cela engendre une perte de maitrise des opérateurs historiques et donc des risques supplémentaires (gestion des partenaires et des sous-traitants)

[77] (GSMA - Remote SIM Provisioning for Machine to Machine, 2014)
[78] (Les opérateurs mobiles avalisent la spécification Embedded SIM dédiée au marché M2M, 2013)
[79] (Apple prêt à collaborer avec les opérateurs sur une mini carte SIM, 2012)

Enfin, il existe aujourd'hui un paradoxe entre le « business model » qui vise à offrir des prix toujours plus bas au consommateurs et des exigences de sécurité de plus en plus élevées, notamment de la part des organismes gouvernementaux. Un des enjeux dans les années à venir sera surement de concilier ces deux aspects, si possible dans un contexte européen.

Note : l'association GSMA regroupe une majorité d'acteurs industriels et opérateurs du secteur des télécoms. Elle dispose d'un groupe de travail « Fraud and Security »[80] dédié à sécurité dans les réseaux mobiles.

5.12.4. Faiblesses BGP

BGP4[81] est le protocole de routage mis en œuvre au sein d'Internet depuis 1995. Il a été bâti sur un principe de confiance réciproque de proche en proche entre l'ensemble des opérateurs constituant l'Internet ; cela explique en grande partie l'absence de sécurité dans l'implémentation initiale du protocole. Ce principe de confiance est aujourd'hui remis en cause, notamment en raison de la multiplicité des acteurs/opérateurs.

BGP a subi plusieurs évolutions depuis 1995 pour améliorer sa sécurité (mesures de protection, résilience) et ses performances (rapidité de convergence). Les mesures de sécurité actuellement implémentées sont toutefois insuffisantes dans le contexte actuel et à venir. BGP supporte IPv6 et il va encore perdurer pendant de nombreuses années pour assurer le routage au sein d'Internet. Compte-tenu de sa criticité vis-à-vis du fonctionnement global d'Internet, ce protocole doit faire l'objet d'une attention particulière sur le plan de la sécurité.

Les incidents de sécurité actuellement observés sur BGP sont de deux natures :

- *Les incidents consécutifs à une attaque volontaire.* Les attaques recensées impliquant BGP sont aujourd'hui peu nombreuses, mais elles sont probablement vouées à se développer dans les années à venir. L'attaque la plus importante en terme d'impact est de type MITM[82] ; elle consiste à dérouter discrètement le trafic Internet à des fins d'espionnage (exemple[83] : déroutage de trafic vers l'Islande et la Biélorussie en 2013). Il est aujourd'hui très difficile de se protéger face à ce type d'attaque. Les attaques en déni de service ne sont pas non plus à exclure dans les années à venir.
- *Les incidents involontaires d'origine accidentelle* consécutifs à une erreur de configuration ou à un Bug logiciel. Il s'agit pour le moment des cas les plus fréquemment observés, avec des impacts d'importance variable sur la disponibilité. On recense aujourd'hui près d'une dizaine d'incidents majeurs[84] ayant conduit à une prise de conscience et à des améliorations du protocole sur le plan de la sécurité, notamment en termes de résilience. Pour illustration, l'opérateur Orange enregistre chaque mois 2 erreurs de configuration BGP relatives à son préfixe 2.0.0.0 (les mesures implémentées permettent de détecter et d'éviter l'incident).

[80] (GSMA - Fraud & Security, 2014)
[81] (A Border Gateway Protocol 4 (BGP-4) - RFC4271, 2006)
[82] (Une énorme faille de l'Internet permet de détourner du trafic à volonté, 2013)
[83] (The New Threat: Targeted Internet Traffic Misdirection, 2013)
[84] (ANSSI - Influence des bonnes pratiques sur les incidents (§4), 2013)

Plusieurs améliorations ont permis d'améliorer la sécurité, mais le protocole BGP souffre d'une absence de fédération au niveau international qui pourrait permettre d'imposer certaines mesures de sécurité élémentaires, en particulier l'application des bonnes pratiques[85] pour l'implémentation et la configuration du protocole. La conséquence est que les évolutions sécurité ne sont pas appliquées de manière globale, ce qui nuit à l'ensemble de la sécurité du réseau.

Dans les années à venir, les défis à relever sur BGP seront les suivants :

- Il faut définir une autorité qualifiée capable d'imposer des mesures de sécurité à l'ensemble des acteurs/opérateurs du réseau Internet. Actuellement, un certain nombre d'opérateurs se cantonne à une implémentation minimaliste du protocole BGP en négligeant les aspects sécurité (pour des raisons financières ou historiques) ; les autres opérateurs sont contraints d'implémenter la sécurité sous un angle défensif.
- Il faut apporter des évolutions permettant de sécuriser davantage le protocole (gestion des paquets malformées, authentification et chiffrement dans les échanges). Des solutions sont évoquées au §6.1.2, mais il s'agit d'un exercice difficile car :
    - il faut appréhender l'historique et retenir des solutions qui permettent une migration progressive. En effet, il est impossible de réaliser une migration massive et rapide de l'ensemble des routeurs BGP d'Internet. Il s'agit là d'une des raisons majeures qui ont conduit à l'échec de certaines solutions basées sur la cryptographie notamment.
    - les solutions basées sur une infrastructure à clef publiques posent la question de l'autorité de certification et indirectement des problématiques de gouvernance et de souveraineté vis-à-vis d'Internet.
    - la mise en œuvre de solutions cryptographiques nécessite des ressources de calcul conséquentes que les routeurs actuels sont probablement incapables de fournir à grande échelle. Cela induit également des délais de traitement susceptibles d'altérer le niveau de résilience actuel.

En termes de dimensionnement, les données BGP sont en expansion permanente[86] (taille des tables de routage, nombre d'AS, nombres de préfixes échangés …). Mais les équipements actuels disposent de performances adaptées pour faire fonctionner le protocole à l'échelle d'Internet ; cela devrait toujours être le cas à horizon 2030.

[85] (BGP Best Practices, 2006)
[86] (BGP in 2013 - The Churn Report , 2014)

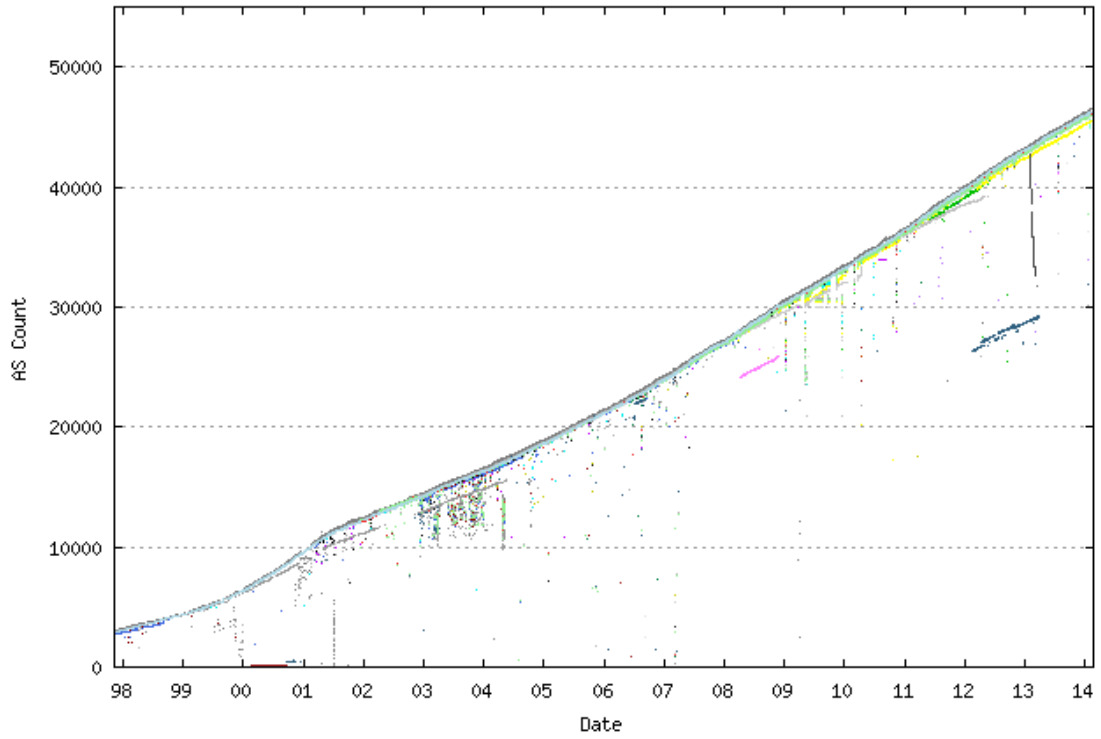

Figure 12 - nombre d'AS vus dans la table de routage BGP par les peers (source: http://www.potaroo.net)

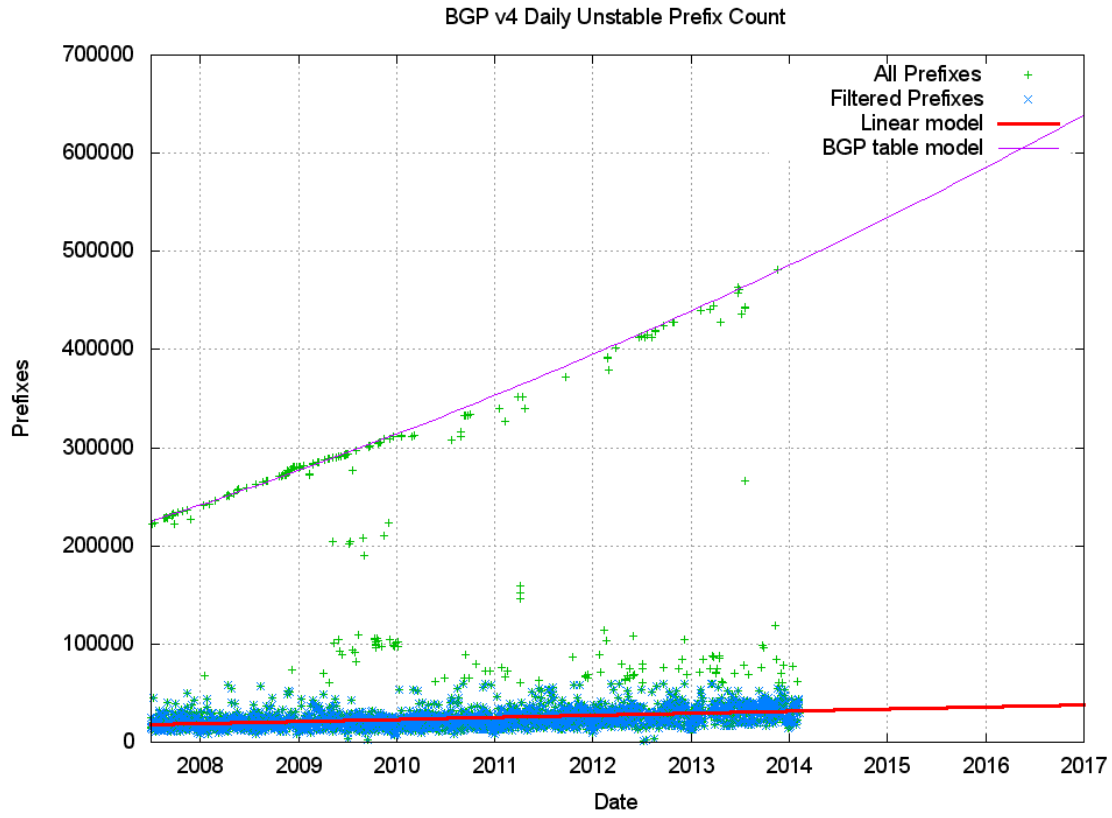

Figure 13 – mises à jour quotidiennes de préfixes vues par AS131072 (source: http://www.potaroo.net)

5.12.5. Faiblesses DNS

DNS est un service historique et incontournable de l'Internet. Malgré ses 30 années d'ancienneté, sa pérennité n'est pas à remettre en cause dans la prochaine décennie. Son rôle va devenir encore plus important avec la progression d'IPv6 ainsi que la multiplication des terminaux et des objets connectés. Concernant le modèle de déploiement, quelques alternatives ont été étudiées pour proposer un modèle « peer-to-peer » offrant une meilleure résilience et une certaine indépendance par rapport à la gouvernance opérée par les Etats-Unis; toutefois le modèle hiérarchique initial perdure et ce encore pour de nombreuses années.

Malgré les évolutions qu'il a subit depuis son lancement, le service DNS demeure complexe et souffre de plusieurs lacunes importantes sur le plan de la sécurité. Plusieurs travaux de synthèse existent sur les problématiques de sécurité du DNS et les contre-mesures possibles, en particulier sur le site de l'ANSSI[87] ainsi que celui de l'AFNIC[88] sous une forme plus vulgarisée. Un des problèmes majeurs actuels est notamment la prolifération des botnets qui exploitent les failles du service DNS pour bâtir des attaques de type DDoS (déni de service distribué)[89].

Le principal enjeu de la prochaine décennie sera probablement la généralisation du DNSSEC (cf. §6.1.1), mais ce nouveau protocole engendrera aussi de nouveaux problèmes. A l'instar de RPKI/BGPSEC, des problématiques de performances (ressources) et de gouvernance (autorité de certification) sont à appréhender.

Un autre enjeu important du DNS est la gouvernance du service qui aujourd'hui est essentiellement sous le contrôle des Etats-Unis. En effet, les TLD sont actuellement situés dans la zone « root » (13 serveurs racine) qui est sous gouvernance de l'ICANN, organisme dépendant du département du commerce des Etats-Unis. A noter toutefois que les Etats-Unis se sont récemment engagés dans une démarche d'ouverture afin que l'ICANN devienne un organisme international d'ici à 2015[90]; les autres états pourraient ainsi disposer d'un pouvoir de contrôle plus important qu'aujourd'hui.

5.12.6. Mutation de la téléphonie conventionnelle

Dans le domaine de la téléphonie, outre la généralisation des réseaux 5G, la principale évolution va probablement concerner l'émergence et la généralisation de la technologie WebRTC[91] qui fait actuellement l'objet d'un draft au niveau de l'IETF.

Le principe de WebRTC consiste à établir les communications téléphoniques ou visioconférences via des navigateurs web. De grands acteurs d'Internet (Google, Facebook, Skype) soutiennent ce standard, dont la principale conséquence risque d'être une perte de contrôle de la part des opérateurs historiques et de maitrise des acteurs de la part des gouvernements. Pour résumer, WebRTC peut être assimilé à une solution Skype normalisée, fonctionnant sur les terminaux fixes et mobiles ; WebRTC devrait ainsi favoriser la convergence fixe/mobile.

[87] (ANSSI CERT-FR - Du bon usage du DNS, 2008)
[88] (DNS : types d'attaques et techniques de sécurisation, 2009)
[89] (Attaques DNS : Connaître son ennemi, 2014)
[90] (ICANN : les USA renoncent au contrôle du DNS racine, 2014)
[91] (WebRTC : introduction et modèle de sécurité, 2014)

Les opérateurs historiques auront toujours un rôle à jouer pour assurer l'interface avec les réseaux téléphoniques conventionnels via des passerelles, mais plus le WebRTC va se généraliser et moins les opérateurs auront le contrôle de la téléphonie.

WebRTC pose plusieurs problèmes de sécurité d'ordre technique, mais également des problèmes de gouvernance, voire de souveraineté.

D'un point de vue technique, même si le standard n'est pas encore figé, les principales problématiques de sécurité à appréhender sont :

- la sécurisation des échanges entre le serveur et les clients, notamment en termes d'authentification côté client (En comparaison avec l'authentification forte mise en place dans les réseaux mobiles, un simple login/mot de passe est-il suffisant au regard des responsabilités juridiques en jeu ?)
- le niveau de sécurité du programme échangé entre le serveur et les clients (API JavaScript), notamment en termes d'intégrité.
- la protection des données à caractère privé (carnet d'adresse, listing des communications, géolocalisation)
- le partage des ressources locales (micro, camera) avec d'autres applications (cela risque de faciliter l'espionnage). La sécurité du logiciel de navigation utilisant l'API WebRTC est évidement un maillon essentiel.

La problématique de gouvernance est probablement la plus importante. En effet, les opérateurs historiques vont perdre la maitrise du service de téléphonie, et le chiffrement systématique des flux WebRTC en bout en bout par les utilisateurs ne va pas faciliter les éventuels contrôles que pourraient réaliser les opérateurs fournissant les accès réseau.

Cette problématique de gouvernance se pose également vis-à-vis de la capacité de l'état français à réaliser des interceptions de communication et à tracer les utilisateurs (relevés de communications), lors de réquisitions judiciaires notamment. En effet, il y a aujourd'hui une collaboration encadrée entre les opérateurs et l'état dans ce domaine et l'ouverture d'un abonnement (ligne téléphonique) fait l'objet d'un processus sécurisé pour garantir l'identité des utilisateurs/clients. Le WebRTC risque de favoriser l'anonymat et l'impossibilité de pouvoir écouter et tracer les communications. Cette problématique de gouvernance et de maitrise étatique est déjà d'actualité avec la société Skype, ce qui ne manque pas créer certaines tensions avec l'ARCEP (Autorité de Régulation des Communications Electroniques et des Postes)[92]. Cette problématique impactant la souveraineté peut être considérée comme relativement mineure pour le moment, mais à plus long terme, cela risque d'être un enjeu majeur vis-à-vis de la capacité de l'état Français à imposer son autorité, dans un contexte où les géants du web sont surpuissants. La question de fond qui va se poser est : comment caractérise-t-on un opérateur et quelles sont ses prérogatives vis-à-vis des autorités ?

Plus largement, les possibilités de réquisitions judiciaires sur le contenu des appareils de téléphonie mobile vont devenir problématiques. Par exemple, Apple a récemment annoncé que même avec une commission rogatoire, la société n'a plus la capacité technique de fournir aux autorités les données stockées sur ses appareils à partir de l'IOS8 si l'utilisateur a utilisé un code de chiffrement[93] ; ce positionnement faisant suite aux affaires Snowden ayant montré une facilité de certains états à accéder à des données personnelles via les infrastructures de télécommunications des opérateurs en dehors d'actions cadrées par la loi du pays.

[92] (SKYPE refuse de se déclarer en tant qu'opérateur, 2013)

[93] (Apple Can't And Won't Provide Access To iPhone Data To Authorities, Even With A Warrant, 2014)

5.12.7. Montée en puissance des OTT et du CDN

La montée en puissance des fournisseurs de contenus (OTT) et des réseaux CDN est déjà d'actualité. Cette tendance va se poursuivre dans la prochaine décennie avec le risque de voir les opérateurs historiques cantonnés à de simples fournisseurs de ressources réseau.

Comme pour la téléphonie, la principale évolution sera de voir les acteurs conventionnels dans les domaines de la télévision et de la diffusion vidéo remplacés par de nouveaux acteurs du web (les OTT).

Sur le plan technique, la principale problématique de sécurité est que les CDN s'incrustent de plus en plus dans les infrastructures des opérateurs, ce qui pose un problème de confiance, notamment en raison de la mutualisation croissante des ressources (cf. la virtualisation des réseaux). En outre, ces services de CDN, deviennent des maillons importants entre les fournisseurs de services et les utilisateurs finaux ; ainsi, des acteurs comme Akamai vont continuer de croitre pour devenir incontournables. Se pose alors la question de la confiance que l'on peut avoir dans ces opérateurs CDN, notamment en raison du fait qu'ils voient passer une très grande partie du trafic Internet.

La diffusion télévisuelle pourrait ainsi être beaucoup exposée qu'actuellement à des risques de piraterie, notamment envers les chaines d'état.

Mais le principal enjeu de sécurité va surtout être concentré sur la maitrise de la diffusion des contenus, par les opérateurs, mais aussi par les états. En France, la diffusion audiovisuelle est actuellement réglementée et régulée par des organismes tels que le CSA. Cette réglementation, qui est appliquée par les opérateurs conventionnels, permet de censurer, de protéger les mineurs, de financer la culture française, d'imposer un minimum de programmes audiovisuels Français, de contrôler les droits d'auteur… La prise de contrôle de la diffusion de contenus par les OTT du net pourrait remettre en cause ce modèle et réduire à l'impuissance les organismes de régulation et contrôle actuels comme CSA, notamment pour les raisons suivantes :

1) Le fait que les fournisseurs de contenus sont et seront localisés à l'étranger, dans des pays où la réglementation leur est favorable, fiscalement, juridiquement et « culturellement ». Par exemple, le fournisseur Netflix, qui a des ambitions sur le marché Français, s'est implanté au Luxembourg puis au Pays Bas pour échapper à la fiscalité Française[94].

2) Les flux sont de plus en plus chiffrés (SSL/TLS), ce qui rend impuissant les opérateurs ou les états en matière de contrôle, notamment sur les contenus. Cette problématique est amplifiée par le fait que la législation Française interdit aux opérateurs de réaliser des analyses en profondeur (DPI) sur les flux réseau.

Dans le nouveau paysage audiovisuel qui se dessine, la protection des mineurs, des droits d'auteur, de l'exception culturelle française, seront des enjeux majeurs. La problématique fiscale, engendrant une concurrence déloyale envers les acteurs historiques, doit également être appréhendée.

