GNOS IE

Les géants du Web et la cybercriminalité

Auteur :

Camille STUDER

Sous la direction de :

Christian HARBULOT

Ce document d'analyse, d'opinion, d'étude et/ou de recherche a été réalisé par un (ou des) membre(s) de l'Association de l'Ecole de Guerre Economique. Préalablement à leurs publications et/ou diffusions, elles ont été soumises au Conseil scientifique de l'Association. L'analyse, l'opinion et/ou la recherche reposent sur l'utilisation de sources éthiquement fiables mais l'exhaustivité et l'exactitude ne peuvent être garantie. Sauf mention contraire, les projections ou autres informations ne sont valables qu'à la date de la publication du document, et sont dès lors sujettes à évolution ou amendement dans le temps.
Le contenu de ces documents et/ou études n'a, en aucune manière, vocation à indiquer ou garantir des évolutions futures. Le contenu de cet article n'engage la responsabilité que de ses auteurs, il ne reflète pas nécessairement les opinions du (des) employeur(s), la politique ou l'opinion d'un organisme quelconque, y compris celui de gouvernements, d'administrations ou de ministères pouvant êtres concernés pas ces informations. Et, les erreurs éventuelles relèvent de l'entière responsabilité des seuls auteurs.
Les droits patrimoniaux de ce document et/ou étude appartiennent à l'Association, voire un organisme auquel les sources auraient pu être empruntées. Toute utilisation, diffusion, citation ou reproduction, en totalité ou en partie, de ce document et/ou étude ne peut se faire sans la permission expresse du(es) rédacteur(s) et du propriétaire des droits patrimoniaux.

EXECUTIVE SUMMARY

Les géants du Web se positionnent aujourd'hui comme les fervents défenseurs d'un monde numérique plus sûr, et mettent au cœur de leur priorité une lutte acharnée contre la cybercriminalité. Cependant, le tsunami causé par Edward Snowden et les révélations du programme PRISM ont mis à mal la réputation des mastodontes du Net. Google, Facebook, Apple, Microsoft, autant de sociétés qui ont été montrées du doigt par les internautes, qui se sont sentis trahis, perdant toute confiance envers ceux qui s'autoproclamaient gardiens d'un Internet respectueux des données et de la vie privée des utilisateurs.

De plus, si la lutte contre la cybercriminalité est une cause noble, elle n'en reste pas moins un segment très rentable pour l'économie dont les géants du Web ne se privent pas, puisqu'ils restent avant tout des compétiteurs dont le profit est le leitmotiv.

Ce leitmotiv pousse ces firmes américaines à conquérir de nouveaux marchés, afin de fuir la saturation des réseaux en Occident. Mais les pays émergents accusent un retard conséquent dans l'intégration des nouvelles technologies à leur société. Les géants du Web n'ont alors qu'un pas à faire pour s'engouffrer dans la brèche de la fracture numérique, et se posent alors comme les sauveurs de ses sociétés où beaucoup reste à faire en matière de numérique. Tout cela au risque de déployer un peu plus le cyberespace et ainsi d'offrir un terrain de jeu encore plus attrayant pour les cybercriminels.

TABLE DES MATIERES

INTRODUCTION

"Breaking : Two Explosions in the White House and Barack Obama is injured", ce tweet du 23 avril 2013 émanant du compte Twitter de l'agence américaine Associated Press et retweeté plusieurs centaines de fois, a créé la panique et fait plonger le Dow Jones de plus de 130 points en très peu de temps. Peut-être était-ce l'effet escompté par les hackers qui se sont emparés du compte de l'Associated Press ? Ou bien souhaitaient-ils uniquement se griser en brisant toutes les barrières de sécurité mise en place par le réseau social ? Dans tous les cas, l'effet produit a été fort dommageable et démontre bien que, aussi puissants soient-ils, les acteurs, et plus particulièrement les géants du Web, restent vulnérables face à une cybercriminalité omniprésente et toujours plus puissante.

Selon la définition officielle du Ministère de l'Intérieur, la cybercriminalité est *« le terme employé pour désigner l'ensemble des infractions pénales qui sont commises via les réseaux sociaux informatiques, notamment, sur le réseau Internet. Ce terme désigne à la fois :*

- *Les atteintes aux biens, fraude à la carte bleue sur Internet sans le consentement de son titulaire ; vente par petites annonces ou aux enchères d'objets volés ou contrefaits ; encaissement d'un paiement sans livraison de la marchandise ; piratage d'ordinateur ; gravure pour soi ou pour autrui de musiques, films ou logiciels*
- *Les atteintes aux personnes : diffusion d'images pédophiles ; diffusion auprès d'enfants de photographies à caractère pornographique ou violent ; atteinte à la vie privée. »*[1]

Cette définition peut être complétée par celle de Solange Ghernaouti, Professeur à l'Université de Lausanne, membre de l'Académie Suisse des Sciences Techniques et Directrice du Swiss Cybersecurity & Research Group. Selon elle, la cybercriminalité est

[1] Site officiel du Ministère de l'Intérieur, http://www.interieur.gouv.fr/A-votre-service/Ma-securite/Conseils-pratiques/Sur-internet/Qu-est-ce-que-la-cybercriminalite, consulté le 29 mai 2014 à 07h57

aujourd'hui indissociable des techniques de *Social Engineering*, soit les dangers liés *« à la fuite ou au vol d'informations favorisés notamment par des techniques d'intelligence et d'ingénierie sociale »* ; ou encore l'ensemble des techniques visant à exploiter des informations collectées sur les internautes, notamment par le biais des réseaux sociaux, afin de les tromper ou de les inciter à réaliser des actions qui permettent ensuite l'intrusion dans des systèmes informatiques, ou la diffusion de programmes malveillants entre autres.

Solange Ghernaouti rappelle également que la cybercriminalité peut aussi se traduire par l'ensemble des *« actions de manipulation d'informations, de propagation de rumeurs, pour nuire à une personne, déstabiliser l'économie, une entreprise, un pays »*.[2]

En juillet 2013, le *Center For Strategic and International Studies*[3] a publié la première étude sur l'impact économique de la cybercriminalité à travers le monde. Selon l'étude, le coût total de la cybercriminalité serait de 500 milliards de dollars par an ; et les Etats-Unis, enregistreraient à eux seuls, une perte nette de 100 milliards de dollars par an et 508 000 suppressions d'emplois.

