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.