[94] (Netflix quitte le Luxembourg et s'installera aux Pays-Bas en 2015, 2014)

5.12.8. Le nouvel écosystème des opérateurs

Incontestablement, les opérateurs et leur écosystème subissent actuellement une transformation majeure qui devrait se poursuivre dans les années à venir. Les principaux changements concernent :

- L'évolution de leur métier historique d'opérateur de télécommunications ; les services et les contenus prennent désormais une place de plus en plus importante
- Les rapports de force avec les fournisseurs de services et de contenus (notamment les OTT via les CDN)
- L'ouverture à la concurrence sur le plan national et international qui, outre les enjeux économiques, a engendré une crise de confiance entre les opérateurs en raison de leurs différences de maturité, notamment sur le plan de la sécurité
- La mutualisation de certaines ressources entre différents opérateurs (voire certains partenaires). Cela va se renforcer avec la virtualisation des réseaux.
- La logique économique « low-cost » primant sur la logique de service public

Ce nouveau contexte actuel et à venir a plusieurs conséquences majeures sur le plan de la sécurité:

1) La logique économique du moins-disant est préjudiciable à la sécurité, surtout lorsque les réglementations diffèrent selon les pays. Par exemple, l'IETF préconise aujourd'hui une liste de bonnes pratiques sécurité applicables aux opérateurs dans le cadre du groupe de travail OPSEC[95] (contrôle des adresses IP, sécurisation BGP et DNS). Or ce ne sont que des préconisations qui n'ont pas un caractère obligatoire ; la conséquence est que certains opérateurs ne les appliquent pas pour des raisons de coût (matériels, personnels). Or Internet est une communauté ou tous les acteurs devraient appliquer les mêmes règles pour bénéficier d'un certain niveau de confiance sur le plan de la sécurité. Il faut garder à l'esprit que la sécurité aura toujours un coût et que cela est incompatible avec la logique économique actuelle.

2) Le nombre croissant d'opérateurs, notamment les opérateurs virtuels, engendrent une complexité qui ne favorise pas la maitrise sécurité du réseau Internet. Cela est particulièrement vrai pour le continent Africain où il existe de nombreux petits opérateurs locaux.

3) L'accès physique et logique aux ressources des opérateurs, notamment au niveau des Datacenters devient de plus en plus difficile à maitriser. En effet, nous passons d'une situation avec un opérateur unique et une gouvernance maitrisée à une situation où doivent cohabiter différents opérateurs, des partenaires (ex : CDN Akamai), des info-gérants/équipementiers en outsourcing, des sous-traitants. Toute cette complexité est préjudiciable à la sécurité, notamment vis-à-vis de la résilience globale du réseau. Cette problématique est aujourd'hui d'actualité sur le continent africain par exemple, mais elle va se généraliser, notamment en Europe.

[95] (IETF Opsec Working Group, 2004)

4) Le partage des ressources physiques et radio et les relations entre opérateurs seront un enjeu important dans les années à venir. Or aujourd'hui, les protocoles de signalisation, de routage et de contrôle (ex : protocole BGP, téléphonie IP) n'offrent pas tous une garantie suffisante en termes de sécurité dans ce nouveau contexte.

Enfin, l'augmentation constante des terminaux et du trafic, notamment avec le développement des objets connectés, engendre une massivité de l'Internet qui pourrait remettre en cause la capacité des opérateurs à maitriser le réseau, en particulier en termes de sécurité. La surveillance et l'investigation devront probablement faire appel à de nouvelles techniques basée sur le concept de Big Data par exemple.

5.12.9. Les dénis de service (DOS / DDOS)

Les dénis de services peuvent avoir différentes origines : disfonctionnement logiciel, erreur de configuration, attaque volontaire. Les attaques en déni de service, notamment de type distribuées, risquent de se développer dans les années à venir, notamment en raison de la multiplication des terminaux mobiles et des objets connectés[96], susceptibles d'être utilisés en rebond par des botnets. L'augmentation de débit sur les futurs réseaux mobiles (cf. la 5G) va également amplifier la puissance des DOS. A noter que de nouveaux impacts, tels que l'atteinte aux batteries des terminaux mobiles et objets connectés sont envisagés.

La fourniture de services DOS/DDOS constitue aujourd'hui un véritable business de dimension internationale[97] pour lequel il faudra apporter une réponse technique et juridique efficace dans années à venir. Les opérateurs auront un rôle important à jouer dans la prévention et la réaction face à ce type d'attaque. Or aujourd'hui, il existe des freins qui empêchent les opérateurs de mettre en œuvre des mesures permettant de lutter contre les dénis de service :

- Le premier concerne la réglementation française qui interdit certaines actions/réactions comme l'analyse en profondeur des paquets (DPI) ainsi que les réponses offensives. Il est toutefois important de noter que les analyses DPI sont de plus en plus difficile à réaliser en raison de la tendance croissante du chiffrement des flux utilisateur ;
- Le second est que des contrôles élémentaires de sécurité ne sont pas réalisés de manière systématique par tous les opérateurs. En effet, il existe une forme d'individualisme de la part de certains opérateurs, lesquels n'appliquent pas les bonnes pratiques recommandées par l'IETF comme la BCP38[98] par exemple. Cette mesure qui consiste à contrôler les adresses IP sources des abonnés permettrait de lutter efficacement contre le DOS et le DDOS, moyennant le fait que tous les opérateurs jouent le jeu. La problématique est telle que le CERT a émis un rappel en 2013[99]. Sans obligation, les opérateurs ont une logique économique et ne travaillent pas pour la gloire. Cette situation perdurera probablement en 2030 ce qui fragilise la sécurité de l'Internet.

[96] (DDoS et smartphones : rien ne sera plus jamais comme avant, 2014)
[97] (Sécurité informatique : ces nouveaux dangers qui guettent nos entreprises, 2013)
[98] (BCP 38 - Network Ingress Filtering : Defeating Denial of Service Attacks which employ IP Source Address Spoofing, 2000)
[99] (Alert (TA13-088A) - DNS Amplification Attacks, 2013)

5.13. La résilience d'Internet

Le réseau mondial est constitué d'un ensemble de nœuds (routeurs) interconnectés par des liaisons nationales, continentales et transcontinentales, en particulier des câbles sous-marins.

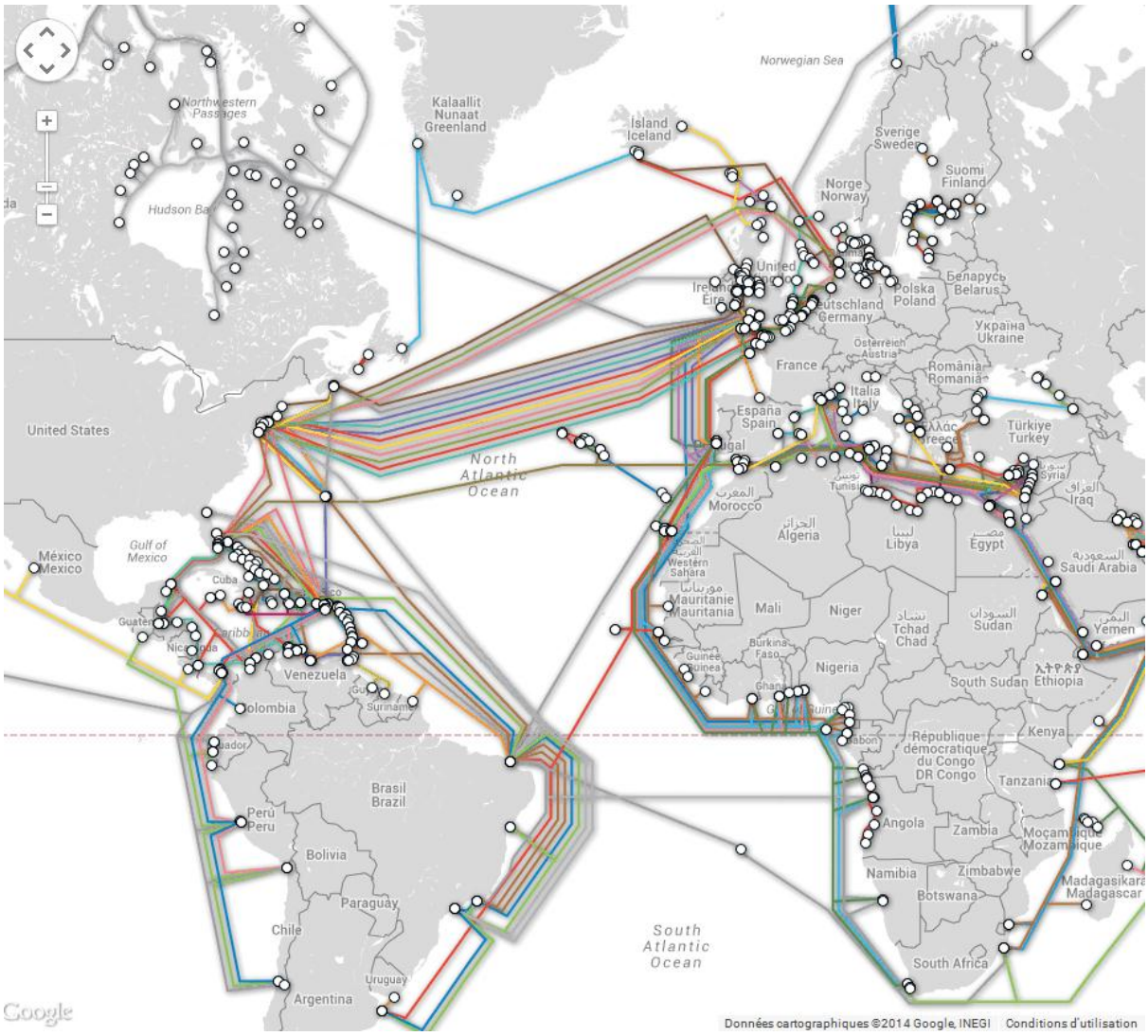

Figure 14 - Câbles sous-marins transcontinentaux (source www.cablemap.info[100])

Le réseau Internet et les protocoles sous-jacents ont été élaborés pour offrir un niveau de résilience élevé (routage dynamique, protocoles adaptatifs). Toutefois, l'augmentation des flux internationaux, notamment entre l'Europe et les Etats-Unis vont nécessiter d'être plus vigilant face aux vulnérabilités des interconnexions névralgiques de l'Internet, en particulier face à des attaques physiques ciblées sur des liens ou des nœuds critiques du réseau (exemple : les liens transatlantiques, les IXP[101] interconnectant les POP Internet des opérateurs).

[100] (Submarine Cable Map, 2014)
[101] (Wikipedia - Internet Exchange Point, 2014)

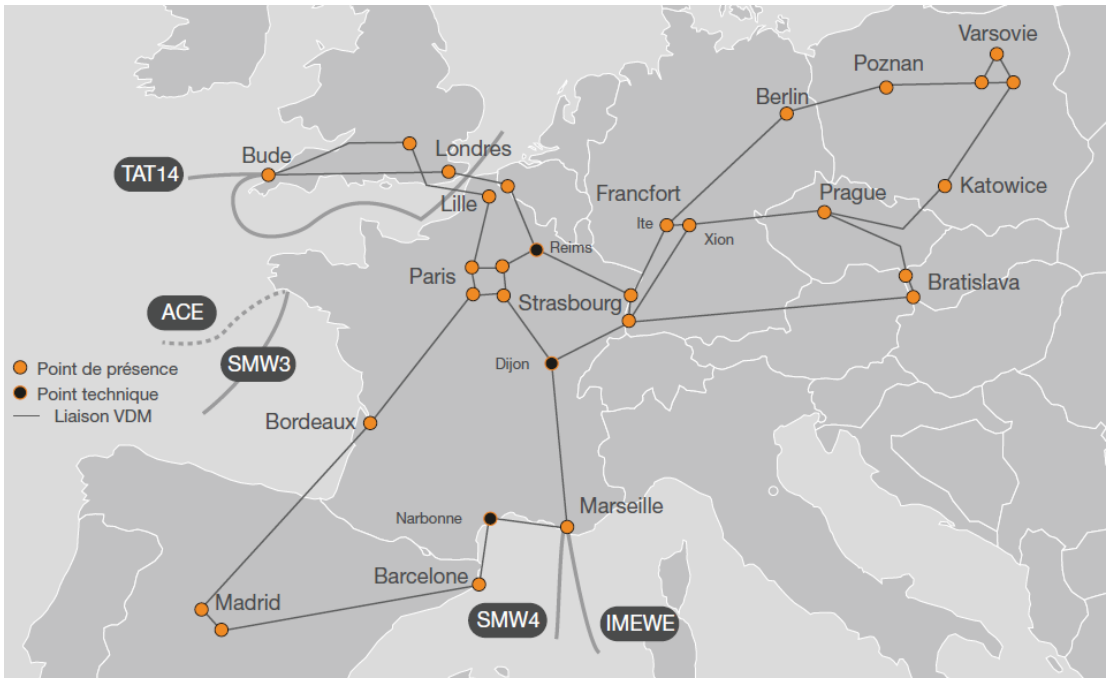

Figure 15 – Orange : Réseau Express Européen (REE)

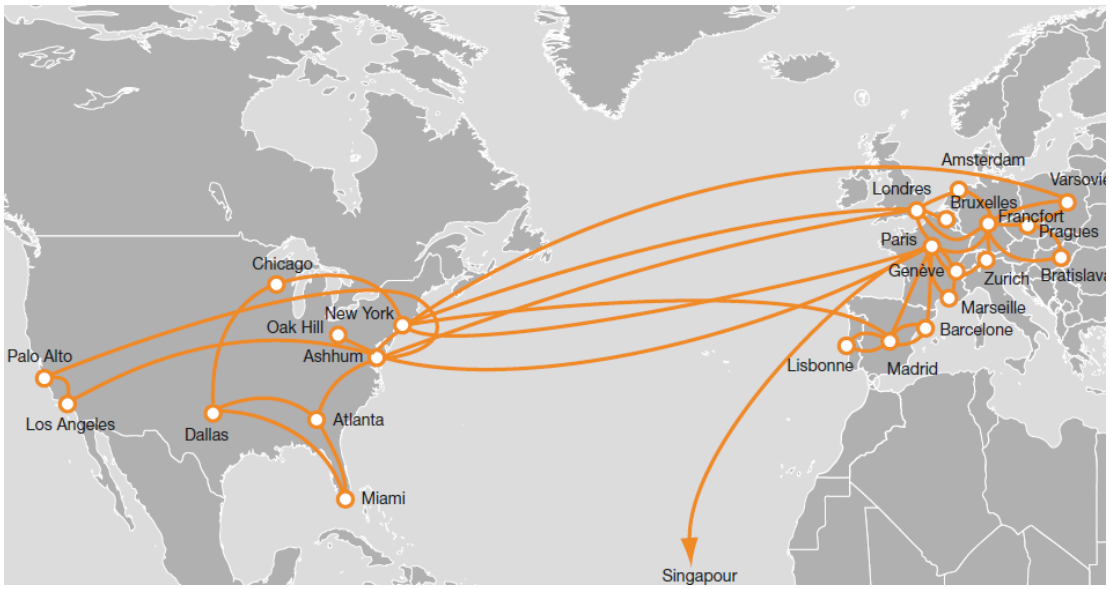

Figure 16 - Orange : réseau Open Transit Internet (OTI)

L'ouverture du marché des télécoms et le recours croissant à la sous-traitance constituent aussi des éléments importants à prendre en compte. En effet, cela va complexifier la problématique de sécurité d'accès aux ressources mutualisés (accès physique aux locaux techniques, aux Datacenter) avec des risques d'atteinte involontaires ou malveillantes aux infrastructures.

Remarque : aux États-Unis, il existe un groupe de travail « Communications Security, Reliability and Interoperability Council's »[102] (CSRIC) dédié à la sécurité et la résilience des systèmes de télécommunications, notamment face des grandes catastrophes.

5.14. Nouveaux types d'infrastructures réseaux

Le continent Africain est actuellement un laboratoire pour la mise au point de réseaux communautaires basé sur le Wifi, le LTE et des suites de protocoles permettant de constituer des réseaux Ad-hoc efficaces, avec le soutien de grandes sociétés comme Google par exemple. Des réseaux communautaires, basés sur le partage de ressources wifi, existent déjà en France, mais la composante Ad-hoc permettant une couverture beaucoup plus étendue demeure encore très marginale. Fort du retour d'expérience dans les pays émergents, il est possible dans les années à venir de voir se développer de manière significative des réseaux communautaires Ad-hoc en France, engendrant des difficultés de régulation et une perte de contrôle étatique. En effet, par nature, les réseaux communautaires ne sont la propriété de personne et il est donc impossible d'identifier formellement des responsabilités, notamment sur le plan juridique. Ce type de réseaux pourrait facilement devenir le support d'activités illégales sur le territoire national.

En termes d'infrastructure, il faut aussi considérer les grands acteurs du net qui ambitionnent de développer leurs propres infrastructure réseau (exemple : le projet d'Internet par satellite de Google[103]). L'objectif affiché est d'offrir un accès Internet aux populations non desservies actuellement, notamment dans les pays émergents. Il s'agit d'un marché de masse avec des tarifs d'abonnement pouvant être divisés par 10 voire 100 par rapport aux tarifs constatés actuellement dans les pays développés. Ce type de réseau, basé sur un modèle économique « low cost », pourrait aussi trouver un large écho dans les pays développés, ce qui pose quelques problématiques importantes :

- Quel va être le niveau de maitrise et de contrôle d'un pays comme la France, face à une infrastructure réseau localisée dans l'espace extra-atmosphérique, donc dans une zone internationale ou la France ne peut faire valoir sa souveraineté ? En effet, sachant qu'il sera extrêmement difficile de contrôler les terminaux utilisateurs, seules les stations sol d'accueil détermineront, à priori, la réglementation applicable en fonction de leur localisation
- Comment appliquer le principe de neutralité du net à un acteur qui est à la fois opérateur et fournisseur de services ? La maitrise totale du bout-en-bout par un acteur unique est-elle une bonne chose sur le plan concurrentiel notamment ?
- Quel sera le niveau de sécurité de ces réseaux ? Sachant que ce type d'infrastructure favorise les risques d'interception de communications.

[102] (The Communications Security, Reliability and Interoperability Council, 2014)
[103] (Google veut tisser un réseau de satellites pour l'Internet pour tous, 2014)

5.15. Surveillance du cyberespace

5.15.1. Les activités légales (surveillance étatique)

Les activités légales de surveillance menées par l'état français ont pour objectif :

- d'assurer la sécurité des citoyens en faisant respecter le droit français dans le cadre de réquisitions judiciaires
- d'assurer la sécurité et la souveraineté de l'état (protection contre le terrorisme, protection du patrimoine industriel, prévention de la criminalité organisée, lutte contre la fraude fiscale …) dans le cadre de procédures administratives

Ces activités sont des activités d'interception et d'écoute réalisées au sein du cyberespace (communications, échanges de données, transactions, données stockées…). Elles sont aujourd'hui réalisées via des organismes spécialisés avec la collaboration des opérateurs et des acteurs du cyberespace opérant sur le territoire national.

A horizon 2030, certaines problématiques majeures vont apparaitre ou être s'amplifiées :

1) La généralisation du chiffrement des flux transitant dans le cyberespace et des données stockées va rendre de plus en plus difficile les interceptions et les réquisitions sur le plan technique. En effet, les services fournis depuis des serveurs situés à l'étranger, notamment les services de Cloud, n'ont pas d'obligation légale de fournir les données confidentielles de leurs utilisateurs. Ces éléments peuvent être exigés directement auprès de l'utilisateur (clé de chiffrement, identifiant/mot de passe), mais il peut très bien refuser et cela empêche en outre les surveillances « discrètes ».

2) La mutation à venir dans le domaine de la téléphonie (nouveaux protocoles, délocalisation des serveurs de contrôle à l'étranger, chiffrement de bout en bout des communications, perte de maitrise des opérateurs historiques) avec des technologies telles que WebRTC risque de rendre inopérants les processus et les systèmes d'interceptions légales actuellement mis en place.

3) Les réseaux privés d'échanges comme TOR, base de l'Internet clandestin (« Darknet ») et largement utilisé à des fins criminelles, sont impossibles à surveiller. Officiellement, même la NSA américaine n'y parviendrait pas avec les moyens techniques et juridiques actuellement disponibles[104]. La seule parade actuelle consiste à infiltrer ces réseaux en se faisant passer pour un utilisateur lambda.

4) Pour assurer la sécurité des citoyens et de la nation, l'état Français pourrait être amené à imposer de nouveaux dispositifs et une nouvelle réglementation (exemple : installation d'un mouchard dans les terminaux, obligations de déposer de manière préalable les clés de chiffrement ou les identifiants auprès d'un organisme étatique,...). Cela pourrait être mal perçu par une partie de la population avec le sentiment d'un état « Big Brother » pouvant générer des risques de révoltes sociales. La liberté du réseau

[104] (Darknet, un internet clandestin à portée de clics, 2013)

Internet, la protection de la vie privée, le droit à l'anonymat, demeurent un enjeu sociétal majeur qui peut aller à l'encontre de la sécurité.

De manière générale, les partenaires historiques que sont les opérateurs auront un rôle à jouer de moins en moins important dans les activités de surveillance étatique du fait des évolutions technologiques à venir dans le cyberespace.

5.15.2. Les activités illégales (détournement d'information)

Les détournements d'informations et la surveillance du cyberespace à grande échelle de la part de certains états, en particulier les Etats-Unis, défraient régulièrement la chronique[105]. Des programmes d'interceptions massives ont ainsi été mis œuvre et ils perdureront probablement encore pendant de nombreuses années, mais avec des moyens et des méthodes différentes.