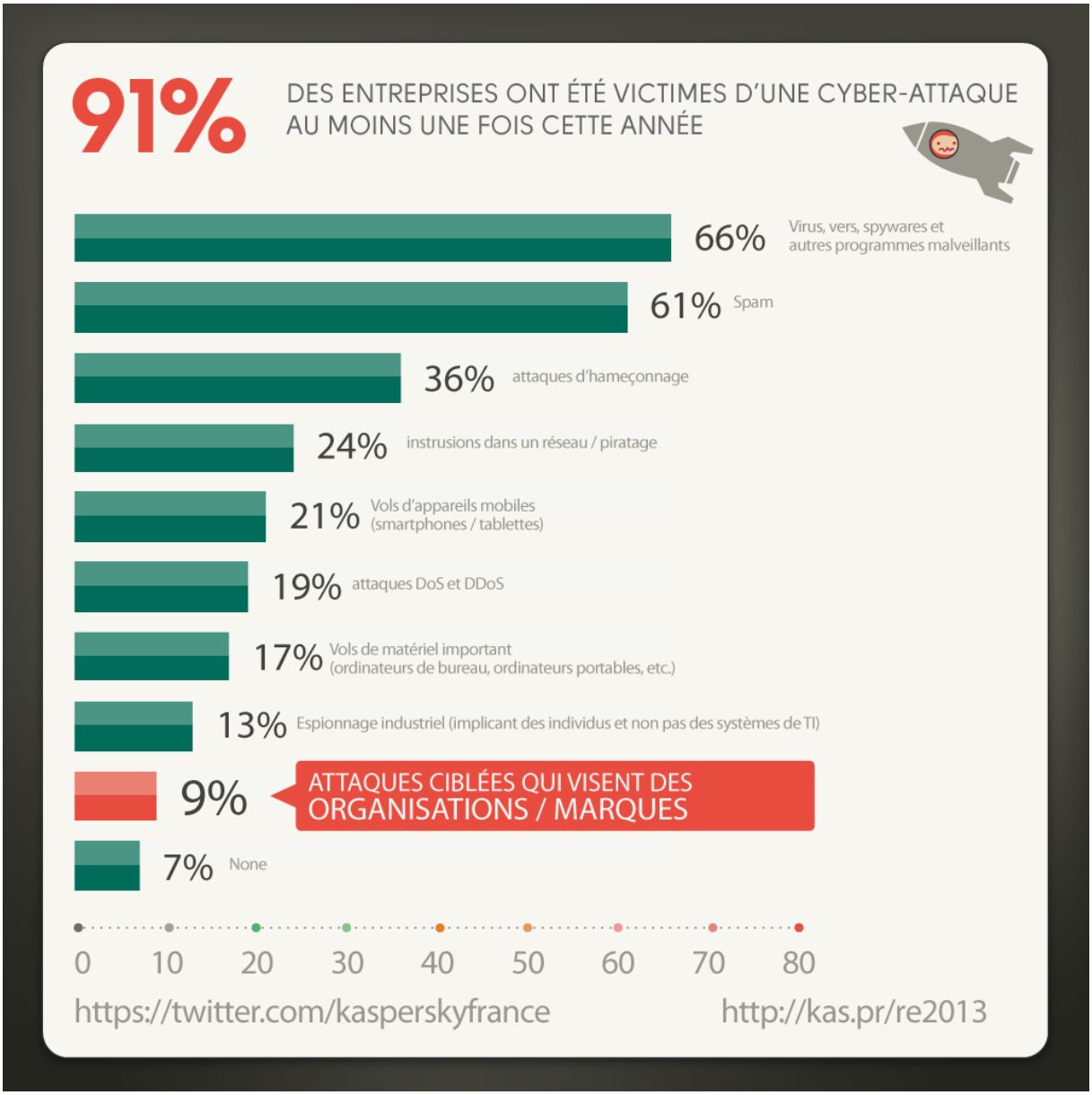
Selon le bulletin de sécurité 2013 du Kaspersky Lab[4], 91 % des entreprises ont été victimes d'au moins une cyber-attaque sur l'année, 9 % de ces attaques étant des attaques dites ciblées, visant une marque ou une organisation spécifique. Le marché de la téléphonie mobile n'est pas en reste, puisque, pour l'année 2013 uniquement, 104 421 logiciels malveillants, ou *malwares*, pour mobiles ont été recensés (98 % d'entre eux étant compatibles avec Android).

Par ailleurs, le Kaspersky Lab a détecté 5 milliards de cyber-attaques, et une moyenne de 315 000 nouveaux *malwares* chaque jour. Enfin, les pays les plus touchés par les cyber-attaques sont, en 2013, les Etats-Unis et la Russie, ces deux pays hébergeant respectivement 25,5 % et 19,4 % des serveurs *malwares*.

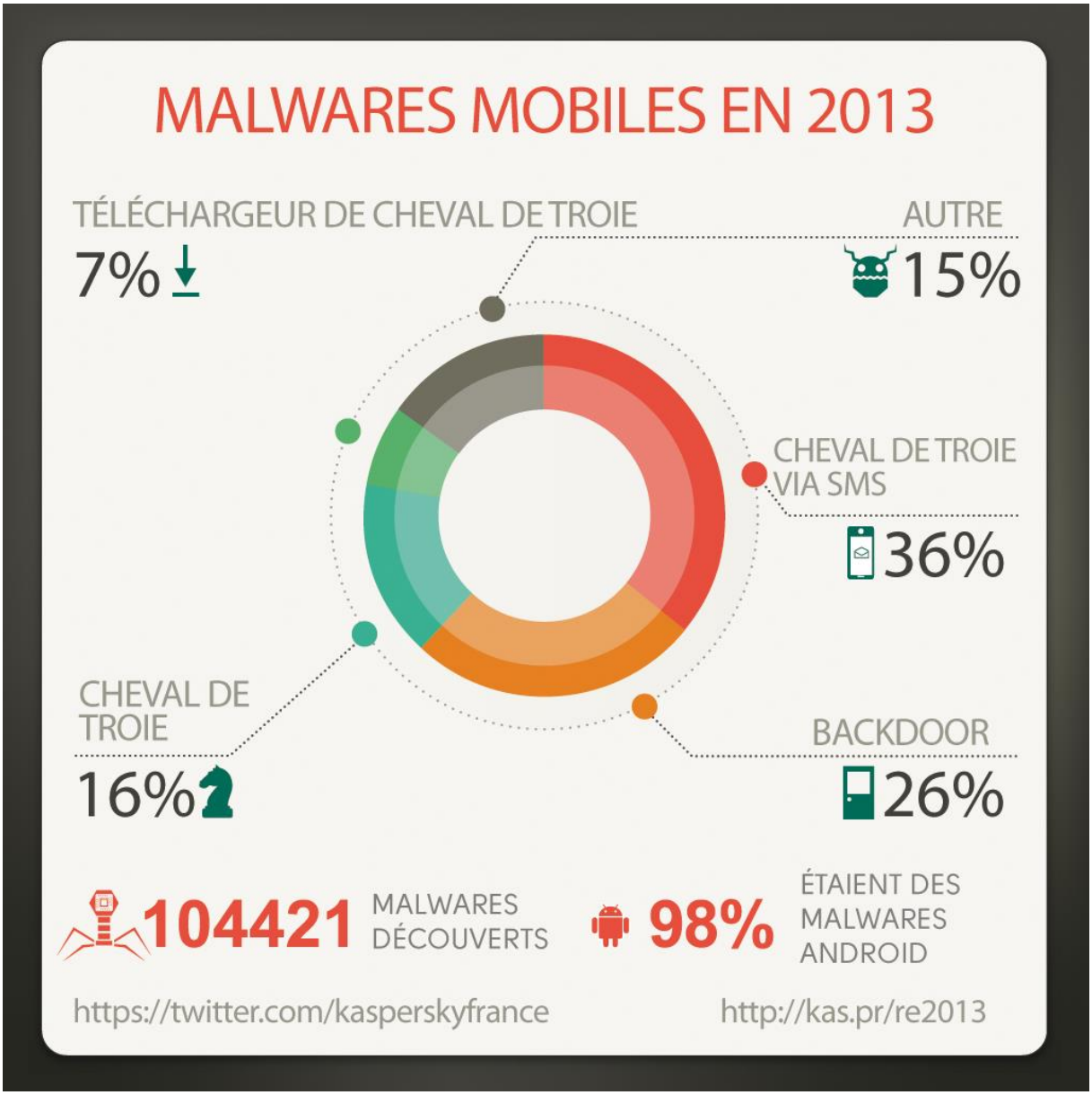
[2] « Cyber-guerre : la Suisse n'est pas prête ! », entretien avec Solange Ghernaouti, Les Observateurs, 01 mars 2013