La première méthode d'interception consiste à capturer les flux réseau. Cette méthode est particulièrement adaptée lorsque les flux réseau sont en clair. Si l'on considère que certains états sont aptes à craquer facilement les algorithmes cryptographiques utilisés sur Internet, cette méthode reste pleinement valable. Les sources d'interception sont multiples :

- La capture de flux sur les réseaux sans-fils est historiquement la plus utilisée. Cela concerne les accès Wifi public, les accès par satellite, mais aussi les réseaux de téléphonie mobile (exemple : le projet AURORAGOLD [106] de la NSA) sur lesquels les fonctionnalités d'authentification et de chiffrement sont peu performantes. A l'avenir, il faut espérer que les évolutions apportées par la 5G permettront de combler ces lacunes de sécurité.
- La capture de flux sur les fibres-optiques : des techniques d'écoute sur le média physique existent[107] ; toutefois les conditions de réalisation sous-entendent l'accès aux infrastructures. Il est beaucoup plus aisé d'opérer en réalisant des dérivations (« port mirroring ») directement au niveau des équipements de commutation, surtout lorsque le trafic transite par un pays à l'origine ou complice de la cyber-surveillance[108]. Ce risque va augmenter et évoluer dans les années à venir en raison de la multiplication des acteurs (équipementiers, sous-traitants, partenaires) qui accèdent de manière plus ou moins contrôlée aux datacenters des opérateurs, notamment dans les pays émergents.
- Le protocole BGP peut être victime d'une attaque MITM ayant pour but de rediriger de manière transparente le trafic vers un AS au sein duquel les flux seront interceptés. Ce scénario, même s'il s'est déjà produit, demeure le moins probable. (cf. §5.12.4)

La seconde méthode d'interception, consiste à compromettre les serveurs et les terminaux utilisateurs afin de collecter, de manière active ou passive, des données, avec le gros avantage qu'à ce niveau, les données sont généralement peu ou pas chiffrées. Les techniques d'interception et de collecte de données s'appuient sur plusieurs vecteurs :

[105] (List of government mass surveillance projects, 2014)
[106] (Operation Auroragold - How the NSA Hacks Cellphone Networks Worldwide, 2014)
[107] (Un appareil qui intercepte les informations transitant via la fibre optique, 2012)
[108] (Les câbles sous-marins, clé de voûte de la cybersurveillance, 2013)

- Infection des serveurs et des terminaux avec des malwares (vol de données, atteinte à la confidentialité). Les objets connectés seront un vecteur important dans les années à venir, car mal sécurisés par conception.
- Piégeage à la source de logiciels voire de matériels (puces silicium) pour capturer des données et rediriger du trafic. Certains équipements cœur de réseaux d'origine américaine ou chinoise peuvent aussi être concernés.

Enfin, une troisième méthode peut désormais être identifiée, c'est la collecte passive des données via les services en mode Cloud mis à disposition des utilisateurs (documents bureautiques, photos/vidéos, données de géolocalisation, données personnels, activité sur Internet…). La tendance croissante à l'utilisation des solutions orientée Cloud (applications SaaS, stockage en ligne, solutions IaaS) concernent beaucoup les particuliers, notamment vis-à-vis de leurs données personnelles, mais de plus en plus les entreprises avec parfois un risque de fuite de leur patrimoine industriel. Cette exportation massive d'informations vers les Datacenter des grands acteurs d'Internet situés à l'étranger (GAFA[109] : Google, Apple, Facebook, Amazon) va s'amplifier dans la prochaine décennie. Outre le fait que ces sociétés imposent une centralisation des services et des données, elles généralisent le chiffrement des flux, même pour des usages qui ne le requiert pas à priori (exemple : moteur de recherche Google, visionnage de vidéo Youtube). La finalité recherchée est bien de collecter massivement des informations hors des territoires nationaux, tout en s'assurant que des tiers (opérateurs, états) ne puissent effectuer aucun contrôle quant à leur contenu.

5.16. La mutation de certains grands domaines sectoriels

5.16.1. La e-éducation

D'ici à 2030, il faut s'attendre à une évolution, voire révolution, dans le domaine de l'éduction. Les initiatives actuelles comme le MOOC (Massive Open Online Course) sont un avant-gout de ce qui se prépare. Cela va permettre un accès beaucoup plus étendu à l'enseignement, notamment dans des domaines spécialisés, pour toute une partie de la population, pourvu qu'elle soit connectée à Internet. L'enseignement à distance pourrait prendre une place prépondérante avec des examens réalisés en ligne. Les principaux risques que cela pourrait engendrer sont bien évidemment les risques de fraude aux examens, mais également une forme d'isolement social ou encore une « unicité « de pensée et une baisse de la diversité intellectuelle.

5.16.2. La e-santé

Le domaine de l'e-santé va probablement connaitre une expansion très importante d'ici à 2030, générant des problématiques sécurité relatives au secret médical et à la protection des données personnelles, mais également d'atteinte aux personnes. Les hôpitaux, accompagné par le programme « Hopital numérique »[110], sont directement concernés.

[109] (G.A.F.A. l'acronyme d'un quatuor qui accapare notre existence, 2014)
[110] (Le programme hôpital numérique, 2014)

Les principales évolutions à anticiper sont les suivantes :

1) La numérisation de l'ensemble de la filière médicale (déjà amorcée aujourd'hui). Cela concerne par exemple le carnet de santé électronique, les dossiers et actes médicaux, les résultats d'examens (ex : radiographies, analyses sanguines), les prescriptions médicales, le cycle de paiement et de remboursement. Les problématiques de protection du secret médical et des données personnelles sont évidentes, mais cela ne doit pas occulter d'autres risques qui pourraient prendre de l'ampleur comme la corruption (volontaire ou involontaire) d'une prescription de médicaments dans une ordonnance ou encore la fraude aux systèmes de santé. La disponibilité des données à caractère médical peut également s'avérer très critique dans des situations d'urgence (accès aux antécédents médicaux, résultats d'examens, dosages médicamenteux)

2) Les objets connectés appliqués à la santé et les applications M2M. En permettant un contrôle et une surveillance continue, la médecine connectée dispose de réels arguments pour s'imposer au plus grand nombre, offrant au patient un confort et une qualité de vie accrus. Déjà présente pour des pathologies chroniques nécessitant une adaptation de traitement et un suivi régulier, la médecine connectée vise à se développer pour des spécialités de plus en plus pointues, avec toujours la même optique : accroître la simplicité d'utilisation du matériel médical et permettre au patient d'améliorer la prise en charge de sa pathologie[111]. Le diabète, les défaillances cardiaques et l'apnée du sommeil sont actuellement les trois pathologies qui, aujourd'hui, disposent de solutions de surveillance à distance les plus abouties et utilisées ; demain les applications seront étendues à d'autres maladies chroniques et surtout, elles fonctionneront dans un mode « actif » via l'utilisation de nano-dispositifs médicaux, notamment pour l'administration de médicaments. La liste de solutions d'e-médecine connectée est vaste :
   - *Pompe à insuline connectée*[112]
   - *Pacemaker et défibrillateur connectés*[113]
   - *Puce contraceptive Microchips*[114]
   - *Pillcam* : une petite pilule qui, une fois ingérée par un patient, se pilote à distance par le médecin pour pouvoir explorer les tréfonds du corps humain, ainsi que les lentilles connectées de Google (en cours de développement) qui intègrent de la réalité augmentée et récupèrent des données de santé via le fil lacrymal, comme le taux de glucose ou de glycémie
   - *STM3* : Une solution à base de capteurs qui permet à un médecin de récolter et traiter les données de son patient, à distance et en temps réel.
   - *Transwatch* : Une montre connectée d'urgence médicale qui s'active d'une simple pression sur un bouton.
   - *Air Liquide Healthcare* : Une solution pour le suivi à distance des patients souffrant d'apnée du sommeil.
   - *Keynae* : Différents objets connectés aux applications diverses, comme le suivi de patients atteints de diabète, d'hypertension, ou encore souffrant de maladies chroniques

[111] (M2M et e-Santé : la médecine de demain, 2013)
[112] (Hack de pompe à insuline, 2011)
[113] (Un patient israélien reçoit un nouveau pacemaker « connecté », 2014)
[114] (La pilule du futur sera une puce contraceptive... télécommandée !, 2014)

- *e-pilulier* : Destiné aux patients nécessitant des prises de médicaments journalières, ce pilulier permet le tri et la distribution automatisée de ces médicaments. Les pilules sont ensachées par le pharmacien, qui se base sur les traitements prescrits par le médecin, puis placées dans le pilulier. A une heure donnée, le patient peut alors récupérer et prendre ses médicaments. En cas de non-prise du sachet, le pilulier se bloque et le médecin est alerté.
- *Mimo* : body connecté pour les bébés. Il permet de surveiller l'état de santé des nouveaux nés à distance[115].

Le risque principal de cette médecine connectée est évidemment la prise de contrôle à distance par un cybercriminel, pouvant aboutir à des situations de prise d'otage voire, dans un cas extrême, tuer le patient qui est équipé de ces objets[116] (pompe à insuline, pacemaker). D'autres scénarios graves peuvent également être imaginés, comme générer des situations de paniques par l'envoi de fausses informations (exemple : saturer les services d'urgence en simulant des accidents cardiovasculaires sur un grand nombre d'individus ou en déclenchant des systèmes d'alertes personnels)

3) La médecine en ligne dont les principaux atouts sont la rapidité, la simplicité va de développer. Elle pourra s'appuyer sur la numérisation de la filière médicale et l'Internet des objets médicaux. D'un point de vue sécurité, des problématiques de responsabilité juridique vont de poser ainsi que probablement des problèmes de confiance dans la relation médecin/patient.

4) Les actes médicaux à distance (chirurgie notamment) via des appareils chirurgicaux connectés seront probablement mis au point et utilisé à grande échelle en 2030. La sureté de fonctionnement sera la principale préoccupation d'un point de vue sécurité.

5) Le développement des prothèses bioniques sera probablement une révolution majeure dans la prochaine décennie

Note : La maîtrise d'ouvrage opérationnelle des systèmes d'information de santé a été réorganisée avec la création de l'ASIP Santé, agence chargée d'élaborer les grands référentiels d'interopérabilité et de sécurité des systèmes d'information de santé[117].

5.16.3. Le secteur bancaire

Le secteur des banques et assurances est actuellement en pleine mutation et cette tendance va se poursuivre. Les changements majeurs concernent :

1) La généralisation de la banque en ligne avec des applications de plus en plus critiques d'un point de vue sécurité. Cela permet notamment une ouverture sur le marché mondial, engendrant une concurrence plus importante qu'actuellement, et donc potentiellement préjudiciable à la sécurité. Cela laisse entrevoir des impacts importants en cas de cyberattaque (ciblée ou à grande échelle) sur le plan

[115] (Mimo connecte votre bébé, 2014)
[116] (Le défibrillateur de Dick Cheney modifié par crainte d'un assassinat par piratage, 2013)
[117] (France numérique 2012-2020 / Bilan et Perspectives, MINEFI, 2011)

économique. Des cas de cyberattaque se sont déjà produits, avec des effets, certes, limités[118]. Les systèmes de paiement traditionnels sont également touchés en raison de leur interconnexion croissante au cyberespace[119]. Une réglementation nationale ou européenne imposant l'utilisation de certificats clients (token, CNIE) constituerait une avancée significative sur le plan de la sécurité.

2) Le développement de nouveaux moyens de paiement, en particulier le m-paiement avec les mobiles qui expose davantage les utilisateurs à des problèmes de sécurité (vol ou perte du terminal par exemple). En effet, beaucoup de solutions de m-paiement actuelles pèchent au niveau de l'authentification des utilisateurs.

3) L'essor des monnaies virtuelles (aussi appelée crypto-monnaies) comme le Bitcoin qui échappent à tout contrôle bancaire et gouvernemental. Ces monnaies étant conçues par nature pour échapper à la fiscalité et garantir l'anonymat de leurs utilisateurs, elles sont largement utilisées pour des activés illégales et criminelles (trafic de drogues, d'armes, proxénétisme, blanchiment d'argent, financement du terrorisme). En outre, ces monnaies sont essentiellement basées sur une confiance communautaire sans garants (états, banques centrales). L'effondrement d'une e-money est donc possible et pourrait avoir des conséquences graves sur le plan économique et social[120]. Le rapprochement entre certains acteurs bancaires institutionnels (exemple : Paypal avec le Bitcoin[121]) peut également faire craindre l'apparition de nouveaux risques.

Cette digitalisation et cette connectivité toujours accrue du domaine bancaire permettent d'envisager des scénarios très pessimistes. Une atteinte à l'intégrité et à la disponibilité des données pourrait générer une crise bancaire à l'échelle mondiale avec des impacts sociaux potentiellement très graves. Un cas récent[122], avec des impacts toutefois modérés, constitue déjà une alerte à considérer très sérieusement.

A noter que les cyberattaques vont également constituer un risque de plus en plus important vis-à-vis du cours boursier des grandes entreprises[123], avec des conséquences économiques et sociales majeures.

Enfin, sur le plan pénal, il est important de noter qu'aujourd'hui, il moins risqué pour un criminel de « braquer » une banque ou un particulier de manière « numérique » que physiquement. Une réflexion sur la pénalisation de tels actes sera un enjeu important de la prochaine décennie.

[118] (HSBC visée par des hackers « justiciers », 2012)
[119] (Après Target : un nouveau malware cible les lignes de caisses, 2014)
[120] (Les limites des Bitcoins, 2014)
[121] (PayPal et Ebay répondent à Apple Pay avec le BitCoin, 2014)
[122] (Le hack géant de la banque JPMorgan Chase a touché 76 millions de clients, 2014)
[123] (Alerte aux cyberattaques sur les marchés, 2014)

5.17. Enjeux économiques et sociaux

5.17.1. Cyberdépendance des entreprises

Internet est devenu aujourd'hui incontournable pour de nombreuses entreprises françaises, notamment les grandes entreprises et les PME. Cette tendance devrait se poursuivre avec une extension aux plus petites entreprises. Cette connectivité au cyberspace va devenir aussi vitale que l'accès à l'électricité et la résilience du cyberespace pour les entreprises sera un défi majeur dans les années à venir. La problématique d'e-réputation va également devenir cruciale pour toutes les entreprises.

Le e-commerce devrait progresser pour probablement devenir le principal canal de consommation, notamment dans le domaine alimentaire et il faut peut-être s'attendre à un déclin spectaculaire et rapide du modèle des centres commerciaux qui règnent actuellement, ce qui pourrait générer de graves mouvements sociaux. De manière plus générale, la concurrence entre les entreprises va être exacerbée, notamment sur le plan international, ce qui pourrait générer des tensions majeures sur le plan national et international, notamment en raison de l'inégalité des régimes fiscaux et des niveaux de vie.

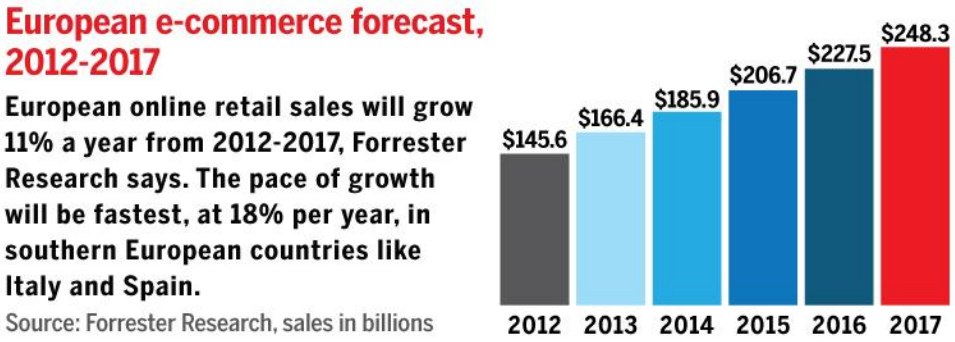

Figure 17 - projection de croissance sur le e-commerce en Europe (source : Forester)

Le télétravail, aujourd'hui peu développé pour des raisons culturelles, va probablement connaître un essor important d'ici à 2030, ce qui va accroitre le risque d'espionnage industriel, notamment au niveau des PME et TPE qui ont peu de moyens pour se défendre.

La progression du BYOD[124] semble aussi inéluctable, ce qui risque d'amplifier des problèmes déjà connus :

- des problèmes de sécurité « techniques » liés à la cohabitation d'applications personnelles et professionnelles
- des problèmes de protection des données personnelles et plus largement de la vie privée, notamment vis à vis de l'employeur
- des problèmes psycho-sociaux engendrés par la non-déconnexion de la sphère professionnelle

[124] (CNIL Innovation et Prospective : Intimité et vie privée du travailleur connecté : BYOD, capteurs, sécurité, 2014)

5.17.2. Cyberdépendance des citoyens

Les citoyens deviennent chaque jour de plus dépendant du cyberespace, et cet état de fait est parfois subi pour une partie de la population. Internet est utilisé au quotidien, de manière directe ou indirecte (cf. les objets connectés) et les applications sont de plus en plus nombreuses : e-commerce, relations sociales, médias, divertissement, santé, formalités administratives … A noter aussi la difficulté croissante pour se « déconnecter » de la sphère professionnelle avec le développement du BYOD par exemple. Des phénomènes d'addiction sont par ailleurs constatées dans certains domaines : les réseaux sociaux, les jeux vidéo en ligne, les jeux d'argent en ligne, la pornographie.

En très peu de temps de nombreuses maladies nouvelles sont apparues et de plus en plus de phénomènes psychologiques ont été associés aux pratiques Internet : pathologies affectives (anxieuses et dépressives), troubles de la conduite et de la personnalité et affections associées (névroses : évitement, phobies…, mais aussi psychoses). A horizon 2030, il faut s'attendre à une généralisation massive de ces maladies ou troubles du comportement.

En France, l'hôpital de Marmottan s'est spécialisé dans certaines de ces addictions et pathologies dites « sans drogue » et souvent comorbides :

- *l'impossibilité de se déconnecter* : travail, maison, même devant la télévision, en mangeant sur le canapé ou au lit, les objets connectés concentrent nos sens ;
- *l'hyperactivité* : mails, réseaux sociaux, messageries instantanées, vidéo-conférences, regarder des vidéos, écouter de la musique, consulter l'actualité…
- *la surinformation* due au flot incessant d'informations sur tous les sujets et à la peur de ne pas être « aware » ; un phénomène qui en découle est la désinformation: tout et son contraire sur chaque sujet: qui croire (individu ou moteur de recherche) ? Que croire ? Il est de plus en plus difficile d'accéder à des connaissances fiables, de trouver l'équilibre, dans un monde ou valeurs et repères fondent comme neige au soleil ; de beaux jours en prévision pour les gourous (Etas compris), les leaders d'opinion et les egos en manque d'auditeurs ou de disciples ?
- *l'ego-navigation ou cyber-égocentrisme* : consiste à faire des requêtes incessantes sur sa personne pour connaître sa cyber-réputation ; Internet permet de croire que l'on est unique, que l'on a 10 000 amis ou « likes », que l'on est aimé… seul devant son écran ;
- *le web-voyeurisme* : phase 2 du cas précédent, vos investigations s'élargissent à vos amis plus ou moins proches, à vos anciennes conquêtes amoureuses, éventuellement à des stars (chanson, cinéma...) ;
- *la virtualisation personnelle* : dont les premiers symptômes peuvent être l'agoraphobie et l'anorexie, qui évolue vers une recherche maladive de rencontres et d'amour via l'Internet, souffrance qui se développe parallèlement à cette peur incapacitante qu'a la personne de rencontrer ces gens dans la vie réelle ;
- *la cyberchondrie ou web-hypochondriaques* : vous effectuez des recherches sur toutes sortes de maladies graves alors qu'au mieux vous avez une maladie imaginaire, au pire une maladie minime dont vous grossissez les symptômes jusqu'à en devenir réellement malades ;
- *l'obsessionnel* : perfectionniste il crée des dossiers, range, classe, modifie, corrige, vérifie, teste sans cesse ses connaissances… sa musique, ses photos, ses fichiers ;
- *la wikipediolie* : vous sacrifiez votre vie personnelle ou professionnelle pour rédiger des articles sur l'encyclopédie en ligne Wikipedia (ou une autre), et cela devient compulsif...

- *le web-exhibitionniste* : dont l'exemple type est le blog sur lequel on dévoile sa vie privée... parfois très privée !
- *le cyber-harcèlement* : le réseau social Aka Aki (disparu en 2012 modèle économique indéfini) vous indiquait quels étaient vos contacts à proximité immédiate, tout comme le service de géolocalisation comme Google Latitude (supprimé le 9 août 2013) qui vous permettait de suivre la position GPS d'un individu ; Google Maps a été utilisé à des fins de surveillance allant jusqu'à permettre des cambriolages.
- *la démultiplication de la personnalité* (trouble dissociatif de l'identité T.D.I.) : avatars, pseudos et login, de boites messageries, forums de discussion, sites de rencontre… l'Internet permet à tout un chacun de s'inventer une nouvelle vie, de présenter un personnage nouveau à chaque connexion. Ce qui pour certains semble être devenu un mode de vie qu'ils contrôlent, d'autres, adolescents ou des personnes fragiles, peuvent croire en leurs personnages au point d'y laisser leur peau.
- *l'addiction aux jeux en ligne* : démodés les jeux vidéo sur consoles, l'Internet a permis les jeux multi-joueurs en temps réel ainsi que les jeux d'argent ; si l'utilisation prolongée de la réalité augmentée et des effets 3D peut provoquer des crises d'épilepsie ou favoriser le stress ou l'obésité, ces jeux sont aussi à l'origine de nombreuses pratiques ou effets pathologiques. Si certains joueurs en ligne utilisent des couches pour adultes pour éviter de perdre s'ils devaient se rendre aux toilettes, il faut savoir que lors de jeux de guerre, souvent violents et immoraux, exacerbent l'agressivité, l'impulsivité et favorisent le passage à l'acte ;
- *la paranoïa* : une impression d'être tout le temps espionné, surveillé, se mettre à tout surveiller, crypte tous ses dossiers et fichiers. Cela arrive aussi à tous ceux qui se sont mis en vitrine sur l'Internet : réseaux sociaux ou professionnels, blogs, sites… qui figent notre évolution : l'Internet sorte de paranoïa pénitentiaire ;
- *la schizophrénie* : à force de multiplier les identités avec une facilité déconcertante, à grands renforts de psychotropes il finit par parler à l'ordinateur en croyant communiquer avec Dieu.

A horizon 2030, le principal problème qui risque de toucher une majeure de la population sera ce sentiment d'être en permanence surveillé, notamment avec les progrès de la géolocalisation, de la reconnaissance faciale, des capteurs biométriques, mais surtout la miniaturisation et la multiplication des sources d'informations (caméra vidéo notamment). Les conséquences iront de la pathologie (paranoïa par exemple) jusqu'à un activisme « anti-cyber » qui pourrait devenir un enjeu de société majeur. Les problématiques de droit à l'oubli numérique qui se posent actuellement ne sont que le début d'une longue série de préoccupations à venir.

5.17.3. Cyberdépendance gouvernementale

L'état Français est de plus en plus dépendant d'Internet, notamment en raison de l'accélération croissante de la dématérialisation et des procédures administratives en ligne. L'état Français s'est ainsi fixé pour objectif, une dématérialisation complète des formalités administratives d'ici à 2020 (cf. page 45 - France numérique 2012-2020[125]). L'abandon du support papier pour toutes les procédures administratives internes et externes amène toutefois quelques questions quant à la résilience des informations en cas de perte de données (les solutions de sauvegardes

[125] (France numérique 2012-2020 / Bilan et Perspectives, MINEFI, 2011)

et archivages numériques ne sont pas à tout épreuve ; par exemple, les supports pourraient être altérés par les rayonnements électromagnétiques consécutifs à une tempête solaire).

L'état envisage également de généraliser un nouveau dispositif d'identification : la CNIE (Carte Nationale d'Identité Electronique) qui pourrait être utilisé pour réaliser de l'authentification forte ou la signature électronique. Ce dispositif devrait améliorer considérablement la sécurité sur Internet pour les citoyens, notamment dans les transactions commerciales, mais aussi pour les formalités administratives. Le développement du vote électronique via Internet sera aussi un enjeu important dans les années à venir.

5.17.4. Une révolution sociétale ?

Le cyberespace actuel évolue rapidement, sur le plan technique, mais également social et cela préfigure peut être un changement profond de la société et des valeurs humaines d'ici à 2030. Une révolution sociétale est-elle en marche ? Ce qui est certain, c'est que de nombreux indicateurs et tendances actuelles confirment que les comportements humains et la vie en société vont évoluer.

Le contact humain pourrait réduire progressivement pour aboutir à un monde ou les personnes communiqueront de plus en plus par l'intermédiaire de machines. Le cyberspace du futur verra apparaitre également une nouvelle relation avec les machines que seront les robots. Les réseaux sociaux pourront être vus comme un artifice qui tentera de combler ce déficit de relation humaine. Au final, il y a un risque d'isolement par rapport au monde réel qui peut aboutir sur la perte de valeurs républicaines essentielles comme la solidarité, la fraternité. En effet, le cyberespace conduit à un repli sur soi, propice à l'égocentrisme et à l'égoïsme. La mondialisation, sous-jacente à Internet, favorisera un modèle néo-libéral préjudiciable au civisme et au patriotisme. En outre, une exclusion du cyberespace conduira de plus en plus à une exclusion de la société.

Autre trait caractéristique de la société à venir est la recherche permanente d'une forme d'instantanéité et l'impatience croissante des individus. Cela engendre un relayage de plus en plus rapides informations, qui n'ont plus le temps d'être correctement appréhendées et vérifiées, favorisant la désinformation, voire la propagande et la manipulation.

Enfin, l'e-réputation va constituer une problématique majeure dans les années à venir. Plutôt cantonnée aux entreprises actuellement, l'e-réputation va impacter de plus en plus l'ensemble des citoyens. L'e-réputation sera longue à construire et en revanche très rapide à détruire avec des conséquences parfois à vie pour les individus. De nouveaux risques pourraient devenir des problèmes de sécurité publiques majeurs, par exemple, les mises au défi via les réseaux sociaux, le chantage par rapport à la vie privée, avec des impacts pouvant être mortels (accidents, suicides).

5.18. Enjeux réglementaires et juridiques

5.18.1. Protection des mineurs

Le cyberspace constitue une zone de grand danger pour une catégorie particulière de la population que sont les mineurs. Le phénomène est actuel et va empirer en raison de l'hyper-connectivité à venir et du fait que ces mineurs qui interagissent avec le cyberespace seront de plus en plus jeunes.

Les mineurs sont considérés comme immatures car non conscient de certains risques. Or, le cyberespace est le lieu de tous les dangers dans bien des domaines (accès à des contenus illicites ou interdits aux mineurs comme la pornographie ou les jeux d'argents, exposition au détournement de mineurs et aux « prédateurs » en tout genre, sensibilité par rapport à leurs données personnelles)

Force est de constater qu'aujourd'hui l'état ne protège pas suffisamment les mineurs. Déléguer cette responsabilité aux parents est insuffisant, car ces derniers sont bien souvent dépassés par les progrès de la technologie et pas toujours conscient des risques. L'état devra jouer un rôle prépondérant dans la prévention, la réglementation et la sanction pénale.

5.18.2. Protection de la vie privée

La protection de la vie privée est une problématique transverse majeure qui va devenir de plus en plus importante dans les années à venir[126]. Les données personnelles dans le cyberespace seront en effet de plus en plus nombreuses en quantité et en diversité en raison de la multiplication des terminaux et des applications, et de la croissance des performances réseau. La part de données personnelles générées par les objets connectés sera croissante, notamment les données à caractère biométrique[127].

Le principe de protection de la vie privée dans les traitements informatiques a vu le jour en France dans les années 1970 avec notamment la création de la CNIL. L'objectif était principalement idéologique et philosophique avec le refus d'une forme de fichage à grande échelle, notamment par les états. Cet objectif initial est en passe d'évoluer fortement pour plusieurs raisons :

- ce sont désormais des entreprises, multinationales et puissantes (GAFA), qui collectent et maitrisent une grande partie des données personnelles des citoyens. Il est intéressant de noter que ce phénomène récent préoccupe fortement les citoyens américains.
- les données personnelles alimentent la cybercriminalité (usurpation d'identité, chantage)
- les données personnelles constituent de plus en plus une manne financière colossale. En 2020, la valeur des données personnelles collectées en Europe pourrait atteindre 1000 milliards de dollars[128].
- Les conséquences d'une exploitation malveillante des données personnelles peuvent être catastrophiques sur les plans personnel, professionnel et financier : être identifié sur une photo compromettante peut briser une réputation, un couple, faire perdre un emploi.

En matière de protection de la vie privée, les principaux enjeux à appréhender sont :

- le développement de la géolocalisation. Quelques scénarios de vulnérabilités peuvent d'ores et déjà être imaginés :
  - un individu se rendant régulièrement dans un établissement de santé peut laisser penser qu'il souffre d'un problème médical. Cette information peut être exploitée défavorablement par un employeur, une assurance prévoyance/santé, un organisme de crédit ;

[126] (CNIL Innovation et Prospective : Vie privée à l'horizon 2020, 2013)
[127] (CNIL Innovation et Prospective : Le corps, nouvel objet connecté, 2014)
[128] (Vos données personnelles valent 315 milliards d'euros, 2012)

- les relations extra-conjugales peuvent être détectées et exploitées par des tiers à des fins de chantage ou demande de rançon.

En outre, des travaux de recherche sont actuellement menés pour établir des signatures de parcours type et effectuer des corrélations avec d'autres individus ne disposant pas forcement d'une source de données de géolocalisation. Cela permet d'établir les relations entre les individus et de tracer plus efficacement leurs déplacements. Dans ce contexte, le concept de « pay as you drive »[129] en voie de développement dans le domaine des assurances automobile doit faire l'objet d'une vigilance particulière.

- les progrès de la reconnaissance faciale et ses applications, par exemple l'analyse des émotions du visage (état physiologique, mensonge, peur, …). Avec des lunettes connectées (type Google Glass) et une reconnaissance faciale en temps réel, il pourrait devenir possible de scanner instantanément et à son insu, le profil de n'importe quel individu croisé dans la rue, bouleversant ainsi les codes sociaux établis. Dans le domaine de la publicité, la reconnaissance faciale est déjà utilisée pour contextualiser des messages sur des panneaux publicitaires[130].
- le développement de la biométrie notamment à travers les objets connectés (capteurs). Ces données, pouvant être à caractère médical, intéressent naturellement les assureurs par exemple. Certains assureurs peuvent même fournir le capteur biométrique (bracelet connecté[131]) en compensation d'une prime d'assurance moindre.
- le développement du « Big Data ». Par exemple, des requêtes récurrentes dans un moteur de recherche sur un centre d'intérêt spécifique peuvent constituer une information pouvant être valorisée. Une recherche sur une maladie ou un symptôme médical peut également être exploitée à l'insu de son auteur, et ce pendant plusieurs décennies.
- la remise en cause de l'efficacité des techniques d'anonymisation actuelles, notamment face aux progrès de la ré-identification[132]
- l'absence d'une réglementation à l'échelle mondiale et l'inadéquation des sanctions pénales actuelles face à ces nouveaux enjeux. La proportionnalité des sanctions est une solution actuellement envisagée au niveau européen[133].

Au-delà des problématiques concrètes, l'évolution du monde, de plus en plus numérique et connecté, amène quelques questions fondamentales :

- Faut-il repenser la notion de vie privée ?
- Le principe du droit à l'oubli est-il viable techniquement et juridiquement ? Faut-il migrer vers un droit à l'effacement ou au déréférencement ?
- Le principe d'anonymat peut-il s'appliquer ?
- Faut-il remettre en cause le principe de liberté sur Internet pour assurer davantage de sécurité ?

[129] (PAYD : Pay as you drive, 2014)
[130] (La vidéosurveillance vous fait flipper ? Attendez de voir ce qu'on vous prépare, 2014)
[131] (Axa entrouvre la porte de l'utilisation des objets connectés dans l'assurance, 2014)
[132] (CNIL : Le G 29 publie un avis sur les techniques d'anonymisation, 2014)
[133] (Bruxelles veut imposer l'oubli numérique, 2012)

Il est intéressant de noter que la protection de la vie privée et la gestion des données personnelles deviennent des sujets très centraux pour de nombreuses entreprises. Le principe de « privacy management » fait désormais partie de la stratégie d'entreprise.

5.18.3. Evolution du risque juridique

Aujourd'hui, la loi identifie clairement les titulaires d'abonnements mobile et Internet comme responsables sur le plan juridique des infractions qui pourraient être commises (sauf à démontrer la responsabilité d'un tiers).

A horizon 2030, cela va se complexifier dans la mesure où les individus auront de plus en de plus de mal à cerner et à maitriser le parc de terminaux et d'objets connectés qui sont sous leur responsabilité. En outre, le niveau d'automatisation croissant des objets connectés (ex : robots domestiques, voiture autoguidée, maison domotique) pose une problématique majeure de responsabilité sur le plan juridique : qui est responsable ? Le propriétaire de l'objet ou son fabricant ? Les assurances doivent être intégrer le « risque numérique » ?

D'autre part, la multiplication des objets connectés engendrera une multitude de sources d'informations pouvant servir de preuve dans le cadre d'une enquête judiciaire. L'intégrité de ces informations sera cruciale dans la mesure où une falsification pourra être utilisée à charge ou à décharge. De tels scénarios existent déjà, notamment avec l'essor des smartphones, qui par conception offrent des capacités de programmation très importantes (création de faux SMS ou de faux emails par exemple).

5.18.4. Harmonisation européenne

Même s'il existe de grandes directives au niveau européen, notamment dans le domaine de la protection de la vie privée[134], leurs déclinaisons au niveau des réglementations nationales demeurent hétérogènes ; c'est le cas pour les interceptions légales par exemple. Cela concerne aussi les réglementations fiscales qui sont très variables selon les pays. Par exemple : des pays comme le Luxembourg ou les Pays-Bas sont aujourd'hui considérés comme des prédateurs fiscaux[135] vis-à-vis d'autres pays européens.

Au final, chaque pays possède sa propre réglementation, ce qui place chaque état, notamment la France, et dans une plus large mesure l'Europe, en position de faiblesse par rapport au reste du monde et notamment face aux géants de l'Internet que sont Google, Apple, Facebook, Microsoft, Amazon …

5.19. Les freins au développement d'Internet

A horizon 2030, la pérennité d'Internet n'est probablement pas à remettre en cause. Toutefois, les prochaines années vont voir apparaitre certains freins susceptibles de remettre en cause son développement actuel, en particulier et par ordre d'importance :

- La problématique de l'énergie. En effet, malgré les progrès technologiques, le cyberespace est de plus énergivore et cette énergie risque de couter de plus en plus

[134] (Des règles plus strictes pour protéger les données personnelles à l'ère numérique, 2014)
[135] (Véronique Cayla (Arte) prône la résistance à Google et autres prédateurs numériques, 2013)

cher, générant ainsi des impacts sur le plan financier mais aussi écologique, et nécessitant de revoir certains modèles économiques actuels[136] ;

- La problématique des matières premières nécessaires à la fabrication des terminaux et des objets connectés notamment (métaux précieux, terres rares), dont le cout pourrait croitre considérablement dans les années à venir, notamment en raison de leur raréfaction et de leur surexploitation. Exemple : le cours du Lithium, métal utilisé dans la fabrication des batteries, a vu son prix multiplié par dix entre 2003 et 2008[137] ;
- La problématique de la limite physique du spectre fréquentiel pour les réseaux mobiles. En effet, une large part du spectre est actuellement utilisée et il va être de plus en plus difficile à l'avenir d'en augmenter les performances ;
- Les problématiques de santé publique, notamment par rapport aux éventuels effets d'une exposition trop importante aux ondes électromagnétiques. Actuellement sujette à de nombreuses controverses, si un impact sur la santé humaine était avéré et démontré, cela pourrait avoir des répercussions majeures sur l'écosystème des réseaux mobiles, lesquels sont aujourd'hui une des pierres angulaire du cyberespace ;
- Une mauvaise perception du cyberespace en termes de sécurité (vie privée, fraude) par les citoyens pourrait générer une perte de confiance et un rejet massif de la part d'une partie de la population ;
- L'évolution des systèmes de facturation pour face à la surconsommation des ressources (forfait => facturation à la consommation) pourrait faire évoluer fortement les usages et potentiellement remettre en cause certains modèles économiques actuels. Les projets de taxation sur le trafic Internet[138] ou sur les données[139] s'inscrive également dans ce contexte ;
- Le business-model actuel du « tout gratuit » pourrait évoluer vers des services de plus en plus payants. La contrepartie est que les utilisateurs pourraient devenir plus exigeants en termes de qualité de service, mais aussi sur le plan de la sécurité. En effet, lorsqu'un service est gratuit, l'utilisateur peut hésiter à faire valoir ses droits, alors qu'en position de client, il dispose d'une légitimité plus importante.
- La fin du principe de neutralité du net[140] qui, en favorisant les gros acteurs industriels au détriment des innovations, pourrait remettre en cause les fondements même d'Internet : liberté et égalité.

Enfin, il est important de mentionner la Cyberbalkanisation[141] (SplinterNet[142] chez les anglo-saxons) qui est une tendance croissance susceptible de mettre en péril le modèle actuel « open Internet » promu par les États-Unis. De plus en plus de pays victimes de l'espionnage des Etats-Unis et n'acceptant plus l'hégémonie des Etats-Unis envisagent sérieusement de rétablir leur souveraineté nationale vis-à-vis d'Internet, en appliquant le principe de la balkanisation. Des pays comme la Chine et la Corée du nord ont déjà appliqué depuis longtemps ce principe, mais il s'agit de pays cherchant avant tout à réaliser un contrôle politique sur leurs populations. La nouvelle tendance est que cela concerne

[136] (Le coût écologique d'Internet, 2010)
[137] (Le lithium en Bolivie : quels enjeux stratégiques ?, 2009)
[138] (La Hongrie veut taxer l'utilisation d'Internet, 2014)
[139] (Fleur Pellerin veut une taxe Internet pour 2014, 2013)
[140] (Neutralité du Net, 2014)
[141] (Sénat : L'ère du soupçon et les efforts de « containment » du risque de balkanisation du web, 2014)
[142] (Wikipedia - Splinternet, 2014)

désormais des grandes démocraties (Allemagne[143], Brésil[144], Inde). La Russie[145] a également récemment envisagé d'appliquer ce principe. Différents degrés de balkanisation sont possibles, ils sont illustrés dans le schéma ci-après :

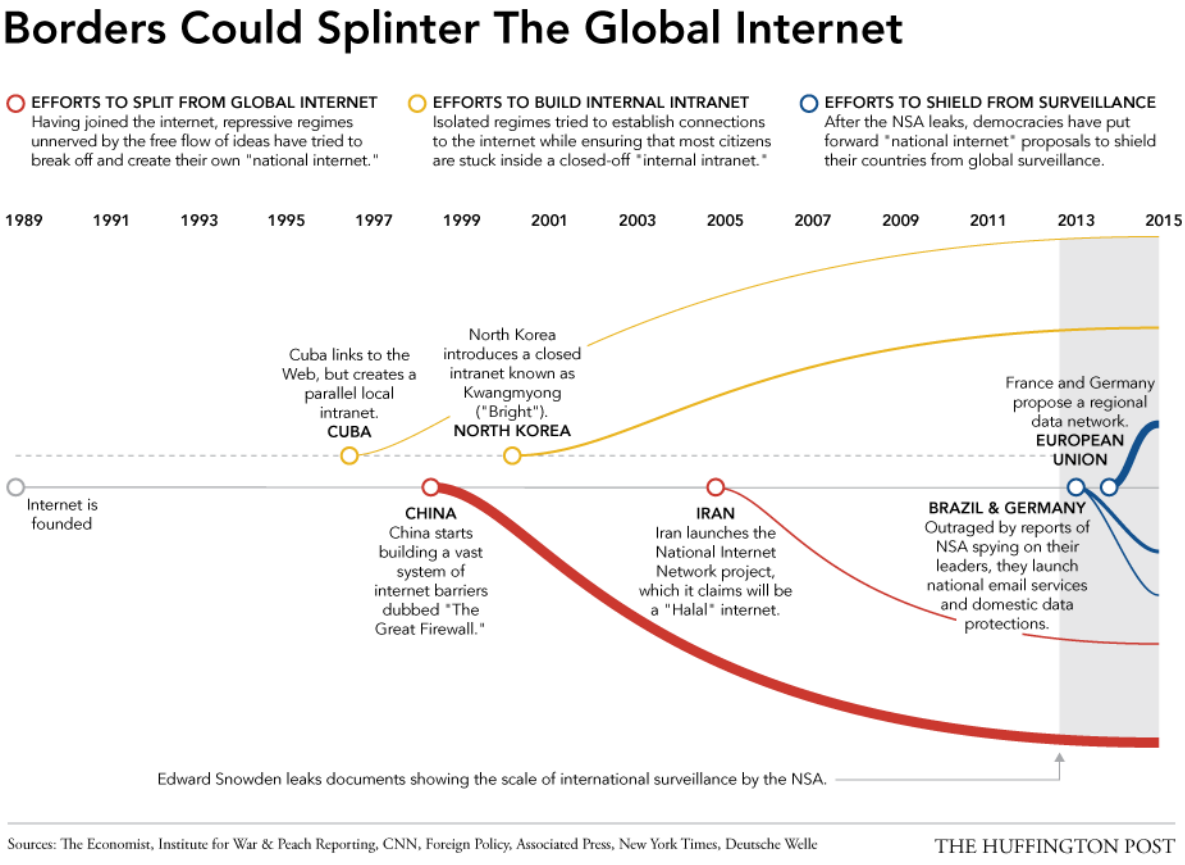

Figure 18 - Balkanisation de l'Internet (source : The Huffington Post)

Selon de nombreux acteurs du web (exemple Google[146]), responsables politiques et journalistes, la balkanisation de l'Internet pourrait constituer une atteinte aux libertés individuelles et être un frein à l'innovation[147]. Il s'agit même peut-être de la plus grande menace à venir ; certains acteurs évoquant déjà la mort d'Internet sous sa forme actuelle[148]. L'association « Reporters sans Frontières » a publié en 2014 un rapport[149] sur ce qu'elle considère comme les ennemis d'Internet et dans lequel la balkanisation de l'Internet est clairement ciblée. La position de l'Union Européenne manque de clarté,

[143] (Europe : un pas de plus vers la balkanisation d'Internet, 2014)
[144] (Brazil plans to go offline from US-centric internet , 2013)
[145] (The 'Balkanisation' of Russia's internet, 2014)
[146] (Etats-Unis: l'espionnage risque de «casser internet», prévient un dirigeant de Google, 2014)
[147] (Réguler le Web : la très mauvaise réponse inspirée aux Etats par le scandale de la NSA, 2013)
[148] (Cybercensure et balkanisation du Web, 2012)
[149] (Reporters sans frontières - Les enemis d'Internet, 2014)

6. Nouvelles mesures et dispositifs de sécurité

Ce chapitre a pour objectif de présenter des mesures et des dispositifs pouvant contribuer à améliorer la sécurité du futur cyberespace, au regard des enjeux de sécurité décrits dans le chapitre précédent. L'objectif est également d'identifier les challenges à venir en matière de sécurité sur des sujets pour lesquels il existe un vide aujourd'hui.

Les mesures présentées sont de différentes natures : technique, organisationnelle, réglementaire. Certaines mesures donnent lieu à une analyse des conséquences techniques, mais également sociétales et juridiques quant à leur mise en œuvre. Les mesures techniques sont transposables dans le contexte des réseaux militaires et gouvernementaux.

Les mesures de sécurité présentées sont basées sur plusieurs sources :

- Le pôle Recherche&Développement du groupe Orange et sa veille technologique, notamment en matière de sécurité (notamment pour les mesures techniques)
- La communauté expert sécurité du groupe Orange qui associe le pôle R&D et les équipes opérationnelles du groupe
- Des travaux de recherche documentaire spécifiques (articles/ressources Internet principalement)

6.1. Les contre-mesures techniques

6.1.1. DNSSEC

Selon les grands acteurs d'Internet, en particulier les opérateurs, l'enjeu majeur dans les années à venir sera la généralisation de DNSSEC[150] à l'échelle globale d'Internet, qui offrira une avancée significative sur le plan de la sécurité. La perception de l'intérêt de DNSSEC a été fortement accrue par la révélation de la faille Kaminsky permettant des attaques de type « DNS cache poisoning »[151]. Les premières implémentations DNSSEC datent déjà d'une dizaine d'années, mais, ce protocole peine à s'imposer pour plusieurs raisons (dont certaines sont communes avec ROA/RPKI ou BGPSec). Note : l'AFNIC propose un guide pour l'implémentation de DNSSEC[152].