[3] "The Economic Impact of Cybercrime and Cyber Espionage", Center for Strategic and International Studies, Juillet 2013

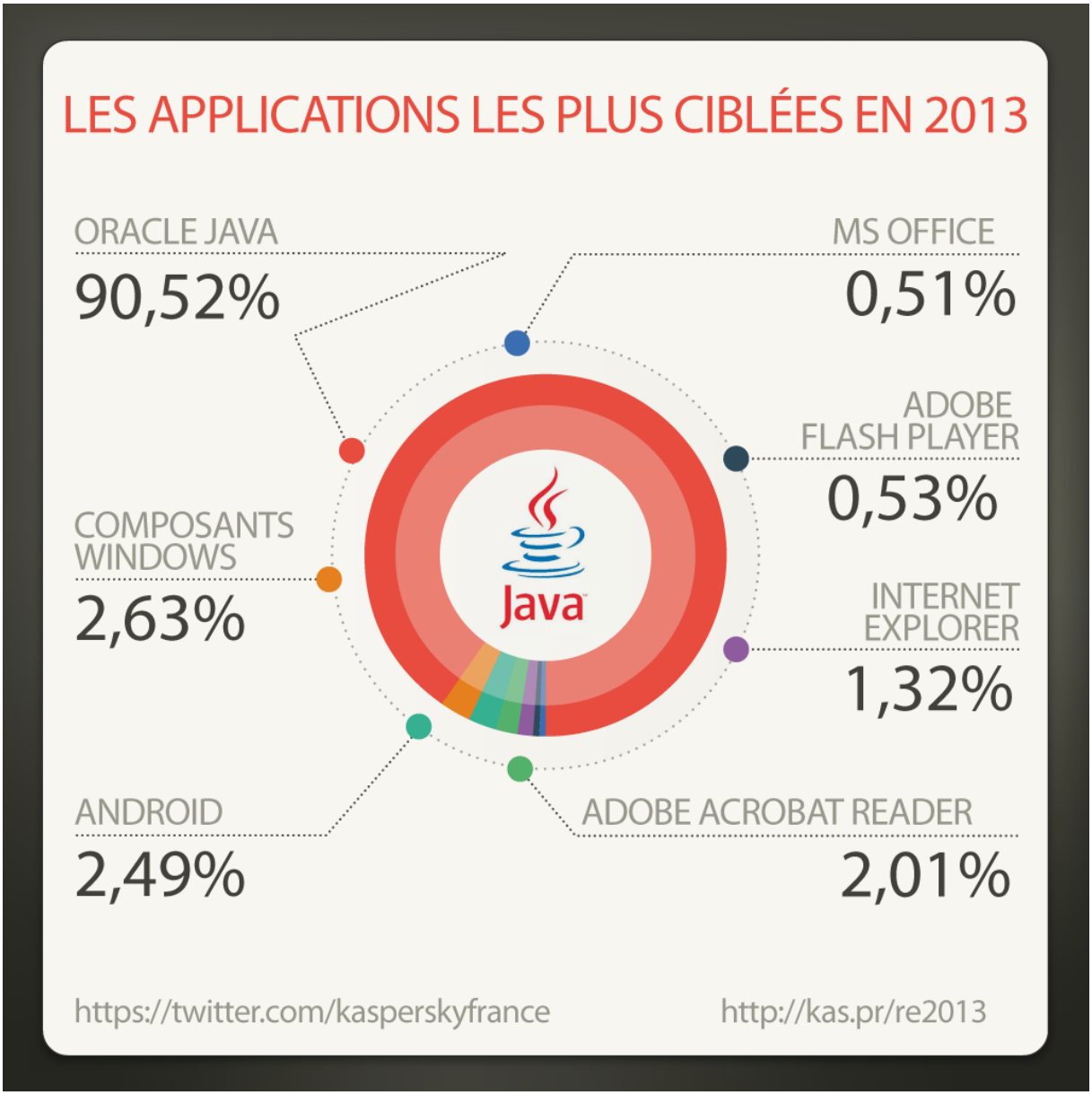
[4] « Kaspersky Security Network », Kasperky Lab, décembre 2013



Les principales menaces cybercriminelles de 2013, Kaspersky Lab



Les principales menaces cybercriminelles de 2013, Kaspersky Lab



Les principales menaces cybercriminelles de 2013, Kaspersky Lab

Ainsi, la cybercriminalité occupe sans conteste la sphère numérique. Qu'en est-il donc des Microsoft, Google, Facebook et autres Twitter ? En effet, si ces géants du Web ont la mainmise sur ce secteur, comment gèrent-ils la montée incessante du cybercrime ? Sont-ils contributeurs malgré eux ou simples victimes ? Surfent-ils sur la vague du marché de la cybersécurité pour accroître leur compétitivité, ou sont-ils, au contraire, amenés à unir leurs savoir-faire ? Nous tenterons ici de présenter une ébauche de réponse à ces interrogations.

I. PARADOXES, DIFFICULTES ET ETATS D'AMES, LES LIAISONS DANGEREUSES DES GEANTS DU WEB ET DE LA CYBERCRIMINALITE

Nous tenterons ici d'exposer la complexité, pour les géants du Web, d'avoir le « bon rôle », à l'heure où le monde numérique est chaque jour un peu plus vulnérable. En effet, si les grands groupes du numérique ont toujours clamé haut et fort être du côté des internautes, l'affaire Snowden a légèrement ébranlé ce postulat. Par ailleurs, la grande famille des géants du Web est avant tout une famille de compétiteurs, dont le profit est le principal leitmotiv.

A. PRISM, OU COMMENT LES GEANTS DU WEB ONT PERDU UNE CERTAINE CREDIBILITE

Si les géants du Web se sont toujours positionnés en fervents défenseurs des droits et libertés des internautes, la récente affaire Snowden a quelque peu ébranlé la crédibilité d'Apple, Microsoft et Google notamment. En effet, suite aux révélations d'Edward Snowden concernant le programme de surveillance américain PRISM, les géants du Web ont été pointés du doigt par les usagers d'Internet, suite à leur rôle d'intermédiaire dans la transmission de données au Gouvernement américain.

A ce titre, la société Microsoft a permis à la NSA d'intercepter les emails cryptés ainsi que les *chats* des utilisateurs des messageries Outlook et Hotmail, contournant ainsi son propre système de sécurité justement mis en place pour empêcher la récupération de données par des pirates. De plus, la NSA a pu surveiller les appels passés depuis Skype, propriété de Microsoft.

Il en a été de même pour Google, Facebook, Apple, Yahoo ! et d'autres grandes firmes, qui ont dû, tour à tour, répondre aux allégations d'Edward Snowden, preuves à l'appui.

Les internautes se sont donc légitimement posé la question de la fiabilité de ces mastodontes du Net. *Quid* de leur transparence ? *Quid* de leur rôle réel dans la récupération de données personnelles ? Si Google et Microsoft ont tenté de se racheter une image en lançant une procédure devant la justice fédérale américaine afin de réclamer le droit de communiquer davantage auprès des internautes sur les règles de collaboration avec les services secrets et le Gouvernement[5], leur fiabilité était d'ores et déjà légèrement entachée.

De plus, le fait que Google ait reçu, en une seule journée, 12 000 demandes d'utilisateurs qui ont souhaité être effacés des résultats de recherche[6], témoigne bien du manque de confiance des internautes, conscients que leur vie privée et leurs données personnelles peuvent à tout moment être récupérées sans leur consentement et pour un usage qu'ils n'ont pas choisi au préalable.