Les principaux apports de DNSSEC sont :

- L'authentification des données contenues dans les réponses DNS ;
- L'intégrité de ces données (protection des enregistrements) ;
- La preuve de non existence.

DNSSEC autorise également une architecture alternative pour le stockage de certificats et d'empreintes de certificats X.509 : DANE[153] (DNS-based Authentication of Named Entities) -

[150] (ANSSI - Architecture DNS sécurisée, 2011)
[151] (Wikipedia - Empoisonnement du cache DNS, 2014)
[152] (Déployer DNSSEC, comment, quoi, où ?, 2014)
[153] (AFNIC - Sécuriser les communications sur Internet de bout-en-bout avec le protocole DANE, 2013)

RFC 6394, RFC 6698. DNSSEC combiné à DANE permettrait de répondre à la crise de confiance actuelle dans le modèle PKIX, socle essentiel de la majeure partie des connexions sécurisées sur Internet (SSL/TLS). Les AC (Autorités de Certification) deviennent innombrables et plusieurs attaques ont mis en évidence les limites du modèles PKIX. Avec DANE, un titulaire de nom de domaine peut signer le certificat fourni par le serveur Web (avec la PKI DNSSEC) et le publier dans la zone DNS du domaine, offrant ainsi au titulaire du nom de domaine la possibilité d'informer l'application (ex. : un navigateur web) sur les moyens de valider le certificat provenant du serveur Web.

Toutefois l'adoption de DNSSEC engendre de nouvelles problématiques sur les plans technique et organisationnel, qui expliquent le retard actuel en termes de déploiement :

- *Gouvernance et souveraineté* : DNSSEC introduit un tiers de confiance qui dispose d'un pouvoir très important. Aujourd'hui, l'ICANN, organisme sous contrôle américain, gère la zone root[154] et confie le rôle d'autorité de certification à Verisign qui est aussi une société américaine. Cela pose donc un problème de souveraineté nationale, qui existe déjà aujourd'hui avec DNS, mais qui va être amplifié avec DNSSEC. Pour limiter cette dépendance, une alternative pourrait consister à déléguer le rôle d'autorité de certification à certains états pour les TLD qui les concernent directement (exemple : le .fr pour la France)
- *Gestion des certificats* : une lacune importante de DNSSEC est l'absence de règles et de processus universels pour la gestion des certificats et des clés associées. Cela concerne notamment les processus de révocation et de renouvellement des certificats. Par exemple, la durée de validité des certificats utilisés pour DNSSEC n'est aujourd'hui pas normalisée pour les différentes zones. Ce dernier point est important car il n'est pas possible de valider une zone protégée par DNSSEC dont les certificats ont expiré.
- *Compatibilité* : Un déploiement à l'échelle Internet nécessite une compatibilité avec les systèmes et les standards existants, en particulier les équipements de sécurité comme les Firewall (analyse protocolaire, taille des paquets)
- *Ressources* : L'ajout d'une couche cryptographique nécessite des ressources de traitement supplémentaires, ce qui peut poser des soucis de performances sur les équipements fortement sollicités, notamment les serveurs.
- *Fiabilité/Complexité* : DNSSEC complexifie et centralise encore davantage l'architecture du service DNS. Inévitablement, cela fragilise la fiabilité globale du service, notamment en raison des risques d'erreurs humaines induites par la gestion de la couche sécurité du DNSSEC (exemple : en 2012, une erreur de signature sur le nom de domaine de la NASA a abouti à un blocage de leur site web)[155]. Plus globalement, la centralisation de la sécurité au niveau des serveurs root devient critique dans la mesure où une compromission de la clé privée pourrait engendrer un effondrement de la résolution DNS à l'échelle Internet.
- *impact plus élevé des attaques par amplification DNS* : DNSSEC peut amplifier les dénis de service basé sur l'amplification DNS. En effet, avec le DNS standard, l'effet levier est de 1 pour 20 ; avec DNSSEC, il passe à 1 pour 73.

[154] (Serveur racine du DNS, 2014)
[155] (DNSSEC Error Caused NASA Website To Be Blocked, 2012)

Plus généralement, malgré ses atouts incontestables sur le plan de la sécurité, il faudra veiller à ce que la confiance accordée dans DNSSEC ne soit pas compromise par le scénario qui s'est produit avec SSL/TLS et la PKIX, à savoir la multiplication anarchique des Autorités de Certification. Aujourd'hui, des sociétés jugées comme dignes de confiance sur les plans technique et organisationnel (ex : Verisign) permettent de garantir la chaine de confiance. Sur le long terme, il faudra maintenir ce niveau de confiance en contrôlant sévèrement les autorités de certification, sans céder aux tentations économiques qui aujourd'hui posent un réel problème avec le modèle PKIX.

En termes de déploiement, l'implémentation de DNSSEC est plutôt timide[156]. Cela est grandement dû aux problématiques exposées ci-dessus, mais aussi en raison du fait qu'aucun pays n'impose DNSSEC. Les serveurs DNS racine, les serveurs autoritaires gérant les TLD et certains grands hébergeurs sont déjà « DNSSEC ready », mais l'efficacité de cette mesure ne sera réellement effective que lorsque toute la chaine de communication sera compatible (les opérateurs, les hébergeurs, les résolveurs DNS des serveurs et des terminaux clients). Les opérateurs devraient notamment être plus moteurs dans le déploiement du DNSSEC. En réalité, il faudra probablement attendre un incident de sécurité majeur à l'échelle mondiale pour faire avancer les choses.

6.1.2. ROA/RPKI et BGPSEC

Sur le plan technique, les mesures suivantes sont envisagées pour sécuriser davantage le protocole BGP :

- La protection contre les messages malformés (fiabilisation du protocole), à l'origine de certains incidents en déni de service notamment.
- La mise en œuvre de solutions basées sur la cryptographie asymétrique pour authentifier les AS opérateurs et lutter contre l'usurpation de préfixes (ROA/RPKI, BGPSec).

ROA/RPKI[157], normalisé par l'IETF, a pour but de certifier l'AS origine avec ses préfixes. Pour cela chaque opérateur signe les annonces qu'il émet et vérifie toutes les annonces qu'il reçoit (ce traitement de vérification peut être différé à postériori pour améliorer la rapidité de convergence du routage). La certification devrait s'appuyer sur 5 RPKI racines maitrisées par les RIR Internet ; la France dépend du RIPE NCC qui gère l'Europe et une partie de l'Asie, notamment le moyen Orient. Des systèmes de cache peuvent être mis en œuvre au sein des réseaux opérateurs pour optimiser le fonctionnement de RPKI. RPKI est aujourd'hui en test dans un contexte universitaire et il est déployé de manière embryonnaire chez certains opérateurs (Orange notamment) à des fins expérimentales. A noter que peu de certificats ont été demandés à l'heure actuelle.

BGPSec fait l'objet d'un groupe de travail à l'IETF ; il s'appuie sur RPKI et contrairement à ROA/PKI, il permet à un AS de valider la conformité d'un chemin d'AS (attribut AS_PATH),

[156] (Résilience de l'Internet français §2.3 Taux de pénétration de DNSSEC, 2013)
[157] (RFC 6483 - Validation of Route Origination Using the Resource Certificate Public Key Infrastructure (PKI) and Route Origin Authorizations (ROAs), 2012)

depuis l'origine jusqu'au voisin lui ayant transmis l'annonce. BGPSEC pourrait ainsi permettre de lutter plus efficacement contre des attaques basées sur la redirection de trafic. Remarque importante : Même avec une garantie complète sur chemin/routage, les attaques MITM sur les flux client demeurent possibles sur un chemin validé. BGPSec n'est pas normalisé et non implémenté dans les équipements actuels. A noter que cette solution est très gourmande en ressources dans le contexte Internet, notamment lors des phases d'initialisation des équipements (convergence du protocole de routage).

Pour être efficace, ces mesures techniques nécessiteraient d'être appliquées par l'ensemble des opérateurs, ce qui n'est aujourd'hui pas envisageable à court termes compte-tenu des raisons exposées au §5.12.4. Se pose également une problématique de gouvernance dans le sens où les opérateurs auront moins de liberté par rapport à aujourd'hui ; la maitrise de la sécurité étant désormais davantage sous le contrôle du responsable de la RPKI (RIPE NCC notamment). Enfin, comme pour toute solution basée sur une PKI, les problématiques de gestion des clés et des certificats sont à appréhender (distribution, renouvellement, révocation).

NB : Une synthèse détaillée sur la sécurisation de BGP a été réalisée par l'Université de Strasbourg en 2013[158]. L'ANSSI a également publié un rapport sur la résilience de l'Internet Français[159], avec un chapitre complet concernant BGP.

6.1.3. Identifiant service operateur sur Internet

Les opérateurs de téléphonie mobile et fournisseurs d'accès Internet disposent d'un ensemble de données utilisateurs nécessaires à l'exploitation opérationnelle de leurs réseaux : numéro de téléphone, identifiant de cellule GSM, paire de cuivre ADSL, répartiteur DSLAM, etc. Ces données, nativement fiables et rafraîchies fréquemment, peuvent être réutilisées à des fins d'authentification. On peut alors qualifier ces données d'« identifiants service opérateur », qui pourront être, indirectement et par des mécanismes d'anonymisation préalables, mis à disposition de fournisseurs de services tiers désirant améliorer l'identification ou l'authentification de leurs clients afin de sécuriser les transactions en ligne ou simplifier le parcours client. Pour ce faire, des solutions de « scoring » d'authentification peuvent être implémentés et renforcés avec des données opérateurs, dans le cadre d'une démarche RBA (Risk Based Authentication).

Un utilisateur dispose typiquement de plusieurs contextes (medias) qui peuvent évoluer : un ordinateur fixe à son domicile, un smartphone 4G dans les transports, un PC portable au bureau, une tablette Wifi à l'hôtel, une borne d'accès à l'aéroport, etc. Chacun de ces dispositifs est en mesure de transmettre des informations matérielles, applicatives ou opérateur pouvant représenter une caractéristique particulière et distinguable, qui pourra alors être liée à un poids qui altère le coefficient de risque, ainsi qu'à un coefficient éventuel de fiabilité. Ces informations qualifiées pourraient ainsi être exploitées afin de participer au « scoring » d'authentification des transactions et opérations en ligne.

[158] (Université de Strasbourg - Sécuriser le routage sur Internet, 2013)
[159] (ANSSI - Résilience de l'Internet français, 2013)

Si ces principes sont techniquement simples à mettre en œuvre, deux obstacles potentiels sont à anticiper :

- Les méthodes d'anonymisation doivent être explicitées et qualifiées, afin de garantir que les données des clients de l'opérateur ne sont en aucun cas transmises à des tiers ;
- Pour être universelle, cette méthode d'authentification nécessite la collaboration de l'ensemble des opérateurs afin de fournir *a minima* des moyens d'accès identiques et normalisés, et dans l'idéal un moyen d'accès unifié multi-opérateur.

6.1.4. Authentification non observable

Confidentiel Orange (voir annexe C)

6.1.5. Nouveaux procédés de supervision et de détection par voie réseau

Les évolutions récentes et rapides du paysage de l'informatique se traduisent depuis peu dans l'apparition de nouvelles manières de superviser la sécurité des réseaux, à l'aide de nouveaux types de capteurs. Plusieurs facteurs expliquent cette évolution :

- Le déclin des PC au profit des terminaux mobiles va s'accentuer d'ici 2030, à tel point que le visage classique du poste de travail d'entreprise risque de se transformer en profondeur ;
- A cette transformation du parc matériel est associée la montée en puissance rapide de l'écosystème Google, à travers notamment Android, qui sera le grand gagnant de la bataille des OS que nous observons actuellement ;
- L'intrication des OS avec les services « Cloud » sera tellement forte et transparente qu'il deviendra impossible de localiser une donnée ou une application sur un terminal : messagerie, stockage, travail collaboratif vont progressivement quitter le giron de l'entreprise. Ainsi, le SI des organisations va basculer progressivement et silencieusement vers les datacenters de grandes sociétés principalement américaines ;
- Les révélations de l'affaire Snowden[160] donnent déjà des résultats en normalisation, où l'IETF s'est donné pour mission de chiffrer intégralement les protocoles de communication existant et à venir dans les prochaines années ;

Cette dominance d'acteurs comme Google ou IBM à l'horizon 2030, leur offre de valeur séduisante comparativement aux applications sur les SI internes, leur force de frappe normative, et l'avènement d'un Internet intégralement chiffré (l'utilisation de SSL par défaut en est d'ores et déjà le premier signe) vont progressivement rendre très difficile la supervision de la sécurité sur un réseau d'entreprise : superviser les flux internes sera très insuffisant et la cible primaire d'une telle supervision devra être les flux vers les services Cloud externes.

Dans le domaine des télécommunications, cette externalisation risque de se développer rapidement avec l'avènement de la 5G, à travers la mutualisation complète des réseaux dans certains pays au profit de certains constructeurs qui fourniront aux opérateurs des infrastructures clef en main.

Ceci se traduit également par un appauvrissement de la supervision : il est d'usage actuellement de croiser des logs provenant du réseau, des systèmes et des applicatifs afin de tirer une information multi-couches ; dans un modèle où l'application est hébergée à l'extérieur, seuls les logs réseau resteront à la portée de l'organisation. Et encore, dans un monde

[160] (Wikipedia - Révélations d'Edward Snowden, 2013)

intégralement chiffré, les flux réseaux eux-mêmes deviendront inaccessibles aux organisations ne possédant pas la capacité de les déchiffrer à la volée : la bonne volonté de l'IETF peut ainsi à moyen terme se traduire par un aveuglement des dispositifs de détection d'intrusion.

Cependant, pour une organisation qui aurait conservé la maîtrise des trois piliers de son SI que sont le réseau, le système et l'application, la recherche scientifique apportera d'ici 2030 des avancées importantes en matière de corrélation d'événements multi-niveaux et de détection d'intrusions et de fraudes complexes. En effet, le saut capacitaire représenté par le « Big Data » -- qui brise un verrou majeur de ces applications – va être suivi d'un saut technologique en matière d'intelligence artificielle et de « data mining », permettant ainsi une supervision nettement plus efficace d'environnements technologiques hétérogènes et complexes. Les systèmes de détection d'intrusion actuels (plutôt centralisés), devraient ainsi évoluer vers des systèmes collaboratifs et distribués (« Distributed and Collaborative Intrusion Detection System »).

6.1.6. Nouveaux modèles de protection contre les dénis de service

La protection contre les attaques en déni de services, en particulier les DDOS, doit s'appuyer sur plusieurs piliers :

- la prévention (répartition des ressources par exemple) ;
- la surveillance pour détecter l'attaque et mesurer les impacts ;
- l'analyse pour comprendre et localiser l'origine de l'attaque ;
- la réponse (confinement de l'attaque, mesures correctrices et réactives).

Il existe aujourd'hui plusieurs moyens de se défendre contre les DOS/DDOS[161], notamment au niveau réseau via les principes de « Black Holing » (rejet sélectif du trafic en fonction des adresses IP) et « Clean Pipe » (filtrage/nettoyage évolué du trafic en temps réel par un tiers). Les opérateurs Internet et les hébergeurs sont ainsi au cœur de la lutte contre les dénis de service.

A plus long terme, de nouveaux modèles de protection sont envisagés :

- La reconfiguration dynamique du réseau via SDN[162] pour mettre en œuvre du Black Holing
- L'utilisation du Big Data (approche collaborative entre opérateurs) pour la détection et le traitement des DOS/DDOS
- L'exploitation du critère de géolocalisation (origine des flux) pour bloquer le trafic malveillant en provenance de sources inconnues ou suspectes
- La mise en œuvre de règles de filtrage affinées, notamment en termes de volumétrie, au niveau du Backbone avec des mécanismes comme BGP Flowspecs (RFC 5575[163])
- La réponse offensive (interdite aujourd'hui)

[161] (Wikipedia : Denial-of-service attack, 2014)
[162] (Leveraging SDN for Efficient Anomaly Detection and Mitigation on Legacy Networks, 2014)
[163] (RFC 5575 : Dissemination of Flow Specification Rules, 2009)

6.1.7. Analyse comportementale des malwares

L'analyse des malwares constitue un enjeu quotidien pour la sécurisation du cyberspace, le défi étant d'assurer un niveau de détection et de réactivité toujours plus élevé. Dans les années à venir, la lutte contre les malwares sera de plus en plus basée sur une analyse dynamique :

- établissement de bases de signatures comportementales statistiques (exemple : navigation sur une page web) pour détecter des comportements déviants
- isolement sur des sandbox au niveau du réseau pour analyser le comportement et les effets potentiels d'un flux réseau (le SDN présente un fort intérêt dans ce contexte). L'idée est de construire des terminaux virtuels/fictifs pour observer le comportement d'un écosystème dans la durée sans se présenter en coupure du flux normal.

Cette analyse comportementale présente des atouts majeurs :

- elle permet de lutter contre les mécanismes d'offuscation de code mise en œuvre par les malwares
- l'approche statistique rends possible l'analyse de flux chiffrés (sans avoir à les déchiffrer)

6.1.8. Traçabilité sur l'usage des données

La traçabilité sur l'usage des données a notamment pour objectif de prévenir les fuites de données (DLP). La finalité consiste à vérifier que les données sont utilisées conformément à une politique préalablement établie. Les solutions techniques qui existent actuellement sont focalisées sur les données au niveau utilisateur ; elles combinent des mécanismes basés sur du chiffrement asymétrique (marquage des données) ainsi que des outils de surveillance, notamment la détection d'intrusion. Compte-tenu de la complexité de mise en œuvre et des contraintes d'exploitation, ces solutions sont restreintes à des usages spécifiques.

Dans les années à venir, les mesures assurant la traçabilité des données seront focalisées au niveau des couches réseau. L'idée est d'insérer des marqueurs dans les entêtes réseau permettant de gérer la localisation des flux de données. Combiné à l'usage de puce TPM dans les équipements réseau, la finalité est de pouvoir contrôler de manière certaine l'origine, la destination et le cheminement des flux à travers un réseau. Il ne s'agit pour le moment que d'un concept, qui au-delà des difficultés techniques (modifications protocolaires), pose des problématiques de gouvernance et de confiance (autorité de certification) et d'exploitation (administration, gestion des alertes de supervision).

6.1.9. Réseau polymorphe (MTD : Moving Target Defence)

Confidentiel Orange (voir annexe C)

6.1.10. Zero trust network architecture (ZTNA)

« Zero Trust Network Architecture »[164] (ZTNA) est un nouveau concept pour appréhender la sécurité du réseau. Il part du principe que l'on ne fait pas confiance au réseau (les équipements, les interfaces, les utilisateurs) ; tout le trafic est considéré comme une menace jusqu'à ce qu'il soit validé et autorisé. La sécurité doit donc s'appuyer sur une vérification systématique et être

[164] (Le modèle sécurite Zéro Trust - Le nouveau paradigme sécurite, 2013)

traitée au plus proche des applications. Le concept ZTNA existe depuis plusieurs années, mais n'est pas normalisé.

Les principes de mise en œuvre de ZTNA sont les suivants :

- Le réseau doit être segmenté en zones de confiance partageant les mêmes exigences de sécurité (notion de MCAP : Micro Core And Perimeter) ; les MCAP sont interconnectés via une « Segmentation Gateway » intégrant les fonctions de sécurité (firewall, contrôle d'accès chiffrement, IDS/IPS, journalisation…)
- Toutes les ressources sont accessibles de manière sécurisée indépendamment de leur emplacement.
- Le contrôle d'accès est appliqué de manière stricte sur la base du besoin d'en connaitre (niveau de privilèges minimum)
- Il faut tracer et inspecter systématiquement l'ensemble du trafic réseau
- La sécurité des réseaux doit être gérée de manière centralisée (approche SDN pour la sécurité)

La philosophie de ZTNA est de construire le réseau en fonction des exigences de sécurité (et non d'adapter la sécurité au réseau existant). C'est pourquoi, ZTNA n'est pas applicable de manière simple aux modèles de réseaux actuels. Son éventuelle mise en œuvre est davantage à rechercher dans les réseaux internes supportant des applications critiques. A noter que ZTNA nécessite des moyens techniques importants et très performants et peut aussi se heurter à des contraintes légales (ex : journalisation systématique du trafic).

6.1.11. Les réseaux quantiques

Un réseau quantique est constitué de liaisons optiques qui exploitent la propriété physique de non-observabilité des particules lumineuses (photons) pour transmettre des secrets. Le principe est d'échanger des clés de chiffrement entre deux extrémités avec la garantie qu'elles ne soient pas observées/interceptées par un tiers. Ce principe nommé QKD « Quantum Key Distribution »[165], abusivement appelé « cryptographie quantique », permet de renouveler très fréquemment et de manière décorrélée les clés utilisées pour chiffrer les données.

Les Etats-Unis et plus récemment la Chine ont engagé des travaux de recherche pour le déploiement des premiers réseaux quantiques sur leurs territoires respectifs[166]. La mise en œuvre de ces réseaux, à usage gouvernemental, est envisagée en 2016. Dans le cas de la France, cette technologie présenterait un intérêt certain dans le domaine des réseaux militaires stratégiques ou gouvernementaux.

6.1.12. Chiffrement homomorphe

En matière de cryptographie, la prochaine décennie devrait être marquée par le développement du chiffrement homomorphe[167]. Cette technique de chiffrement asymétrique est caractérisée par le fait qu'elle permet de réaliser des traitements sur des données chiffrées sans avoir à les

[165] (Wikipedia - Quantum key distribution, 2014)
[166] (La Chine et les USA construisent leurs premiers réseaux quantiques, 2014)
[167] (Le chiffrement homomorphe, 2014)

déchiffrer. Cela présente donc un intérêt certain dans le cyberespace, notamment pour répondre aux enjeux de protection des données personnelles.

Les applications envisagées sont multiples :

- Traitement anonyme de données personnelles dans le Cloud
- Transcodage de fichiers vidéo et photo chiffrées pour les adapter aux différents terminaux d'un utilisateur.
- Vote électronique (accès au résultat global sans connaissance des votes unitaires)
- Recherche de la présence d'un mot dans un texte chiffré
- Anonymisation de bases de données (exemple : numéro de carte bancaire)
- Contrôle d'une politique de sécurité sans avoir accès aux données

Les implémentations actuelles du chiffrement homomorphe sont encore très élémentaires ; elles ne permettent de réaliser que des opérations simples telles que l'addition ou la multiplication. Les opérations complexes nécessitent des ressources de calcul très élevées. Globalement, le chiffrement homomorphe est encore au stade expérimental et l'enjeu à venir sera de résoudre la problématique des performances nécessaire à ce type de chiffrement.

6.1.13. Cloud et virtualisation

La virtualisation qui est actuellement largement implantée au niveau des serveurs va s'étendre au niveau du réseau via les modèles SDN et NFV. La virtualisation est aujourd'hui sujette à de nombreuses préoccupations en termes de sécurité, en particulier concernant la confidentialité des données, mais aussi la résilience.

La virtualisation est un socle essentiel des services en mode Cloud. A l'heure actuelle, outre la problématique de la souveraineté qui se pose naturellement, il faut considérer que la technologie du Cloud n'est pas mure sur le plan de la sécurité. C'est pourquoi, Il existe plusieurs programmes de recherche européens dédiés au Cloud, notamment le programme « Trusted Cloud Europe »[168] qui est axé spécifiquement sur la sécurité et la résilience.

Pour améliorer le niveau de sécurité de la virtualisation et plus largement du cloud, plusieurs évolutions ou axes d'études sont envisagés :

- *Auto-stabilisation* [169] : basée sur une architecture répartie de l'hyperviseur de virtualisation, l'auto-stabilisation a pour objectif d'améliorer la résilience des services et le cloisonnement inter-VM. Sur le plan de la sécurité, l'auto-stabilisation permet de lutter contre les dénis de service et les menaces de type Rootkit.
- *Cloud réparti*[170] : le principe consiste à fragmenter les données, les encrypter et à les disséminer dans une multitude de serveurs localisés dans des zones géographiques différentes afin d'assurer une meilleure résilience.
- *« Blind Storage* [171]*»* : permet de stocker des données chiffrées dans un cloud, et de les partager avec des tiers à des fins de traitement, sans que ces données ne soient jamais

[168] (Commission Européenne : Trusted Cloud Europe, 2014)
[169] (Self-Stabilizing Virtual Machine Hypervisor Architecture for Resilient Cloud, 2014)
[170] (Vifib joue la carte du cloud réparti, 2013)
[171] (Dynamic Searchable Encryption via Blind Storage, 2014)

accessibles directement en clair. Il s'agit d'une application de la cryptographie homomorphique qui permet de manipuler des données sans les déchiffrer entièrement.

- *Hyperviseur de confiance* : plusieurs travaux de recherche sont menés pour améliorer le niveau de sécurité des hyperviseurs, notamment pour des applications gouvernementales. La cryptographie homomorphe est un axe technique envisagé, car cela pourrait permettre de faire fonctionner des machines virtuelles sous forme chiffrée. Il existe déjà des hyperviseurs de confiance, notamment dans le domaine de l'embarqué, mais ils souffrent d'une limitation majeure sur le plan des performances. Un des objectifs majeurs des travaux de recherche est donc de concilier sécurité et performances.
- *Contrôle d'accès interopérable* : l'objectif est de développer un contrôle d'accès plus fin et interopérable entre les différents fournisseurs de services Cloud. Les problématiques de multi-tenancy et de contrôle d'accès hiérarchique s'inscrivent également dans ce contexte.

Enfin, une nouvelle tendance voit le jour et est probablement voué à se développer dans les années à venir : La « Containerisation »[172]. Il s'agit d'un nouveau modèle de virtualisation ne faisant pas appel aux hyperviseurs classiques. A noter qu'un hyperviseur engendre une perte de 3 à 4% des performances globales ; avec la containerisation, il n'y a aucune baisse de performances. Le principe de containerisation est aujourd'hui soutenu par le projet open-source Docker[173]. En termes de sécurité, la containerisation est peu mature et engendrera de nouvelles problématiques.

6.1.14. Sureté de fonctionnement des infrastructures critiques

Le commencement de l'ère industriel a été accompagné d'un cortège d'incidents, d'accidents ou d'événements catastrophiques. Le risque zéro n'existe malheureusement pas pour les activités industrielles à cause de l'occurrence de défaillances humaines ou matérielles. Pour tenter de maitriser ces risques, des méthodes, des techniques et des outils scientifiques ont été développés dès le début du 20e siècle pour évaluer les risques potentiels, prévoir l'occurrence des défaillances et tenter de minimiser les conséquences des situations catastrophiques lorsqu'elles se produisent. L'ensemble de ces développements méthodologiques à caractère scientifique représente, la discipline de la Sûreté De Fonctionnement (SDF). L'arrivée des technologies de l'information au sein des systèmes industriels a conduit à complexifier les infrastructures industrielles. Ainsi, la SDF a dû évoluer: de nouveaux modèles sont arrivés pour traiter les défaillances des systèmes notamment issues des erreurs logicielles. Le concept de « faute » a été introduit, ce qui permet également de traiter une partie des risques liés à la cybersécurité (ex : erreur de développement). Les concepts d'attaques malveillantes et volontaires sont toutefois très peu pris en compte. Seuls des domaines très critiques, tel que la sureté nucléaire, ont réellement lancé très récemment des initiatives pour intégrer sûreté et Cybersécurité (ex : IEC 62859). L'exercice est complexe car les deux approches sont totalement distinctes. Les processus SDF étant historiquement intégrés aux processus industriels, il sera nécessaire de les compléter pour prendre en considération la cybersécurité. Il

[172] (Virtualization is dead, long live containerization, 2014)
[173] (Docker, 2014)

serait en effet peu efficient de décliner de nouveaux processus spécifiques à la cybersécurité et dédié au monde industriel. De fait, deux étapes majeures des processus SDF devront évoluer:

- La phase d'analyse de risques devra prendre en compte le caractère non limité et parfois illégitime des moyens de l'attaquant. De fait, les attaques fondées sur l'exploitation non autorisée des services, en se faisant passer pour une entité autorisée, devront être traitées ;
- Le traitement des exigences devra également évoluer afin de ne pas s'en tenir à des méthodes algébriques formelles permettant de prouver l'absence de risques. La prise en compte de critères qualitatifs devra pouvoir être possible. Typiquement, d'un point de vue stratégie de défense, une gouvernance devra être mise en place afin de permettre l'intervention d'entités extérieures de type étatique dans le cadre d'une infrastructure critique.

6.1.15. Négociation automatique des politiques de sécurité

Aujourd'hui, de plus en plus d'organisations et d'entreprises coopèrent et se coordonnent pour échanger des données et des services dans des écosystèmes dynamiques. Ce processus implique un grand nombre d'acteurs que sont les clients et les fournisseurs services. Afin de garantir la sécurité, l'interopérabilité et les performances, les différents acteurs doivent conclure des accords de services avec des contraintes de délais courts.

La négociation des politiques de sécurité est un aspect important de ce processus. L'objectif est de parvenir automatiquement à un accord mutuel sur la politique de sécurité qui sera respecté et exécuté entre un client et un fournisseur.

Les solutions actuelles pour négocier des politiques de sécurité entre acteurs différents telles que celles proposées par exemple dans WS-Trust[174], reposent sur des fonctions de mise en correspondance purement syntaxique : la négociation échoue si cette mise en correspondance est impossible. Dès lors, sont mis en œuvre des développements et des processus d'intégration complexes, spécifiques, et peu évolutifs, ce qui constitue subséquemment un frein à l'établissement d'écosystèmes larges et dynamiques.

Les futurs travaux de recherche ont pour objectif de développer un modèle permettant l'interopérabilité sécurisée de services et des échanges de ressources entre services contrôlés par des politiques de sécurité différentes. Ils sont dans le prolongement de travaux antérieurs comme le modèle XeNA[175] et concerne la définition et la mise en œuvre des protocoles permettant aux organisations de négocier ces politiques d'interopérabilité, ainsi que des modèles pour administrer les politiques d'interopérabilité. L'approche envisagée pour ce futur modèle repose sur une mise en correspondance sémantique. Parmi les verrous identifiés, il s'agira notamment de spécifier une ontologie de sécurité ainsi qu'une logique pour comparer les exigences de sécurité à négocier. Un autre verrou est la normalisation du processus d'établissement des contrats d'interopérabilité afin de répondre au besoin d'automatisation de la génération de ces contrats.

6.1.16. Sécurité des composants logiciels et matériels

Confidentiel Orange (voir annexe C)

[174] (Wikipedia - WS-Trust, 2014)
[175] (XeNA: an access negotiation framework using XACML, 2014)

6.2. Formation et sensibilisation

Les solutions techniques ne peuvent pas et ne pourront pas traiter à elles seules les problématiques de cybersécurité. La formation et la sensibilisation des individus vont plus que jamais représenter une dimension essentielle de la sécurité du cyberespace dans les années à venir.

En France, les aspects formation et sensibilisation à la sécurité et aux usages du cyberespace sont aujourd'hui largement répandus dans les entreprises ayant une culture historique du risque SSI. Toutefois, de nombreuses entreprises, de plus en plus cyberdépendantes, n'ont pas cette culture et c'est encore plus vrai avec le grand public pour lequel cela demeure encore trop timide et retreint à des prises de conscience individuelles. Dans les années à venir, l'état français aura donc un rôle majeur à jouer pour mettre en œuvre une politique efficace dans ce domaine à l'instar de ce qui peut exister dans le domaine de la sécurité routière par exemple.

En plus des actions déjà menées dans le domaine professionnel, les principaux axes de cette politique devront concerner :

- l'intégration de la cybersécurité dans les cursus scolaires, depuis l'école élémentaire jusqu'aux formations universitaires, notamment sur la composante comportementale ;
- la réalisation de campagnes de sensibilisation récurrentes dans les médias avec un focus particulier sur les responsabilités et le rôle éducatif des parents ;
- l'intégration de modules cybersécurité obligatoires dans toutes les formations aux métiers de l'informatique et des télécoms. Actuellement, il s'agit d'une lacune majeure, notamment dans les métiers du développement logiciel. A noter l'initiative récente CYBEREDU[176] qui vise à apporter une composante cybersécurité dans les formations supérieures en informatique en France.

6.3. Normalisation et Conformité de la cybersécurité

Normalisation et conformité de la sécurité informatique sont des sujets déjà maitrisés par certains secteurs d'activités sensibles et critiques (exemple : le domaine militaire, le domaine bancaire, les opérateurs d'importance vitale). De manière générale, plusieurs référentiels normatifs existent déjà : série ISO27K, ISO 15408 (critères communs), PCI-DSS.

A horizon 2030, ce principe de normalisation et de conformité (sous-entendu la certification sécurité) devra être étendu sur un périmètre beaucoup plus large qu'aujourd'hui. En effet, la cyberdépendance croissante des citoyens, notamment sur le plan économique et social, nécessitera une plus grande maitrise étatique de la cybersécurité.

De manière générale, l'enjeu à venir sera donc de standardiser la sécurité avec des labels qui seraient fonction du contexte d'utilisation et de la réglementation sectorielle ; les objets connectés sont particulièrement concernés (par exemple, il n'existe aujourd'hui aucune contrainte sur le plan de la sécurité informatique pour commercialiser une webcam grand public ou un logiciel de navigation web). La principale difficulté sera probablement de définir des référentiels et des processus de qualification communs, au niveau européen voire international. Sur le plan européen, ne faudrait-il pas intégrer au marquage CE des exigences portant sur la cybersécurité des produits (matériels et logiciels) ?

[176] (Démarche CyberEdu : l'ANSSI élargit la sensibilisation à la cybersécurité !, 2014)

Les exigences de sécurité seraient essentiellement techniques (ex : algorithme de chiffrement, taille des clefs, qualité des générateurs d'aléas), mais pourraient aussi inclure d'autres notions :

- la garantie sur les conditions de développement logiciel (plateformes de développement, qualification et compétences des développeurs)
- la garantie de pouvoir disposer des mises à jour de sécurité sur une certaine durée et d'être informé pro-activement de leurs disponibilités
- la capacité à réaliser des audits de sécurité

Toutefois, il s'agit peut-être d'un vœu pieux, car ce type de démarche engendre des problématiques majeures :

- des surcouts financiers importants pour la conception et la fabrication des produits (matériels et logiciels) ;
- des délais supplémentaires dans le cycle de développement des produits (phases de qualification sécurité)
- un coût financier et humain pour les états (organismes de certification et de contrôle)
- le caractère obligatoire ou optionnel/informationnel des labels ?
- le cas particulier des produits open-source (absence de responsables) ?

Bref, cela constitue potentiellement un frein à l'innovation et au développement économique et certains acteurs du monde numérique s'en inquiètent déjà[177].

6.4. Stratégique et législatif

6.4.1. Cyber-stratégie

Les états devront jouer un rôle important dans la régulation et la gouvernance du futur cyberespace au risque de laisser croitre la cybercriminalité et la cyber-insécurité. Dans le futur, le rôle protecteur de l'état français envers ses citoyens dans le monde réel devra être renforcé dans le monde virtuel que constitue le cyberespace ; en effet, beaucoup de citoyens subissent la menace cyber, sont livrés à eux-mêmes et n'ont pas le temps ni les compétences nécessaires pour se défendre.

En outre, la France et plus largement l'Europe doivent recouvrer davantage de souveraineté qu'actuellement sur le cyberespace. Le rapport France numérique 2012-2020[178] préconise ainsi de faire émerger une gouvernance européenne et internationale de l'Internet, pour la rendre moins dépendante des Etats-Unis (cf. page 66 du rapport). L'ouverture récente de l'ICANN[179] pour le contrôle du DNS est une étape importante de ce processus d'internationalisation de la gouvernance d'Internet. Dans le domaine de la cybersécurité, il est important de mener une politique de reconquête industrielle, notamment sur les produits de sécurité, comme le préconise le plan 33 « cybersécurité »[180] soutenu par le gouvernement français.

[177] (Cybersécurité : frictions entre l'Etat et le monde numérique, 2014)
[178] (France numérique 2012-2020 / Bilan et Perspectives, MINEFI, 2011)
[179] (ICANN : les USA renoncent au contrôle du DNS racine, 2014)
[180] (AFDEL - Livre blanc « Filière cyber-sécurité en France » , 2014)

A horizon 2030, la cyber-stratégie visant à assurer davantage de souveraineté numérique devrait être majoritairement établie au niveau Européen. En effet, l'Union Européenne dispose d'un poids et d'atouts importants sur la scène internationale :

- elle est l'une des premières puissances économiques mondiales
- son marché intérieur (cyberéconomie) est très important
- elle concentre 7 des 10 plus gros nœuds de transit Internet à l'échelle mondiale
- elle est une zone de transit majeure vers d'autres continents (en particulier l'Afrique)

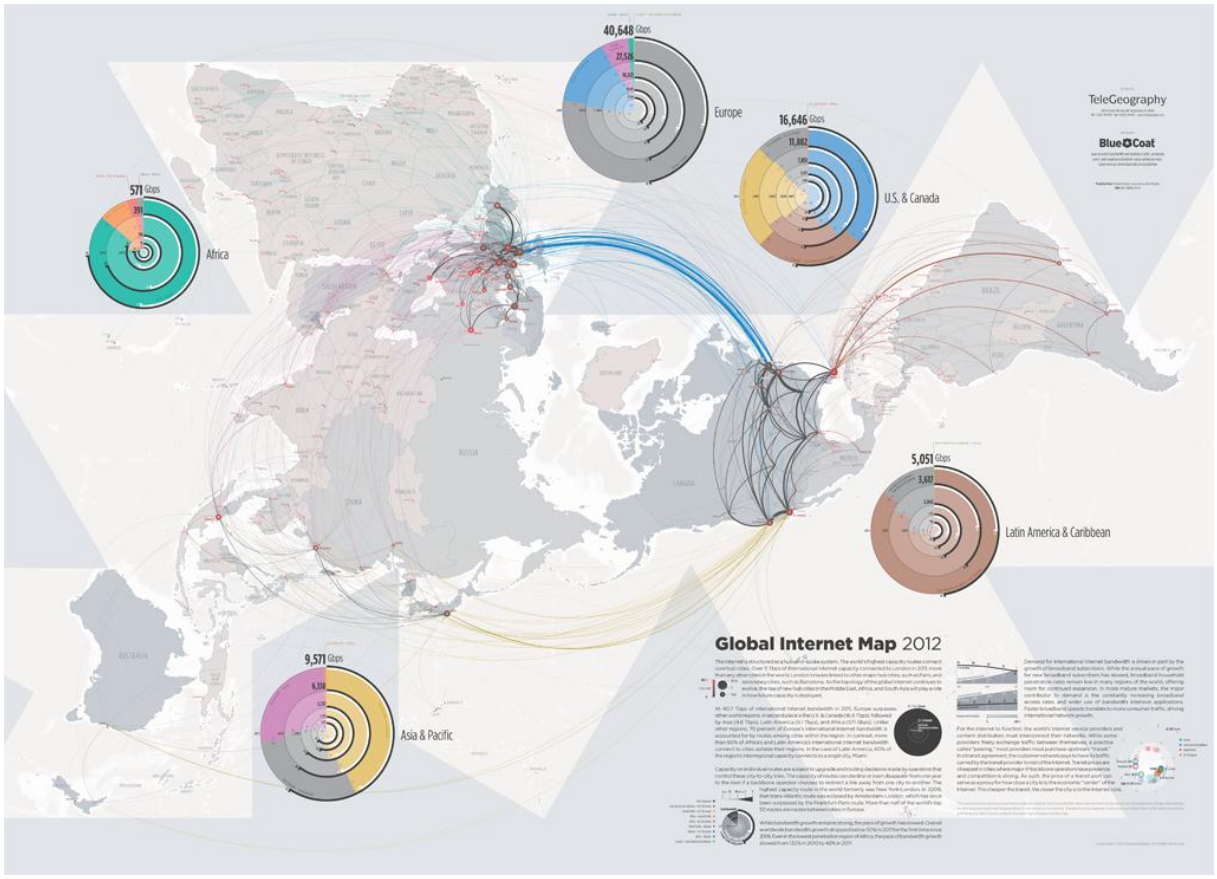

Figure 19 - répartition du trafic Internet mondial en 2012 (source TeleGeography[181])

Toutefois, les institutions européennes souffrent de plusieurs points faibles qui, aujourd'hui, ne favorisent pas l'émergence d'une cyber-stratégie commune :

- par nature, il y a des différences culturelles et économiques
- il existe des rapports de force internes et une compétition économique entre les pays (sur le plan fiscal par exemple)
- il n'y a pas de volonté politique effective au niveau de l'UE ; la tendance est plutôt de prôner un libéralisme économique semblable à celui des Etats-Unis.
- L'UE est trop bureaucratique (multiples organismes), ce qui complexifie et ralentit les prises de décisions

[181] (Global Internet Map 2012, 2012)

- la base industrielle dans le domaine numérique est en décroissance et loin derrière celle des autres grandes puissances que sont les Etats-Unis et la Chine

En conclusion, il ne pas attendre pendant des années une Europe qui a du mal à se décider. A l'instar de l'Allemagne[182], la France devrait prendre l'initiative d'assurer sa souveraineté numérique au niveau national avec la collaboration éventuelle d'autres pays partenaires. Une réelle politique industrielle dans le domaine du numérique est le socle de cette souveraineté ; elle doit porter en priorité sur le matériel (micro-électronique), le logiciel, les opérateurs télécoms, les fournisseurs de services (ex : le Cloud Souverain).

6.4.2. Balkanisation

La cyber-balkanisation est un concept de plus en plus évoqué, et parfois mis en œuvre par certains états (cf. §5.19). Le concept est encore flou, mais son but principal est de fournir à un état les moyens lui permettant de maitriser la souveraineté et la sécurité de l'Internet sur son territoire. Plusieurs leviers peuvent être utilisés :

- Le cloisonnement « perméable » : segmentation du réseau associé à un filtrage périphérique (notion de frontière numérique)
- La gouvernance des services critiques (exemples : DNS, BGP)
- La maitrise d'autorités de certification (X.509)
- la labélisation/certification des matériels, des logiciels, des services
- La localisation des services et des données

A horizon 2030, il serait ainsi possible d'imaginer plusieurs cyber-bulles avec différents niveaux de confiance à l'échelle nationale ou européenne. Ces différents réseaux seraient établis en fonction du contexte et de l'usage, par exemple :

- les systèmes industriels (exemple : les voitures connectées), les infrastructures critiques
- le e-commerce et le monde bancaire
- l'administratif/gouvernemental
- l'Internet ouvert (libre)

Une telle approche génère toutefois des problématiques majeures:

- Comment transposer ce principe de cloisonnement au niveau des terminaux sans compromettre la sécurité multi-niveaux ? (la virtualisation, le SaaS sont des axes de solution)
- Cela nécessite la mise en œuvre de passerelles pour échanger des informations entre les différents niveaux, notamment vers l'Internet ouvert (« Open Internet »)
- Le cout matériel et humain, potentiellement très élevé, est-il supportable par l'état français, l'UE ?
- Cela peut aggraver certains risques (perte de compétitivité de l'industrie nationale, isolement sur le plan international, frein à l'innovation, mouvements sociaux en raison de l'atteinte potentielle aux libertés individuelles)

[182] (L'Allemagne veut renforcer sa « souveraineté numérique », 2014)

A plus court terme, la France pourrait commencer par constituer un réseau dédié aux OIV avec des contraintes de sécurité fortes, afin d'assurer résilience et souveraineté. Sur ce réseau, des mesures telles que DNSSec et RPKI/BGPSec seraient obligatoires par exemple. Des autorités de certification (X.509) seraient mises à disposition ou contrôlées par des organismes étatiques. La certification des matériels et logiciels serait également un pilier important. Compte-tenu du développement des objets connectés, notamment dans le secteur industriel, un tel réseau devrait également inclure la composante mobile (LTE/5G). En Europe, le projet « Clean Pipe »[183] entamé par l'Allemagne semble être le plus avancé dans ce domaine.