Le fait est que PRISM a suscité une certaine insécurité chez les internautes. Ainsi, ceux qui affirmaient haut et fort être de fervents défenseurs de la protection, de la sécurisation des données personnelles, mettant au point des systèmes sécurisés toujours plus performants pour lutter contre le cybercrime, se sont retrouvés de l'autre côté de la barrière. Non pas que Microsoft et consorts soient devenus eux-mêmes des cybercriminels, mais il est légitime de s'interroger sur leur double rôle. D'un côté protecteurs des internautes, garantissant une

[5] Les entreprises américaines doivent, dans le cadre du Foreign Intelligence Surveillance Act de 1978, et amendé depuis à plusieurs reprises, notamment en 2001 par le USA Patriot Act, « unir et renforcer l'Amérique en fournissant les outils appropriés pour déceler et contrer le terrorisme ». Cela comporte notamment la transmission des données des internautes, l'accès à des bases cryptées…etc.

[6] Google a du se conformer à la décision de la Cour de Justice Européenne visant à permettre aux internautes européens de bénéficier d'un « droit à l'oubli ». En ce sens, les particuliers ont désormais le droit de faire supprimer des résultats de recherche les liens vers des pages comportant des informations personnelles les concernant, notamment si elles sont périmées ou inexactes.

navigation sur le Web sécurisée et à l'abri des regards ; d'un autre côté, « complices » du Gouvernement et des services de renseignement, prêts à livrer des données sans état d'âme.

Là réside donc toute la difficulté des géants du Web. Comment être à la fois du côté des internautes sans enfreindre les règles de l'Etat dans lequel ils se trouvent, et inversement, comment obéir aux doléances des Gouvernements sans trahir les engagements de confidentialité pris auprès des consommateurs.

Les révélations d'Edward Snowden ont mis en lumière la problématique de l'encadrement d'Internet et des règles nationales et internationales qui sont particulièrement complexes à mettre en œuvre. Les géants du Web se retrouvent donc au cœur de ce capharnaüm, oscillant tour à tour entre la défense et le respect des internautes et la soumission aux Gouvernements et autres services de renseignement. Ne nourrissent-ils pas là, malgré eux, une partie de la cybercriminalité en cassant leur système de sécurité au nom de la lutte contre le terrorisme par exemple ?

Si le « gang » des GAFA[7] est donc aujourd'hui dans une position délicate et à la reconquête de sa crédibilité auprès des internautes, cela n'empêche pas ces acteurs majeurs du numérique de poursuivre, inlassablement et malgré tout, leur lutte contre la cybercriminalité.

[7] Nom d'usage dans le milieu du Web pour regrouper les principaux acteurs de la toile : Google, Apple, Facebook, Amazon

B. LES *MODUS OPERANDI* DES GEANTS DU WEB POUR S'APPROPRIER LE MARCHE DE LA CYBERCRIMINALITE

Il ne se passe pas un jour sans qu'un système de sécurité soit cassé, sans qu'un ordinateur ait été piraté, sans que des données aient été interceptées. Les géants du Web doivent être en éveil permanent, afin de réagir au plus vite et, de préférence, avant la concurrence.

En effet, si la cybercriminalité représente la nouvelle criminalité organisée, celle du XXIème siècle, il n'empêche que le marché de la cybercriminalité reste un marché comme les autres, au sein duquel chacun tente de se positionner comme leader de la lutte contre le cybercrime.

Chacun y va donc de son initiative, proposant tour à tour des mesures, structures ou partenariats toujours plus performants.

Nous nous intéresserons ici à deux incontournables du Web, qui semblent occuper toute la place sur le terrain de la cybercriminalité : Microsoft et Google.

L'ultra communication de Microsoft

Contrairement à Google, la firme de Redmond, Microsoft, n'est pas avare en communication concernant ses diverses actions œuvrant pour la lutte contre la cybercriminalité.

Le 15 novembre 2013, la firme lançait son *Microsoft Cybercrime Center* aux Etats-Unis, souhaitant ainsi *« faire avancer le combat mondial contre la cybercriminalité »*. Ce centre s'est doté de 1 600m² de laboratoires de recherche et d'investigations et regroupe deux entités clés : la *Digital Crime Unit* (DCU) qui s'occupe d'intercepter les attaques type *malwares* ; et l'*Intellectual Property Crime Unit* (IPCU), qui traite plus particulièrement des problématiques relatives à la propriété intellectuelle.

Le *Microsoft Crime Unit*, qui comprend actuellement 100 experts dédiés, a pour but d'élaborer et de fournir des outils permettant de détecter les cybercriminels et la manière dont ils procèdent. Parmi les outils d'ores et déjà utilisés par le centre, on retrouve notamment « SitePrint » et « PhotoDNA ». Le premier vise à détecter et collecter les points communs entre les différents sites malveillants, qui pourraient, au premier abord, apparaître non liés les uns aux autres. Il permet ensuite d'identifier les pirates qui sont derrière ces sites et de comprendre et d'appréhender leur mode opératoire. Le second outil permet de tracer les signatures des photos qui sont envoyées, échangées par les internautes, à partir de codes d'identifications spécifiques. Cela permet de lutter contre la circulation d'images pédopornographiques notamment.

David Finn, responsable monde de la cybersécurité a assuré qu'en *« combinant des outils et technologies sophistiqués avec les bonnes personnes et de nouvelles perspectives, on peut rendre Internet plus sûr »*.

Microsoft n'en est pas à son coup d'essai, en 2011 déjà, le géant du Web avait lancé l'association Phishing Initiative, créée en partenariat avec LEXSI et PayPal afin de permettre la détection de sites de phishing[8] présumés et ainsi de les bloquer avant qu'ils ne puissent faire des victimes.

Si cette initiative n'a été expérimentée que sur le marché francophone au jour d'aujourd'hui, elle a permis, en près de trois ans, de collecter 150 000 adresses de sites signalées par 30 000 internautes différents. 68 000 des 150 000 adresses ont été confirmées comme étant des sites de phishing.

Enfin, dès 2009, Microsoft a soumis à la Commission européenne, avec de nombreux autres partenaires tels que des universités américaines entre autres, le projet baptisé

[8] Le terme phishing, ou hameçonnage, désigne une technique utilisée par des pirates pour récupérer les données personnelles des internautes. Ils prennent souvent une fausse identité, telle qu'un organisme bancaire, Amazon ou encore eBay, qui est connue du consommateur et en qui il a toute confiance. Le meilleur moyen de réaliser des actes de phishing est en réalisant de faux sites webs ou en envoyant des mails frauduleux. Les pirates comptent alors sur la naïveté des internautes pour pouvoir opérer.

« 2CENTRE »[9], visant à unir les compétences et savoir-faire de nombreux industriels, autorités publiques et d'autres acteurs majeurs dans le but d'élaborer et de créer des centres d'excellence de formation et de recherche dans le domaine de la cybercriminalité, afin de former, notamment, les experts de demain aux techniques d'investigation sur le cybercrime.

Deux centres d'excellence ont déjà vu le jour, l'un à Dublin et dirigé par l'*University College of Dublin*, l'autre à Troyes et piloté notamment par l'Université de technologies de Troyes, l'Université de Montpellier I et la Gendarmerie nationale.

Selon Microsoft, *« l'innovation technologique, les conseils aux utilisateurs et des partenariats sont essentiels pour s'attaquer à la complexité sans cesse croissante du cybercrime »*.

La discrétion de Google

La firme de la Silicon Valley, quant à elle, se caractérise par son peu de communication auprès du grand public concernant sa politique de lutte contre la cybercriminalité. En effet, Google privilégie des communications ponctuelles destinées à des utilisateurs précis, ou informe sa communauté via son blog dédié, le *Google Online Security Blog*.[10] S'il communique peu, le moteur de recherche numéro un mondial n'en agit pas moins pour autant.