Il est intéressant de noter que la Chine applique depuis des années certaines contraintes de cloisonnement et de sécurité très fortes (filtrage des flux, contrôle de la localisation, contrôle des autorités de certification, restrictions sur le chiffrement des flux) ; et cela n'empêche pas la Chine d'innover et de concurrencer les Etats-Unis (exemples : Allibaba, Baidu).

6.4.3. La localisation des services et des données

La localisation des services et des données est fondamentale pour assurer la souveraineté numérique d'une nation et garantir le respect de la loi sur un territoire donné (réglementation relative à la vie privée et aux données personnelles, fiscalité).

L'Union Européenne, en particulier la France, est aujourd'hui victime d'une évasion à grande échelle des données personnelles (et professionnelles) vers des pays où sa juridiction ne s'applique pas pleinement[184]. C'est pourquoi, à horizon 2030, à l'échelle nationale et européenne, il faudra clairement se poser la question de la relocalisation physique de certaines données et services (Datacenters) sur les territoires européens. Les initiatives de cloud souverain lancées en France (exemple : Cloudwatt[185]) constituent une première étape vers ce recouvrement de souveraineté. Des pays comme la Russie sont déjà plus avancés en projetant de rendre obligatoire d'ici 2016, le stockage de l'ensemble des données personnelles de ses concitoyens sur le territoire russe[186].

6.4.4. Evolution de la réglementation et de la fiscalité

A l'instar de ce qui existe déjà dans certains secteurs fortement réglementés comme l'industrie automobile ou le transport aérien, il devient important de disposer d'une réglementation efficace et cohérente au sein du cyberespace. Pour protéger les citoyens, les entreprises mais aussi l'état, de nouvelles mesures réglementaires sont évoquées :

- Autoriser la sécurité offensive (actuellement seule la sécurité défensive est autorisée sur le plan juridique)
- Réguler des solutions de chiffrement en fonction de l'usage et du contexte (puissance des algorithmes cryptographiques, séquestre ou droit d'accès étatique aux clés de chiffrement)
- Légiférer sur les usages BYOD

[183] (Clean Pipe : le bouclier anti NSA de Deutsche Telekom, sera finalisé pour 2016, 2014)
[184] (L'Union européenne, colonie du monde numérique ?, 2014)
[185] (Cloud souverain : cloudwatt, 2014)
[186] (Données personnelles : la Russie veut forcer la main des géants du Net, 2014)

- Renforcer les obligations en matière de protection de la vie privée (labellisation/certification des services, notion de « privacy management » au sein des entreprises, principe de container sécurisé et maitrisé par les individus)
- Revoir la fiscalité du numérique[187]. Exemple : Instauration d'une data-taxe[188] (digi-douane) sur les données personnelles transitant hors de l'Union Européenne.
- Imposer la domiciliation des entreprises numériques en Europe

Ces évolutions réglementaires, idéalement réalisées au niveau Européen (voire international) devront être accompagnées d'outils de prévention et de répression efficaces, notamment en termes de sanctions pénales. Cela sous-entend des moyens matériels et humains adaptés.

6.4.5. Lutte contre la cybercriminalité

La lutte contre la cybercriminalité est en évolution permanente ; elle doit notamment s'adapter aux nouvelles techniques et méthodes mises en œuvre pour commettre les crimes et délits. En France, un rapport produit en 2014 par un groupe de travail interministériel[189] identifie un certain nombre de mesures et recommandations pour garantir l'efficacité de la lutte contre la cybercriminalité sur le long terme et la protection du citoyen français dans le cyberespace. Les recommandations ont principalement pour objectif de fournir une réponse répressive plus efficace et mieux adaptée aux nouvelles méthodes des cyber-délinquants, tout en respectant les exigences liées à la protection des libertés fondamentales.

Les grands axes sont les suivants :

- Le développement de la coopération internationale, notamment par la mise en œuvre de procédures et dispositifs communs. Cela nécessite au préalable, la définition d'accords internationaux, à l'instar de la convention qui existe déjà au niveau européen[190] ;
- Une politique pénale plus répressive et adaptée à l'écosystème actuel de la cyber-délinquance et plus globalement de la cybercriminalité ;
- Une politique de prévention et de formation (entreprises, particuliers, étudiants …). Le projet CYBEREDU[191] de l'ANSSI qui propose des formations en cybersécurité pour les étudiants des métiers de l'informatique s'inscrit dans ce contexte ;
- Une coopération accrue entre les acteurs concernés (acteurs étatiques, fournisseurs de services, opérateurs de télécommunications, développeurs logiciels, universités). Cela comprend davantage de communication et de transparence entre ces acteurs, notamment par rapport aux incidents de sécurité rencontrés. L'association française CECYF[192], crée en 2014, œuvre en ce sens ;
- Des moyens techniques et humains adaptés. Cela passe notamment par des outils d'analyse forensique efficaces et performants. Pour renforcer les moyens étatiques, la labellisation « Forensique » d'entreprises du secteur privé est une piste envisagée.

[187] (Minefi - Mission d'expertise sur la fiscalité de l'économie numérique, 2013)
[188] (L'Internet industriel, Pierre BELLANGER, 2013)
[189] (Protéger les INTERNAUTES - Rapport sur la cybercriminalité, 2014)
[190] (Conseil de l'Europe - Convention sur la cybercriminalité, 2001)
[191] (ANSSI - CYBEREDU, 2014)
[192] (CECYF - Centre Expert contre la Cybercriminalité Français, 2014)

A. Annexe - Références

Ces sources ont été utilisées pour la réalisation de l'étude.

The Little Black Book of Computer Viruses - Mark A. Ludwig. (1991). Récupéré sur http://www.cin.ufpe.br/~mwsa/arquivos/THE_LITTLE_BLACK__BOOK_OF_C.PDF

BCP 38 - Network Ingress Filtering : Defeating Denial of Service Attacks which employ IP Source Address Spoofing. (2000). Récupéré sur http://tools.ietf.org/html/bcp38

Conseil de l'Europe - Convention sur la cybercriminalité. (2001). Récupéré sur http://www.droit-technologie.org/upload/legislation/doc/82-1.pdf

IETF - SMTP Service Extension for Secure SMTP over Transport Layer Security . (2002). Récupéré sur https://tools.ietf.org/html/rfc3207

IETF Opsec Working Group. (2004). Récupéré sur https://tools.ietf.org/wg/opsec/

A Border Gateway Protocol 4 (BGP-4) - RFC4271. (2006). Récupéré sur http://tools.ietf.org/html/rfc4271

BGP Best Practices. (2006). Récupéré sur http://www.ripe.net/ripe/meetings/regional-meetings/manama-2006/BGPBCP.pdf

ANSSI CERT-FR - Du bon usage du DNS. (2008). Récupéré sur http://www.cert.ssi.gouv.fr/site/CERTA-2008-INF-002/

Attaques en DDoS : De l'Estonie à la Géorgie. (2008). Récupéré sur http://www.orange-business.com/fr/blogs/securite/securite-des-reseaux/attaques-en-ddos-de-lestonie-a-la-georgie/

DNS : types d'attaques et techniques de sécurisation. (2009). Récupéré sur http://www.afnic.fr/medias/documents/afnic-dossier-dns-attaques-securite-2009-06.pdf

Le lithium en Bolivie : quels enjeux stratégiques ? (2009). Récupéré sur http://www.infoguerre.fr/matrices-strategiques/lithium-bolivie-strategie-energie/

RFC 5575 : Dissemination of Flow Specification Rules. (2009). Récupéré sur http://www.ietf.org/rfc/rfc5575.txt

Le coût écologique d'Internet. (2010). Récupéré sur http://www.pourlascience.fr/ewb_pages/a/article-le-cout-ecologique-d-internet-24104.php

ANSSI - Architecture DNS sécurisée. (2011). Récupéré sur https://www.sstic.org/media/SSTIC2011/SSTIC-actes/architecture_dns_scurise/SSTIC2011-Article-architecture_dns_scurise-valadon_perez.pdf

Certificats SSL frauduleux et piratage d'autorités de certification : décryptage. (2011). Récupéré sur http://www.zdnet.fr/actualites/certificats-ssl-frauduleux-et-piratage-d-autorites-de-certification-decryptage-39763617.htm

Courbes elliptiques : un nouveau virage pour le chiffrement. (2011). Récupéré sur http://www.01net.com/editorial/143980/courbes-elliptiques-un-nouveau-virage-pour-le-chiffrement/

Des certificats SSL frauduleux de Comodo autorisent des attaques contre les Webmails. (2011). Récupéré sur http://www.zdnet.fr/actualites/des-certificats-ssl-frauduleux-de-comodo-autorisent-des-attaques-contre-les-webmails-39759360.htm

France numérique 2012-2020 / Bilan et Perspectives, MINEFI. (2011). Récupéré sur http://www.entreprises.gouv.fr/secteurs-professionnels/plan-france-numerique-2012-2020-bilan-et-perspectives-novembre-2011

Hack de pompe à insuline. (2011). Récupéré sur http://korben.info/medtronic-hack.html

Plus de 500 certificats SSL dérobés à une autorité de certification. (2011). Récupéré sur http://www.zdnet.fr/actualites/plus-de-500-certificats-ssl-derobes-a-une-autorite-de-certification-39763572.htm

Apple prêt à collaborer avec les opérateurs sur une mini carte SIM. (2012). Récupéré sur http://www.latribune.fr/technos-medias/electronique/20110520trib000623193/apple-pret-a-collaborer-avec-les-operateurs-sur-une-mini-carte-sim.html

Bruxelles veut imposer l'oubli numérique. (2012). Récupéré sur http://www.lemonde.fr/technologies/article/2012/01/25/bruxelles-veut-imposer-l-oubli-numerique_1634487_651865.html

CSA - Les Français et la criminalité identitaire. (2012). Récupéré sur http://www.csa.eu/multimedia/data/sondages/data2012/opi20120830-Les-francais-et-la-criminalite-identitaire.pdf

Cybercensure et balkanisation du Web. (2012). Récupéré sur http://www.ina-expert.com/e-dossier-de-l-audiovisuel-journalisme-internet-libertes/cybercensure-et-balkanisation-du-web.html

DNSSEC Error Caused NASA Website To Be Blocked. (2012). Récupéré sur http://www.darkreading.com/risk/dnssec-error-caused-nasa-website-to-be-blocked/d/d-id/1136990?

Global Internet Map 2012. (2012). Récupéré sur https://www.telegeography.com/assets/website/images/maps/global-internet-map-2012/global-internet-map-2012-x.png

HSBC visée par des hackers « justiciers ». (2012). Récupéré sur http://maviemonargent.info/2012/hsbc-visee-par-des-hackers-justiciers

L'antivirus, technologie à bout de souffle ? (2012). Récupéré sur http://www.e-xpertsolutions.com/e-news/lantivirus-technologie-a-bout-de-souffle

National Intelligence Council : Global Trends 2030: Alternative Worlds - page 86. (2012). Récupéré sur http://globaltrends2030.files.wordpress.com/2012/11/global-trends-2030-november2012.pdf

Panne géante d'Orange : les dessous techniques de l'incident. (2012). Récupéré sur http://www.journaldunet.com/solutions/securite/panne-d-orange-l-explication-technique-0712.shtml

RFC 6483 - Validation of Route Origination Using the Resource Certificate Public Key Infrastructure (PKI) and Route Origin Authorizations (ROAs). (2012). Récupéré sur http://tools.ietf.org/html/rfc6483

The Digital Universe in 2020 : BigData, Bigger Digital Shadows and Biggest Growth in the Far East - United States. (2012). Récupéré sur http://www.emc.com/collateral/analyst-reports/idc-digital-universe-united-states.pdf

Un appareil qui intercepte les informations transitant via la fibre optique. (2012). Récupéré sur http://www.agenceecofin.com/securite/2412-8175-un-appareil-qui-intercepte-les-informations-transitant-via-la-fibre-optique

Vos données personnelles valent 315 milliards d'euros. (2012). Récupéré sur http://www.01net.com/editorial/579867/vos-donnees-personnelles-valent-315-milliards-d-euros/

80 milliards d'objets connectés en 2020. (2013). Récupéré sur http://www.zdnet.fr/actualites/80-milliards-d-objets-connectes-en-2020-39793776.htm

AFNIC - Sécuriser les communications sur Internet de bout-en-bout avec le protocole DANE. (2013). Récupéré sur http://www.afnic.fr/medias/documents/Dossiers_pour_breves_et_CP/dossier-thematique12_VF1.pdf

Alert (TA13-088A) - DNS Amplification Attacks. (2013). Récupéré sur https://www.us-cert.gov/ncas/alerts/TA13-088A

ANSSI - Influence des bonnes pratiques sur les incidents (§4). (2013). Récupéré sur http://www.ssi.gouv.fr/IMG/pdf/Influence_des_bonnes_pratiques_sur_les_influences_BGP_article.pdf

ANSSI - Résilience de l'Internet français. (2013). Récupéré sur http://www.ssi.gouv.fr/IMG/pdf/Rapport_Observatoire_2013.pdf

Brazil plans to go offline from US-centric internet . (2013). Récupéré sur http://www.thehindu.com/news/international/world/brazil-plans-to-go-offline-from-uscentric-internet/article5137689.ece

CNIL Innovation et Prospective : Vie privée à l'horizon 2020. (2013). Récupéré sur http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/DEIP/CNIL-CAHIERS_IPn1.pdf

Darknet, un internet clandestin à portée de clics. (2013). Récupéré sur http://ecs-paris.com/blogs/digicom-2012/actus-2-0/darknet-internet-clandestin-a-portee-de-clics

Espionnage : pour casser les clefs de chiffrement, la NSA a dû "tricher". (2013). Récupéré sur http://www.lemonde.fr/technologies/article/2013/09/06/pour-casser-les-clefs-de-chiffrement-la-nsa-a-du-tricher_3472728_651865.html

Fleur Pellerin veut une taxe Internet pour 2014. (2013). Récupéré sur http://www.irma.asso.fr/Fleur-Pellerin-veut-une-taxe

General Electric : INDUSTRIAL INTERNET - A European Perspective - Pushing the Boundaries of Minds and Machines. (2013). Récupéré sur http://www.ge.com/europe/downloads/IndustrialInternet_AEuropeanPerspective.pdf

Information-Centric Networking Research Group. (2013). Récupéré sur https://irtf.org/icnrg

La dynamique d'internet - Prospective 2030, Télécom ParisTech. (2013). Récupéré sur http://www.strategie.gouv.fr/publications/dynamique-dinternet-prospective-2030

Le défibrillateur de Dick Cheney modifié par crainte d'un assassinat par piratage. (2013). Récupéré sur http://www.lequotidiendumedecin.fr/actualite/international/le-defibrillateur-de-dick-cheney-modifie-par-crainte-d-un-assassinat-par-pir

Le modèle sécurite Zéro Trust - Le nouveau paradigme sécurite. (2013). Récupéré sur http://www.e-xpertsolutions.com/e-news/le-modele-securite-zero-trust-le-nouveau-paradigme-securite

Les câbles sous-marins, clé de voûte de la cybersurveillance. (2013). Récupéré sur http://www.lemonde.fr/technologies/article/2013/08/23/les-cables-sous-marins-cle-de-voute-de-la-cybersurveillance_3465101_651865.html

Les opérateurs mobiles avalisent la spécification Embedded SIM dédiée au marché M2M. (2013). Récupéré sur http://www.lembarque.com/les-operateurs-mobiles-avalisent-la-specification-embedded-sim-dediee-au-marche-m2m_001439

L'Internet industriel, Pierre BELLANGER. (2013). Récupéré sur http://cast.skyrock.net/pierrebellanger/L_Internet_industriel.pdf

M2M et e-Santé : la médecine de demain. (2013). Récupéré sur http://www.orange-business.com/fr/blogs/usages-dentreprise/machine-to-machine/m2m-et-e-sante-la-medecine-de-demain

Minefi - Mission d'expertise sur la fiscalité de l'économie numérique. (2013). Récupéré sur http://www.economie.gouv.fr/files/rapport-fiscalite-du-numerique_2013.pdf

Public Key Pinning for TLS. (2013). Récupéré sur http://www.delaat.net/rp/2012-2013/p56/report.pdf

Réguler le Web : la très mauvaise réponse inspirée aux Etats par le scandale de la NSA. (2013). Récupéré sur http://www.atlantico.fr/decryptage/reguler-web-tres-mauvaise-reponse-inspiree-aux-etats-scandale-nsa-erwan-noan-904971.html

Résilience de l'Internet français §2.3 Taux de pénétration de DNSSEC. (2013). Récupéré sur http://www.ssi.gouv.fr/IMG/pdf/Rapport_Observatoire_2013.pdf

Sécurité informatique : ces nouveaux dangers qui guettent nos entreprises. (2013). Récupéré sur http://business.lesechos.fr/directions-numeriques/0202902365881-securite-informatique-ces-nouveaux-dangers-qui-guettent-nos-entreprises-8094.php

SKYPE refuse de se déclarer en tant qu'opérateur. (2013). Récupéré sur http://www.arcep.fr/index.php?id=8571&L=0&tx_gsactualite_pi1[uid]=1593&cHash=776a7927e2d50b767ddd1ca984967194http://www.latribune.fr/technos-medias/telecoms/20130312trib000753595/pour-l-arcep-skype-est-un-operateur-telephonique-la-justice-est-saisie.html

The New Threat: Targeted Internet Traffic Misdirection. (2013). Récupéré sur http://www.renesys.com/2013/11/mitm-internet-hijacking/

Une énorme faille de l'Internet permet de détourner du trafic à volonté. (2013). Récupéré sur http://www.lerefugeinformatique.fr/?p=58

Université Amsterdam - Public Key Pinning for TLS Using a Trust on First Use Model. (2013). Récupéré sur http://www.delaat.net/rp/2012-2013/p56/report.pdf

Université de Strasbourg - Sécuriser le routage sur Internet. (2013). Récupéré sur http://www.guiguishow.info/wp-content/uploads/2013/09/RPKI-ROA/Rapport/Rapport-securiser-routage-internet.pdf

Véronique Cayla (Arte) prône la résistance à Google et autres prédateurs numériques. (2013). Récupéré sur http://www.afp.com/fr/node/2762525/

Vifib joue la carte du cloud réparti. (2013). Récupéré sur http://business.lesechos.fr/directions-numeriques/vifib-joue-la-carte-du-cloud-reparti-5936.php

Wikipedia - IP Multimedia Subsystem. (2013). Récupéré sur http://fr.wikipedia.org/wiki/IP_Multimedia_Subsystem

Wikipedia - Révélations d'Edward Snowden. (2013). Récupéré sur http://fr.wikipedia.org/wiki/R%C3%A9v%C3%A9lations_d%27Edward_Snowden

4G white-spaces. (2014). Récupéré sur http://4g-portal.com/tag/white-spaces

5G PPP. (2014). Récupéré sur http://5g-ppp.eu/

AFDEL - Livre blanc « Filière cyber-sécurité en France » . (2014). Récupéré sur http://www.afdel.fr/actualites/categorie/actualite-afdel/article/livre-blanc-filiere-cyber-securite-en-france-l-afdel-appelle-les-pouvoirs-publics-a-ne-pas-tourner-le-dos-aux-forces-du-marche

Alerte aux cyberattaques sur les marchés. (2014). Récupéré sur http://www.lesechos.fr/journal20140826/lec2_finance_et_marches/0203722357562-alerte-aux-cyberattaques-sur-les-marches-1035930.php

ANSSI - Analyse de la sécurité des modems des terminaux mobiles. (2014). Récupéré sur http://www.ssi.gouv.fr/IMG/pdf/Benoit_Michau_-_Securite_des_modems_des_terminaux_mobiles.pdf

ANSSI - CYBEREDU. (2014). Récupéré sur http://www.ssi.gouv.fr/fr/menu/actualites/colloque-cyberedu-de-l-anssi-18-au-20-novembre-2014-a-paris.html

ANSSI - Référentiel Général de Sécurité v2.0 - Annexe B1 - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques. (2014). Récupéré sur http://www.ssi.gouv.fr/IMG/pdf/RGS_v-2-0_B1.pdf

Apple Can't And Won't Provide Access To iPhone Data To Authorities, Even With A Warrant. (2014). Récupéré sur http://www.ibtimes.com/apple-cant-wont-provide-access-iphone-data-authorities-even-warrant-1691221

Après Target : un nouveau malware cible les lignes de caisses. (2014). Récupéré sur http://www.silicon.fr/securite-malware-backoff-ups-caisses-cartes-96214.html

Attaque DDoS de 400 Gbits/s avec amplification NTP : terrifiante de simplicité. (2014). Récupéré sur http://www.viruslist.com/fr/news?id=197471133

Attaques DNS : Connaître son ennemi. (2014). Récupéré sur http://pro.01net.com/editorial/625164/attaques-dns-connaitre-son-ennemi/

Axa entrouvre la porte de l'utilisation des objets connectés dans l'assurance. (2014). Récupéré sur http://www.usine-digitale.fr/article/axa-entrouvre-la-porte-de-l-utilisation-des-objets-connectes-dans-l-assurance.N266435

BGP in 2013 - The Churn Report . (2014). Récupéré sur http://www.potaroo.net/ispcol/2014-02/upds.html

CECYF - Centre Expert contre la Cybercriminalité Français. (2014). Récupéré sur http://www.cecyf.fr/

Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013–2018. (2014). Récupéré sur http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html

Clean Pipe : le bouclier anti NSA de Deutsche Telekom, sera finalisé pour 2016. (2014). Récupéré sur http://www.silicon.fr/clean-pipe-bouclier-numerique-deutsche-telekom-finalise-2016-91976.html