Google, est, à l'instar de Microsoft, vivement impliqué dans la lutte contre la pédopornographie. A ce titre, il a mis en place un outil permettant de déceler les *« Child porns »*, par des algorithmes permettant d'identifier des images et des mots clés. Cet outil permet, en décelant des contenus à caractère pornographique, de mieux lutter contre la pédopornographie.

[9] « 2CENTRE »: Cybercrime Centres of Excellence Network for Training, Research and Education.
[10] Pour aller plus loin : http://googleonlinesecurity.blogspot.fr/

Toujours dans le cadre de la lutte contre la pédopornographie, Google a financé, à plusieurs reprises, des programmes de recherche de l'*Internet Watch Foundation* (IWF), dont le but est de signaler, intercepter, empêcher tout contenu à caractère pédopornographique de circuler sur la toile.

Enfin, si des internautes venaient à taper *« Child porn »* ou d'autres mots clés de ce type comme requête, Google prévoit d'afficher automatiquement un message indiquant que cette requête est interdite. Selon la firme, cette méthode dissuasive est efficiente mais le problème réside dans la faculté de détecter de nouveaux mots clés potentiellement utilisés par des internautes malveillants. Par ailleurs, au niveau européen, Google forme régulièrement des enquêteurs aux outils, et ce, en partenariat avec Microsoft. Pour Benoit Tabaka, Directeur des Relations institutionnelles de Google France, il est *« plus important dans ce cas-là d'être partenaire »*.

Depuis l'affaire PRISM, Google dit avoir renforcé le chiffrement entre ses différents *Data Centres*, y compris les câbles sous-marins, ainsi que le chiffrement de l'usage des outils Google. A ce titre, les usagers ne peuvent plus désactiver l'option de chiffrement sur la messagerie Gmail. Par ailleurs, ce renforcement du chiffrement permet également à Google de masquer les requêtes formulées par les internautes dans certains pays asiatiques, afin que les Gouvernements ne puissent pas y accéder.

Microsoft et Google luttent donc tous deux contre la cybercriminalité, mais ils luttent également pour occuper une place de choix au sein du marché de lutte contre le cybercrime, chacun à sa façon. Le premier est plus disposé à s'afficher de façon presque permanente auprès du grand public, se voulant rassurant et saisissant à bras-le-corps la problématique. Le second, beaucoup plus discret sur la scène médiatique, préfère privilégier ses communications, mieux cibler ses actions et miser sur les interactions avec la communauté Google plutôt qu'avec l'ensemble du grand public.

Chacun des deux mastodontes du Web a un *modus operandi* bien précis, et, s'il s'avère qu'ils sont amenés à travailler main dans la main dans certains cas, ils n'en restent pas moins des concurrents de taille sur un marché comme un autre.

La cybercriminalité reste avant tout un secteur qui, hélas, a le vent en poupe et qui est amené à se développer encore et encore, au grand dam des internautes. Pas si évident qu'il en soit de même pour les géants du Web. En effet, le politiquement correct voudrait qu'on ne retienne que le combat de ces firmes pour anéantir le cybercrime et protéger ses réseaux et ses utilisateurs. Cependant, la vague de cybercriminalité qui envahit notre quotidien ultra-connecté est également une source de *business* pour ces mêmes entreprises.

Tour à tour partisans d'un Internet vierge de toute cybercriminalité ou compétiteurs aguerris, les géants du Web se retrouvent donc dans une position paradoxale et délicate, complexe à justifier mais également difficilement critiquable.

L'écosystème numérique, s'il représente le terrain de jeu des cybercriminels, semble être toujours plus enclin à conquérir de nouveaux marchés, quitte à étendre un peu plus la cybercriminalité à travers le monde.

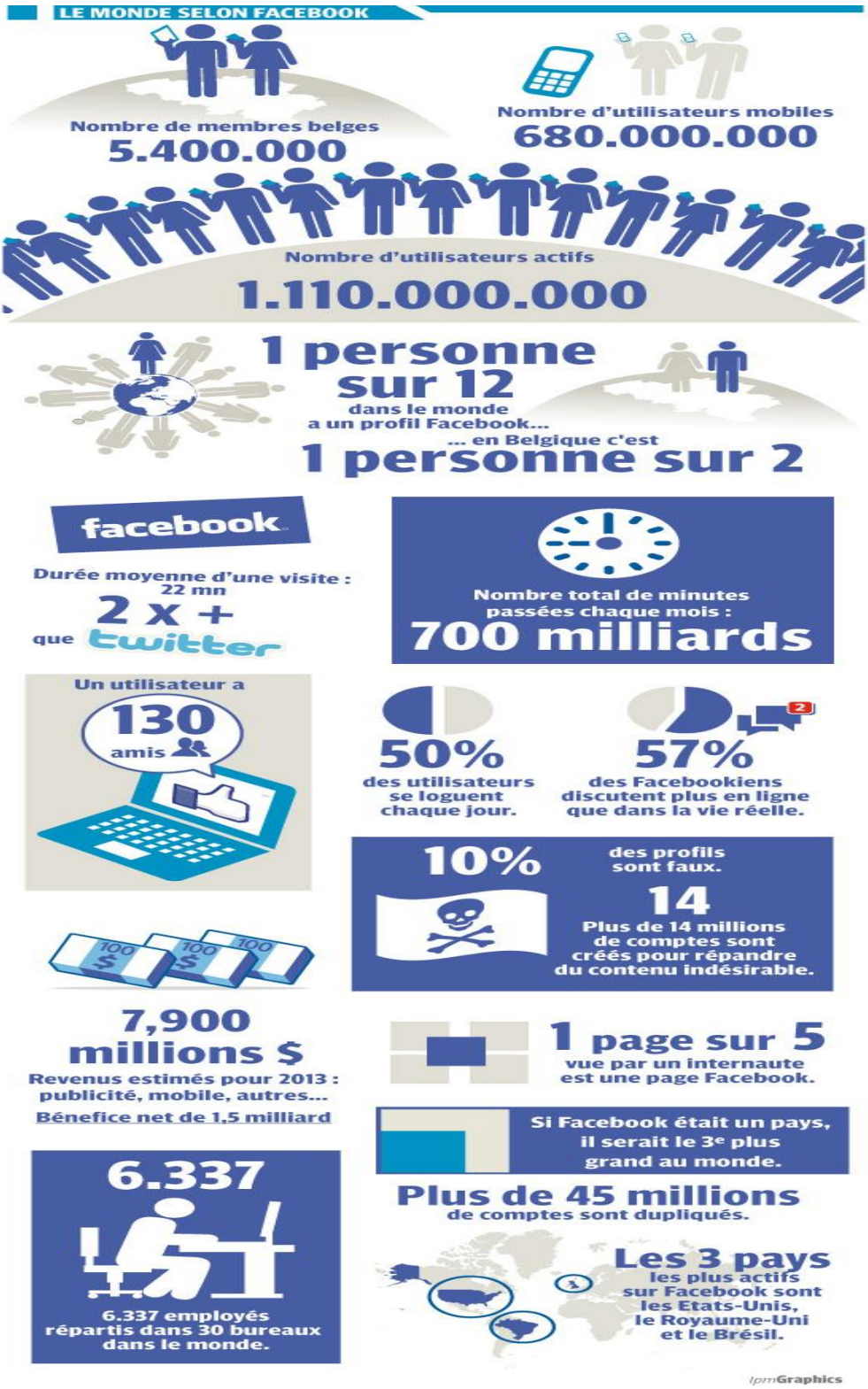
II. LES GEANTS DU WEB ET LES PAYS EMERGENTS, EXEMPLE DE L'AFRIQUE

Les pays émergents sont, de fait, confrontés au retard qu'ils ont pris, vis-à-vis des pays développés, dans l'intégration des nouvelles technologies de l'information et de la communication au sein de leur société. Cela entraîne indubitablement une fracture numérique conséquente.

Deux possibilités s'offrent alors aux géants du Web : combler les lacunes de certains pays en matière de numérique ou accompagner ceux qui ont pris le train en marche dans leur mutation.

A. FACEBOOK A LA CONQUETE DU MARCHE AFRICAIN

Nombre d'utilisateurs actifs de Facebook par mois, SocialBand, 2012



Malgré un succès planétaire indéniable et des chiffres qui parlent d'eux-mêmes, Facebook ne semble pas se satisfaire de son aura numérique et envisage des projets toujours plus démesurés pour conquérir de nouveaux marchés.

« Il y a de gros freins dans les pays en voie de développement pour se connecter et rejoindre l'économie du savoir […] Il nous faut prouver aux personnes qui n'ont pas beaucoup d'argent, dans les pays émergents, qu'il est rationnel pour elles d'en dépenser une partie dans la téléphonie mobile […]. De la même manière que nous avons aux Etats-Unis le numéro 911 permettant de passer gratuitement des appels d'urgence, nous voulons créer un système similaire sur Internet, avec des applications gratuites »[11]. Ces propos, signés Mark Zuckerberg, illustrent la volonté du fondateur de Facebook de remédier à la fracture numérique mondiale, qui empêche actuellement presque cinq milliards de personnes de bénéficier d'un accès à Internet, et donc d'un accès à Facebook. C'est donc tout naturellement que la firme a annoncé, lors de l'édition 2014 du *Mobile World Congress*, son projet d' « Internet pour tous ». Plus précisément, le projet vise à fédérer des leaders du monde des nouvelles technologies, des associations et des experts au niveau mondial, dans le but de collaborer et de mettre au point une offre d'accès à Internet pour les deux tiers de la population qui n'en bénéficie pas encore.[12]Ainsi, la volonté de Mark Zuckerberg, qui a d'ores et déjà réussi à rallier à sa cause Samsung, Ericsson, MediaTek, Opera, Qualcomm et Nokia, est *« chacun de nous. N'importe où. Connectés »*.

Si certains défendront bec et ongles ce projet et n'y verront là rien d'autre que du pur altruisme de la part de Facebook, il convient tout de même de noter que, en filigrane, il serait particulièrement opportun pour le réseau social de bénéficier des retombées d'un Internet accessible à tous. Cela n'a d'ailleurs pas échappé à Bill Gates, fondateur de Microsoft, qui a réagi au projet fou de Facebook en rappelant que *« si nous voulons améliorer la vie sur terre,*

[11] Déclaration de Mark Zuckerberg, lors du Mobile World Congress (MWC) de Barcelone, 2014
[12] Pour aller plus loin : www.internet.org

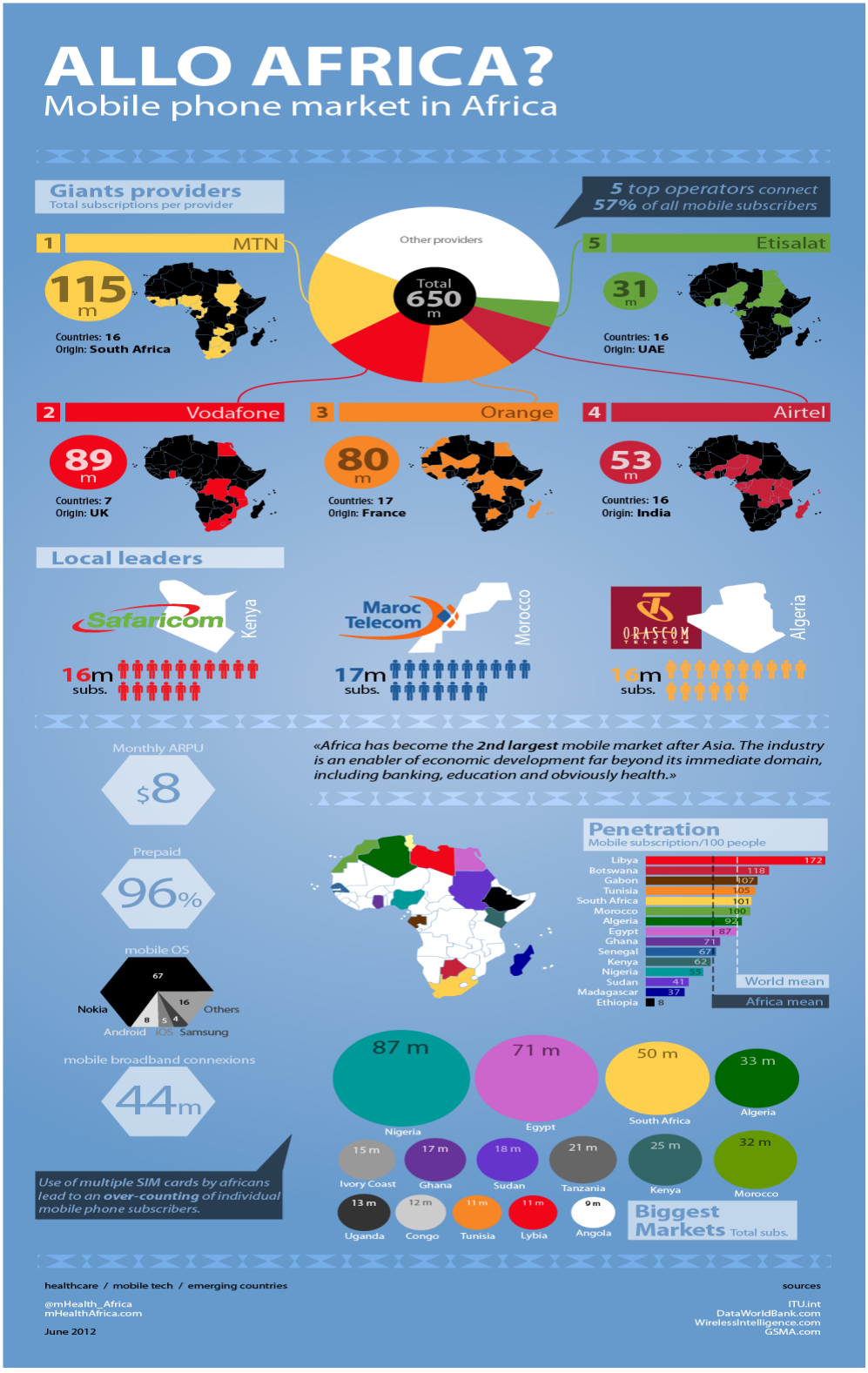
il y a des choses plus fondamentales à gérer, comme la survie et la nutrition des enfants […] Si vous pensez que la connectivité est l'élément clé c'est super. Mais moi non ».

En effet, outre sa volonté de rendre le monde meilleur, Facebook est en perte de vitesse. Le réseau social commence à s'essouffler et pourrait bientôt appartenir à la catégorie des géants du Web éphémères, s'il ne séduit pas au plus vite de nouveaux utilisateurs.

La multinationale vise donc certains pays émergents comme l'Afrique, afin d'y investir et d'y développer des solutions qui permettront d'optimiser, sur le long terme, les capacités d'exploitation d'Internet dans ces territoires.