Cloud souverain : cloudwatt. (2014). Récupéré sur https://www.cloudwatt.com/fr/

CNIL : Le G 29 publie un avis sur les techniques d'anonymisation. (2014). Récupéré sur http://www.cnil.fr/linstitution/actualite/article/article/le-g-29-publie-un-avis-sur-les-techniques-danonymisation/

CNIL Innovation et Prospective : Intimité et vie privée du travailleur connecté : BYOD, capteurs, sécurité. (2014). Récupéré sur http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/DEIP/Lettre_IP_n___7___Intimite_et_vie_privee_du_travailleur_connecte.pdf

CNIL Innovation et Prospective : Le corps, nouvel objet connecté. (2014). Récupéré sur http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/DEIP/CNIL_CAHIERS_IP2_WEB.pdf

Commission Européenne : Trusted Cloud Europe. (2014). Récupéré sur http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=4935

Cryptographie et objets connectés font ils bon ménage ? . (2014). Récupéré sur http://www.orange-business.com/fr/blogs/securite/securite-applicative/cryptographie-et-objets-connectes-font-ils-bon-menage-

Cybersécurité : frictions entre l'Etat et le monde numérique. (2014). Récupéré sur http://www.lesechos.fr/tech-medias/hightech/0203969133313-cybersecurite-frictions-entre-letat-et-le-monde-numerique-1068536.php

DDoS et smartphones : rien ne sera plus jamais comme avant. (2014). Récupéré sur http://www.orange-business.com/fr/blogs/securite/mobilite/quand-la-technologie-se-met-au-service-des-hackers

Démarche CyberEdu : l'ANSSI élargit la sensibilisation à la cybersécurité ! (2014). Récupéré sur http://www.ssi.gouv.fr/fr/menu/actualites/demarche-cyberedu-l-anssi-elargit-la-sensibilisation-a-la-cybersecurite.html

Déployer DNSSEC, comment, quoi, où ? (2014). Récupéré sur http://www.afnic.fr/medias/documents/DNSSEC/afnic-dnssec-howto-fr-v2.pdf

Des armes à feu compatibles avec les Google Glass. (2014). Récupéré sur http://www.lesechos.fr/05/06/2014/lesechos.fr/0203545375739_des-armes-a-feu-compatibles-avec-les-google-glass.htm

Des règles plus strictes pour protéger les données personnelles à l'ère numérique. (2014). Récupéré sur http://www.europarl.europa.eu/news/fr/news-room/content/20140307ipr38204/html

Des trous de sécurité trouvés dans 14 antivirus. (2014). Récupéré sur http://www.silicon.fr/trous-securite-trouves-14-antivirus-95880.html

Devenu trop grand, Internet a subi des perturbations. (2014). Récupéré sur http://www.lemonde.fr/pixels/article/2014/08/15/devenu-trop-grand-internet-est-tombe-en-panne_4472153_4408996.html

Digital Life in 2025 - Cyber Attacks likely to Increase. (2014). Récupéré sur http://www.pewinternet.org/files/2014/10/PI_FutureofCyberattacks_1029141.pdf

Docker. (2014). Récupéré sur https://www.docker.com/whatisdocker/

Données personnelles : la Russie veut forcer la main des géants du Net. (2014). Récupéré sur http://www.lefigaro.fr/secteur/high-tech/2014/07/07/01007-20140707ARTFIG00234-donnees-personnelles-la-russie-veut-forcer-la-main-des-geants-du-net.php

Dragonfly : après Stuxnet, nouvelle attaque réussie contre les systèmes Scada. (2014). Récupéré sur http://www.silicon.fr/apres-stuxnet-nouvelle-attaque-reussie-contre-les-systemes-scada-95359.html

DSI : préparez-vous contre les Cyber-attaques. (2014). Récupéré sur http://www2.deloitte.com/fr/fr/pages/presse/2014/dsi-preparez-vous-contre-les-cyber-attaques.html

Dynamic Searchable Encryption via Blind Storage. (2014). Récupéré sur https://eprint.iacr.org/2014/219.pdf

EC3 : the 2014 Internet Organised Crime Threat Assessment (iOCTA). (2014). Récupéré sur https://www.europol.europa.eu/iocta/2014/toc.html

Etats-Unis: l'espionnage risque de «casser internet», prévient un dirigeant de Google. (2014). Récupéré sur http://www.20minutes.fr/monde/1457401-20141009-usa-espionnage-risque-casser-internet-previent-dirigeant-google

ETSI - Cellular encryption algorithms. (2014). Récupéré sur http://www.etsi.org/services/security-algorithms/cellular-algorithms

Europe : un pas de plus vers la balkanisation d'Internet. (2014). Récupéré sur http://www.lemagit.fr/actualites/2240214657/Europe-un-pas-de-plus-vers-la-balkanisation-dInternet

Europol prédit une vague de cybercrimes par objets connectés. (2014). Récupéré sur http://www.silicon.fr/europol-predit-vague-cybercrimes-objets-connectes-98698.html

F-Secure - Malwares analysis Report - Regin. (2014). Récupéré sur https://www.f-secure.com/documents/996508/1030745/w64_regin_stage_1.pdf

G.A.F.A. l'acronyme d'un quatuor qui accapare notre existence. (2014). Récupéré sur http://www.agoravox.fr/tribune-libre/article/g-a-f-a-l-acronyme-d-un-quatuor-147955

Gartner - pour le SDN, la sécurité n'est pas prête. (2014). Récupéré sur http://www.silicon.fr/dhoinne-gartner-sdn-securite-pas-prete-96692.html

Global Internet Phenomena Report. (2014). Récupéré sur https://www.sandvine.com/trends/global-internet-phenomena/

Google veut amener le wifi en Afrique subsaharienne avec des ballons dirigeables. (2014). Récupéré sur http://www.20minutes.fr/insolite/1164095-20130529-google-veut-amener-wifi-afrique-subsaharienne-ballons-dirigeables

Google veut tisser un réseau de satellites pour l'Internet pour tous. (2014). Récupéré sur http://www.silicon.fr/google-veut-diffuser-linternet-haut-debit-satellites-94744.html

GSMA - Fraud & Security. (2014). Récupéré sur http://www.gsma.com/technicalprojects/fraud-security

GSMA - Remote SIM Provisioning for Machine to Machine. (2014). Récupéré sur http://www.gsma.com/connectedliving/embedded-sim/

ICANN : les USA renoncent au contrôle du DNS racine. (2014). Récupéré sur www.numerama.com/magazine/28768-icann-les-usa-renoncent-au-controle-du-dns-racine.html

IEEE ISCC 2014 "Internet Traffic Analysis : A Case Study From Two Major European Operators. (2014). Récupéré sur http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=6912519

Internet World Stats. (2014). Récupéré sur http://www.internetworldstats.com/stats.htm

Krach d'octobre 1987. (2014). Récupéré sur http://fr.wikipedia.org/wiki/Krach_d%27octobre_1987

L'Allemagne veut renforcer sa « souveraineté numérique ». (2014). Récupéré sur http://www.lesechos.fr/20/08/2014/lesechos.fr/0203714354480_l-allemagne-veut-renforcer-sa---souverainete-numerique--.htm

L'antivirus est mort, dit Symantec. (2014). Récupéré sur http://www.01net.com/editorial/619276/l-antivirus-est-mort-dit-symantec/

La Chine et les USA construisent leurs premiers réseaux quantiques. (2014). Récupéré sur http://www.tomshardware.fr/articles/quantique-reseau-usa-chine,1-54904.html

La cybersécurité est une question de souveraineté, selon Guillaume Poupard. (2014). Récupéré sur http://www.usine-digitale.fr/article/la-cybersecurite-est-une-question-de-souverainete-selon-guillaume-poupard.N264163

La Hongrie veut taxer l'utilisation d'Internet. (2014). Récupéré sur http://www.numerama.com/magazine/31035-la-hongrie-veut-taxer-l-utilisation-d-internet.html

La NSA veut créer un ordinateur quantique pour pouvoir tout décrypter. (2014). Récupéré sur http://www.01net.com/editorial/611146/la-nsa-veut-creer-un-ordinateur-quantique-pour-pouvoir-tout-decrypter/

La pilule du futur sera une puce contraceptive... télécommandée ! (2014). Récupéré sur http://www.industrie-techno.com/la-pilule-du-futur-sera-une-puce-contraceptive-telecommandee.31141

La vidéosurveillance vous fait flipper ? Attendez de voir ce qu'on vous prépare. (2014). Récupéré sur http://rue89.nouvelobs.com/2014/04/25/videosurveillance-fait-flipper-attendez-voir-quon-prepare-251745

L'actuelle bataille des câbles préfigure-t-elle le cyberespace de 2030 ? . (2014). Récupéré sur http://si-vis.blogspot.fr/2014/11/lactuelle-bataille-des-cables-prefigure.html?m=1

Le chiffrement homomorphe. (2014). Récupéré sur http://linuxfr.org/news/le-chiffrement-homomorphe

Le hack géant de la banque JPMorgan Chase a touché 76 millions de clients. (2014). Récupéré sur http://www.20minutes.fr/high-tech/1453995-20141003-hack-geant-banque-jpmorgan-chase-touche-76-millions-clients

Le piratage des voitures autonomes pourrait mener... au chaos routier. (2014). Récupéré sur http://www.01net.com/editorial/633766/le-piratage-des-voitures-autonomes-pourrait-mener-au-chaos-routier/

Le programme hôpital numérique. (2014). Récupéré sur http://www.sante.gouv.fr/le-programme-hopital-numerique.html

Legifrance - Obligations des opérateurs. (2014). Récupéré sur http://www.legifrance.gouv.fr/affichCode.do?idArticle=LEGIARTI000006464073&idSectionTA=LEGISCTA000006181878&cidTexte=LEGITEXT000006070987&dateTexte=20090217

Les limites des Bitcoins. (2014). Récupéré sur http://www.trader-finance.fr/dossier/investissement/les-limites-des-bitcoins.html

Les objets connectés, future cible des hackers. (2014). Récupéré sur http://www.latribune.fr/opinions/tribunes/20140429trib000827485/les-objets-connectes-future-cible-des-hackers.html

Les risques cyber pourraient provoquer un choc mondial (étude Zurich) . (2014). Récupéré sur http://cyber-serenite.fr/actualites/les-risques-cyber-pourraient-provoquer-un-choc-mondial-etude-zurich

Les risques pour le monde en 2014 : Le cybergeddon. (2014). Récupéré sur http://gestion-crise.emoveo.fr/2014/01/16/les-risques-pour-le-monde-en-2014-le-risque-de-cyberattaque/

Les spécialistes s'inquiètent sur la sécurité d'Internet: D'ici 2025, une cyber-attaque pourrait provoquer des morts. (2014). Récupéré sur http://www.rtl.be/info/monde/international/1137216/les-specialistes-s-inquietent-sur-la-securite-d-internet-d-ici-2025-une-cyber-attaque-pourrait-provoquer-des-morts-

Leveraging SDN for Efficient Anomaly Detection and Mitigation on Legacy Networks. (2014). Récupéré sur http://www.netmode.ntua.gr/publications/LeveragingSDNforEfficientAnomalyDetectionandMitigationonLegacyNetworks.pdf

List of government mass surveillance projects. (2014). Récupéré sur http://en.wikipedia.org/wiki/List_of_government_mass_surveillance_projects

L'OTAN prévoit une réaction militaire contre les cyberattaques. (2014). Récupéré sur http://www.numerama.com/magazine/30460-l-otan-prevoit-une-reaction-militaire-contre-les-cyberattaques.html

L'Union européenne, colonie du monde numérique ? (2014). Récupéré sur http://www.senat.fr/rap/r12-443/r12-4434.html

Mimo connecte votre bébé. (2014). Récupéré sur http://www.journaldugeek.com/2014/05/19/mimo-connecte-votre-bebe/

Net Losses : Estimating the Global Cost of Cybercrime. (2014). Récupéré sur http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

Netflix quitte le Luxembourg et s'installera aux Pays-Bas en 2015. (2014). Récupéré sur http://www.nextinpact.com/news/87695-netflix-europe-quitte-luxembourg-et-sinstallera-aux-pays-bas-en-2015.htm

Neutralité du Net. (2014). Récupéré sur http://www.laquadrature.net/fr/neutralite_du_Net

NOMS 2014 - IEEE Network Operations and Management Symposium – Cracovie /Pologne. (2014). Récupéré sur http://noms2014.ieee-noms.org/

Opendaylight project. (2014). Récupéré sur http://www.opendaylight.org

Operation Auroragold - How the NSA Hacks Cellphone Networks Worldwide. (2014). Récupéré sur https://firstlook.org/theintercept/2014/12/04/nsa-auroragold-hack-cellphones/

PAYD : Pay as you drive. (2014). Récupéré sur http://fr.wikipedia.org/wiki/Pay_as_you_drive

PayPal et Ebay répondent à Apple Pay avec le BitCoin. (2014). Récupéré sur http://www.moneticien.com/commerce-et-paiement-electronique/paypal-et-ebay-repondent-a-apple-pay-avec-le-bitcoin/

Première norme sur la softwarization du réseau 'SDN' et la connectivité à la demande. (2014). Récupéré sur http://www.orange-business.com/fr/blogs/cloud-computing/normes-standards-et-certification/premiere-norme-sur-la-softwarization-du-reseau-sdn-et-la-connectivite-la-demande

Premiers livrables ETSI concernant la virtualisation de fonctions réseau. (2014). Récupéré sur http://www.orange-business.com/fr/blogs/cloud-computing/normes-standards-et-certification/premiers-livrables-etsi-concernant-la-virtualisation-de-fonctions-reseau

Protéger les INTERNAUTES - Rapport sur la cybercriminalité. (2014). Récupéré sur http://www.justice.gouv.fr/include_htm/pub/rap_cybercriminalite.pdf

Reporters sans frontières - Les enemis d'Internet. (2014). Récupéré sur http://12mars.rsf.org/2014-fr/wp-content/uploads/FR_RAPPORT_INTERNET_BD.pdf

Self-Stabilizing Virtual Machine Hypervisor Architecture for Resilient Cloud. (2014). Récupéré sur http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6903266

Sénat : L'ère du soupçon et les efforts de « containment » du risque de balkanisation du web. (2014). Récupéré sur http://www.senat.fr/rap/r13-696-1/r13-696-19.html

Serveur racine du DNS. (2014). Récupéré sur http://fr.wikipedia.org/wiki/Serveur_racine_du_DNS

Shellshock, la nouvelle faille qui inquiète Internet. (2014). Récupéré sur http://www.slate.fr/story/92601/bash-nouveau-bug-pire-heartbleed

Submarine Cable Map. (2014). Récupéré sur http://www.submarinecablemap.com/

Target : un sinistre cyber américain estimé à plus de 1Md$. (2014). Récupéré sur http://www.argusdelassurance.com/acteurs/target-un-sinistre-cyber-americain-estime-a-plus-de-1md.72088

Thales parie sur l'Internet à bord des avions pour faire décoller son chiffre d'affaires. (2014). Récupéré sur http://www.lemonde.fr/economie/article/2014/07/16/thales-parie-sur-l-internet-a-bord-des-avions-pour-faire-decoller-son-chiffre-d-affaires_4458248_3234.html

The 'Balkanisation' of Russia's internet. (2014). Récupéré sur https://www.opendemocracy.net/od-russia/alexandra-kulikova/%E2%80%98balkanisation%E2%80%99-of-russia%E2%80%99s-internet

The Communications Security, Reliability and Interoperability Council. (2014). Récupéré sur http://transition.fcc.gov/pshs/advisory/csric/

The World in 2014 : ICT Facts and Figures 2014. (2014). Récupéré sur http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf

Un patient israélien reçoit un nouveau pacemaker « connecté ». (2014). Récupéré sur http://fr.timesofisrael.com/un-patient-israelien-recoit-un-nouveau-pacemaker-connecte

Une nouvelle faille découverte dans OpenSSL. (2014). Récupéré sur http://www.linformaticien.com/actualites/id/33361/une-nouvelle-faille-decouverte-dans-openssl.aspx

Une tempête solaire a frôlé la Terre en 2012. (2014). Récupéré sur http://www.lefigaro.fr/flash-actu/2014/07/25/97001-20140725FILWWW00398-une-tempete-solaire-a-frole-la-terre-en-2012.php

Verizon - 2014 Data breach investigations report. (2014). Récupéré sur http://www.verizonenterprise.com/DBIR/2014/reports/rp_dbir-2014-executive-summary_en_xg.pdf

Virtualization is dead, long live containerization. (2014). Récupéré sur http://diginomica.com/2014/07/02/virtualization-dead-long-live-containerization/#.VEEZ4hDR7r4

VoLTE : des appels via 4G améliorés, le point chez les 4 opérateurs. (2014). Récupéré sur http://www.clubic.com/reseau-mobile/4g/actualite-713739-volte-appels-voix-4g-recapitulatif.html

WebRTC : introduction et modèle de sécurité. (2014). Récupéré sur http://www.orange-business.com/fr/blogs/securite/securite-des-communications-unifiees/webrtc-introduction-et-modele-de-securite

Wikipedia - Calculateur quantique. (2014). Récupéré sur http://fr.wikipedia.org/wiki/Calculateur_quantique

Wikipedia - Empoisonnement du cache DNS. (2014). Récupéré sur http://fr.wikipedia.org/wiki/Empoisonnement_du_cache_DNS

Wikipedia - Internet Exchange Point. (2014). Récupéré sur http://fr.wikipedia.org/wiki/Internet_Exchange_Point

Wikipedia - Post-quantum cryptography. (2014). Récupéré sur http://en.wikipedia.org/wiki/Post-quantum_cryptography

Wikipedia - Quantum key distribution. (2014). Récupéré sur http://en.wikipedia.org/wiki/Quantum_key_distribution

Wikipedia - Splinternet. (2014). Récupéré sur http://en.wikipedia.org/wiki/Splinternet

Wikipedia - WS-Trust. (2014). Récupéré sur http://en.wikipedia.org/wiki/WS-Trust

Wikipedia : Denial-of-service attack. (2014). Récupéré sur http://en.wikipedia.org/wiki/Denial-of-service_attack#Handling

XeNA: an access negotiation framework using XACML. (2014). Récupéré sur https://hal.archives-ouvertes.fr/hal-00448945

B. Annexe - Glossaire

Abréviation	Signification
AAA	Authentication, Authorization, Accounting
AC	Autorité de Certification
ANR	Agence Nationale de la Recherche
ANSSI	Agence Nationale pour la Sécurité des Systèmes d'Information
API	Application Programming Interface
APT	Advanced Persistent Threats
ARCEP	Autorité de Régulation des Communications Electroniques et des Postes
AS	Autonomous System
ASIP	Agence des Systèmes d'Information Partagés de santé
ATM	Asynchronous Transfer Mode
AVT	Advanced Volatile Threats
BOTNET	roBOT NETwork
BYOD	Bring Your Own Device
CDN	Content Delivery Network
CIM	Common Information Model
CNIE	Carte Nationale d'Identité Electronique
CSA	Conseil Supérieur de l'Audiovisuel
CSIRT	Computer Security Incident Response Team
CSIS	Center for Strategic and International Studies
DANE	DNS-based Authentication of Named Entities
DDoS	Distributed Denial-Of-Service
DLP	Data Loss Prevention
DMZ	DeMilitarized Zone
DNSSEC	Domain Name System Security Extensions
DoS	Denial-Of-Service
DPI	Deep Packet Inspection
ECC	ECC : Elliptic Curve Cryptography
EPS	Etude Prospective & Stratégique
ETSI	European Telecommunications Standards Institute
FAI	Fournisseur d'Accès Internet

FTTH	Fiber To The Home
GAFA	Google, Apple, Facebook, Amazon
GSMA	GSM Association
HLR	Home Location Register
IaaS	Infrastructure as a Service
ICN	Information-Centric Networking
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IHM	Interface Homme-Machine
IIC	Industrial Internet Consortium
IMS	IP Multimedia Subsystem
iOCTA	Internet Organised Crime Threat Assessment
IoT	Internet of Things (= Internet des Objets)
IPS	Intrusion Prevention System
ISG	Industry Specification Group (ETSI)
ISP	Internet Service Provider (= FAI)
ITU	Union Internationale des Télécommunications
IXP	Internet Exchange Point
LTE	Long Term Evolution
M2M	« Machine to Machine »
MITM	Man In The Middle
MOOC	Massive Open Online Course
MTD	Moving Target Defence
NaaS	Network as a Service (NaaS)
NFC	Near Field Communication
NFV	Network Function Virtualisation
ODM	Original Design Manufacturers
OIV	Opérateurs d'Importance Vitale
ONF	Open Networking Foundation
OTA	Over The Air
OTT	Over-The-Top
P2P	Peer-to-Peer
PIN	Personal Identification Number
PKIX	Public-Key Infrastructure X.509

POP	Point Of Presence
PPP	Partenariat Public Privé
PUF	Physical Unclonable Function
RADIUS	Remote Authentication Dial-In User Service
RBA	Risk Based Authentication
RGS	Référentiel Général de Sécurité
RIPE NCC	Réseaux IP Européens Network Coordination Centre
RIR	Registre Internet Régional
ROA	Route Origination Authorization
RPKI	Resource Public Key Infrastructure
SaaS	Software as a Service
SCADA	Supervisory Control and Data Acquisition (système de contrôle industriel)
SDDC	Software Defined Data Center
SDF	Sûreté De Fonctionnement
SDN	Software Defined Networking
SII	Système Industriel Interconnecté
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SOC	Security Operating Center
SSL	Secure Sockets Layers
TDM	Time Division Multiplexing
TIC	Technologies de l'Information et de la Communication
TLD	Top Level Domain (DNS)
TLS	Transport Layer Security
TOR	The Onion Router
TPM	Trusted Platform Module
UE	Union Européenne
V2I	Véhicule To Infrastructure
V2V	Véhicule To Véhicule
VoLTE	Voice Over LTE
ZTNA	Zero Trust Network Architecture

C. Annexe - confidentiel Orange

Cette annexe est classée « confidentiel Orange ».

D. Annexe - Contributeurs de l'étude

Cette annexe n'est pas diffusable publiquement.