L'Afrique est un excellent investissement puisqu'il présente un fort potentiel dans le domaine des nouvelles technologies. Le continent devrait compter 600 millions d'abonnés mobiles d'ici à 2016. En Afrique, le mobile est roi. Si les internautes ne représentent que 10 % de la population africaine, le taux de pénétration du marché du mobile est, lui, supérieur à 40 % et a augmenté de 100 % entre 2008 et 2012, soit la plus forte croissance mondiale. De plus, le montant total des investissements en téléphonie fixe et mobile devrait atteindre 145,8 milliards de dollars en 2015, contre 78,8 milliards en 2008.[13]

[13] Chiffres recueillis par le cabinet de conseil PricewaterhouseCoopers (PwC), dans le cadre de son étude sur le développement de la téléphonie mobile en Afrique, septembre 2012



Facebook a donc dû s'adapter aux habitudes des africains en attendant de pouvoir équiper tout le continent d'un accès direct à Internet. Ainsi, la firme de Mark Zuckerberg a transposé, tant bien que mal, son réseau social au « format SMS » et a développé des versions en langues locales comme le swahili, l'afrikaans ou encore l'arabe. Mais tous les efforts de Facebook ne sont pour l'instant pas suffisants car le réseau social ne compte actuellement « que » 54 millions de fidèles. Et le géant américain n'est pas au bout de ses peines car il n'est pas le seul acteur présent sur le continent. En effet, les africains sont friands, pour 50 millions d'entre eux, de Mxit, le concurrent africain de Facebook. Mxit est un concurrent de taille pour Facebook et se targue d'ailleurs d'être leader sur le marché en Afrique du Sud avec 10 millions d'utilisateurs, contre 5,5 millions pour son rival. Par ailleurs, Afrigator et Zoopy, respectivement agrégateur de contenus et plateforme de partages de vidéos, connaissent un succès significatif auprès des Africains, en Afrique du Sud notamment.

Le réseau social a donc tout intérêt à redoubler d'ingéniosité et d'initiatives s'il veut détourner le peuple africain des alternatives locales qui séduisent de plus en plus.

Alors, pour pallier à la saturation des réseaux en Occident et conquérir le monde et plus particulièrement l'Afrique, Facebook a su développer des outils au service de son projet d'un Internet mondial pour un monde hyper connecté. Ainsi, le géant américain a l'intention de « connecter » le continent africain à l'aide de 11 000 drones, appelés « atmosats », fonctionnant comme des satellites à basse altitude et capable de relayer le signal Internet.

A trop vouloir connecter le monde, les géants du Web ne participent-ils pas de la montée en puissance de la cybercriminalité ? En effet, plus le monde est connecté, plus il est vulnérable. Les pirates se renouvellent tous les jours en matière de cyber-attaques, et étendre le réseau Internet étend de façon simultanée leur terrain de jeu, leur champ d'action. Cela leur permet aussi de toucher plus de victimes, d'être malveillants à l'encontre d'internautes encore plus nombreux. De plus, la gouvernance mondiale du Net est une tâche ardue, un vrai casse-tête chinois pour les Autorités. Étendre un peu plus le cyberespace c'est donner du fil à

retordre aux différentes institutions et Gouvernements, qui tentent, tant bien que mal, d'encadrer le monde numérique.

Par ailleurs, Facebook n'est-il pas déjà suffisamment impliqué dans la perte de notion de vie privée et de données personnelles dans le monde merveilleux du numérique ? Si le fondateur du réseau social estime que l'hyper connectivité est *« bonne pour la planète »*, le géant américain a tout de même fortement contribué à la perte de certaines valeurs fondamentales comme le droit à la vie privée. Ainsi, la toile, et plus particulièrement Facebook, sont autant d'espaces où des entités plus ou moins bienveillantes peuvent venir piocher des informations, des données, et en tirer profit sans autorisation préalable.

B. LE CONTINENT AFRICAIN ET LES PREMICES DE LA LUTTE CONTRE LA CYBERCRIMINALITE

Si l'Afrique suscite de nombreuses convoitises de la part des géants du Web, le continent ne néglige en aucun cas les risques cybercriminels présents et à venir auxquels sa population est confrontée.

A ce titre, le Kenya a mis au point une stratégie de cybersécurité par le biais du Plan Directeur des Technologies de l'Information et de la Communication, lancée le 14 février dernier. Ce plan permettra notamment de mieux appréhender les mutations numériques et les risques que celles-ci comportent. Par ailleurs, le Gouvernement kenyan a élaboré un guide des bonnes pratiques destiné aux administrations et entreprises, afin de les sensibiliser à la problématique des risques inhérents à la cybercriminalité.

Au Rwanda, c'est presque 6 millions d'euros qui ont été attribués, pour la période 2013-2014, afin de lancer une vaste campagne de sensibilisation auprès de la population.

En 2013, la Côte d'Ivoire, quant à elle, organisait ses premières Assises de la sécurité informatique, réunissant toute la communauté du Web ivoirien. La Côte d'Ivoire se saisit de plus en plus de la lutte contre la cybercriminalité, car le pays fait face à une recrudescence de cyber-attaques. La Côte d'Ivoire est en passe de devenir le mauvais élève de l'Afrique de l'Ouest, avec des préjudices financiers dus à la cybercriminalité de plus de trois milliards de Francs CFA pour l'année 2012. La police ivoirienne qualifie même le Web comme « paradis numérique » pour les pirates souhaitant opérer en Afrique. A ce titre, la Côte d'Ivoire a également créé la Plateforme de lutte contre la cybercriminalité (PLCC), qui collabore notamment avec son homologue français – l'Office central de lutte contre la criminalité liées aux techniques de l'information et de la communication – pour la réalisation d'investigations approfondies entre autres.

Outre les nombreux attraits qu'elle présente pour les géants du Web qui souhaitent exploiter son potentiel et outre les nombreuses initiatives qu'elle lance pour être à même de répondre et de faire face à une cybercriminalité croissante, il convient de rappeler que l'Afrique reste un pays où la liberté sur Internet reste relative.

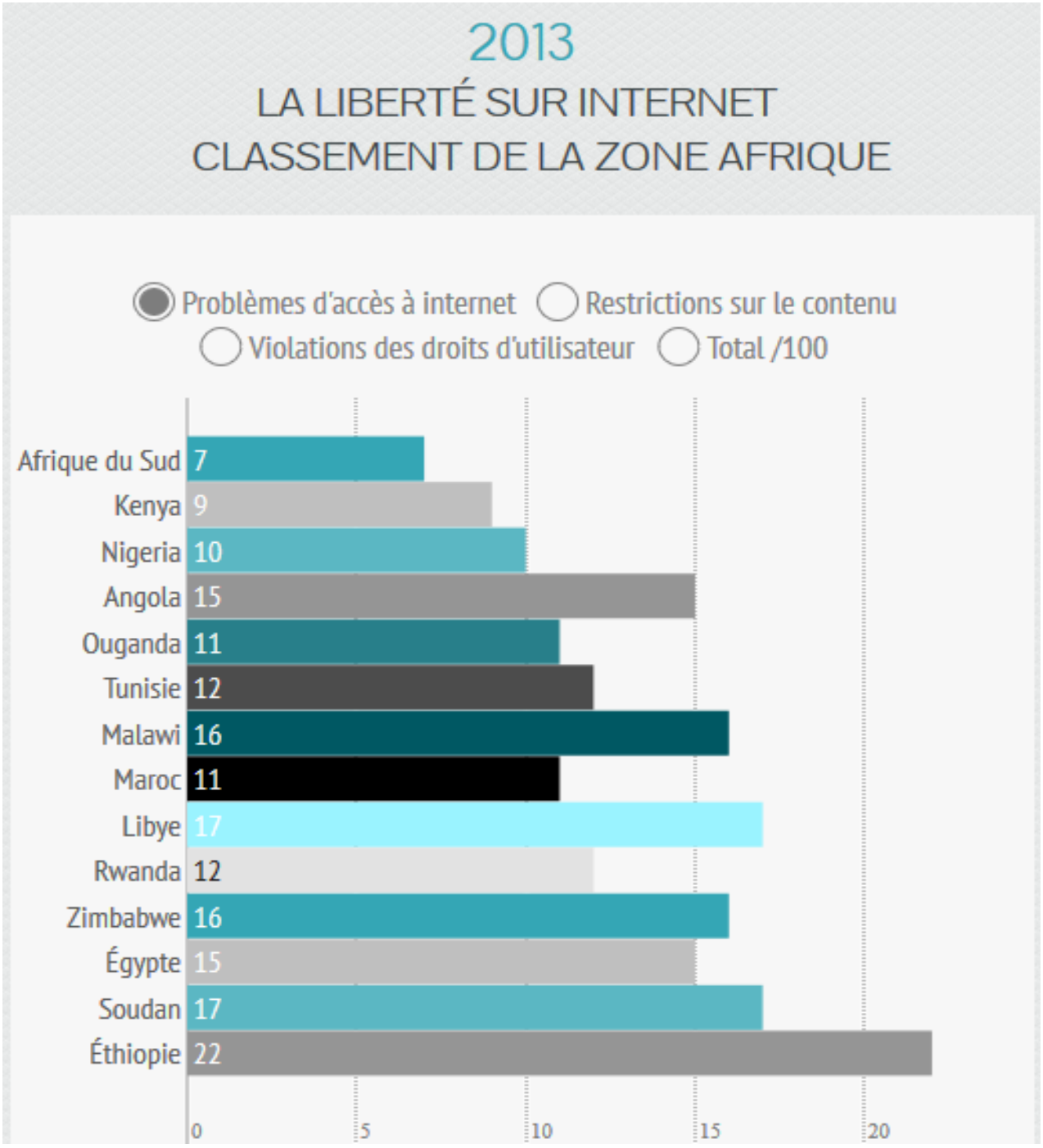
Chaque année, l'ONG américaine *Freedom House* publie son rapport[14] sur la liberté sur Internet à travers le monde. La dernière édition, du 03 octobre 2013, pointe du doigt une liberté de plus en plus en régression dans bon nombre des soixante pays que l'ONG observe.

Parmi ces soixante pays, quatorze sont africains. Le Soudan et l'Ethiopie sont bons derniers dans le respect d'un Internet libre. En effet, le Soudan a pratiqué de façon acharnée la censure des journalistes et des bloggeurs, et un projet de loi a été déposé pour restreindre davantage la liberté d'expression sur Internet. L'Ethiopie, quant à elle, est le seul Etat de l'Afrique subsaharienne à avoir mis en œuvre un système de filtrage du Web au niveau national.

Si l'Afrique du Sud est qualifiée de *« pays africain le plus libre »* par l'ONG, onze des quatorze Etats africains que compte le rapport ne sont que *« partiellement libres »*, et notamment le Kenya, le Malawi, le Nigéria, le Rwanda et le Zimbabwe.

Facebook et les autres géants du Web devront donc prendre leur mal en patience car ils risquent fort de se heurter à la réticence de nombreux Etats africains, qui ne voient pas d'un très bon œil l'utilisation du Web à outrance, notamment à des fins privées, ludiques et divertissantes.

[14] « Freedom In The World 2013 », Freedom House, Octobre 2013



Infographie extraite du rapport « Freedom In The World 2013 », Freedom House

CONCLUSION

Les « dirigeants » du Web n'en ont pas fini de jongler entre éthique, tentation, conquête de nouveaux marchés et fidélisation et satisfaction des internautes.

S'ils ne peuvent pas nier leur implication dans l'affaire Snowden et leur goût très prononcé pour le profit, il est important de rappeler que, à leur décharge, le Net reste une zone de non droit au sein de laquelle il est difficile de satisfaire toutes les parties prenantes et d'harmoniser la législation à l'échelle mondiale.

Ainsi se pose inévitablement la question d'une gouvernance mondiale du Net. Les 23 et 24 avril dernier s'est tenu, à Sao Paulo, une « réunion multipartite mondiale sur l'avenir de la gouvernance mondiale de l'Internet », réunissant plus de 700 parties prenantes. L'objectif de ce sommet : arriver à un consensus sur les grands principes de la gouvernance du Net au niveau mondial. La gouvernance du Net représente un enjeu de taille dans les relations internationales, chaque Etat souhaitant mettre sa pierre à l'édifice de la « souveraineté numérique ».

Le fait est qu'il ne peut y avoir qu'une seule gouvernance du Net, mais plutôt une gouvernance par enjeu. La cybersécurité, la liberté d'expression, la protection des données, l'adoption de standards techniques, sont autant d'enjeux qui ne peuvent être regroupés en une seule et même gouvernance.

La Commission européenne s'est également saisie du sujet, en s'engagent à *« lancer une revue approfondie des risques posés au niveau international par les conflits de loi et de juridiction suscités par l'Internet, et à employer tous les outils disponibles permettant de les résoudre »*.

Les géants du Web bénéficieront donc peut-être un jour d'un Internet plus régulé, plus encadré et dans lequel leur rôle sera mieux défini. En attendant cette nouvelle ère numérique, les mastodontes américains devront combiner du mieux possible leurs différents rôles au sein du cyberespace, et ce, sans perdre de vue que, au-delà des règles imposées par l'économie de marché, leur priorité devrait être, sur le long terme, une réelle lutte contre la cybercriminalité.

BIBLIOGRAPHIE

RAPPORTS

- RAPPORT DE L'ONG FREEDOM HOUSE. Freedom In The World 2013, octobre 2013
- SOLUCOM. Cybercriminalité : comment agir dès aujourd'hui, octobre 2013
- THOMAES R. & LAMBRECHT P. Belgian Cyber Security Guide, Protect Your Information, mars 2014
- LIBRARY OF PARLIAMENT. Cybersécurité et renseignement de sécurité : l'approche des Etats-Unis, juin 2011
- LEMARCHAND H. & LOUIS-SIDNEY B. Cybersécurité des pays émergents, état des lieux, mars 2014
- KASPERSKY LAB. Kaspersky Security Network, 2013
- CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES. The Economic Impact Of Cybercrime And Cyber Espionage, juillet 2013

ARTICLES DE PRESSE

- KIBANGULA T. Top 14 des pays africains les plus libres sur Internet, 08 octobre 2013, http://www.jeuneafrique.com/Article/ARTJAWEB20131007174801/ (site consulté à plusieurs reprises durant la période de rédaction)
- ANKILI H. Mark Zuckerberg veut une Afrique connectée, 23 août 2013, http://www.afrik.com/marc-zuckerberg-veux-une-afrique-connectee (site consulté à plusieurs reprises durant la période de rédaction)
- OLIVIER M. Côte d'Ivoire : blogueurs contre brouteurs !, 22 novembre 2013, http://www.jeuneafrique.com/Article/ARTJAWEB20131121182726/ (site consulté à plusieurs reprises durant la période de rédaction)

- 20MINUTES.FR. L'UE étudie le Darknet pour mieux lutter contre la cybercriminalité, 10 février 2014, http://www.20minutes.fr/societe/1295002-20140210-ue-etudie-darknet-mieux-lutter-contre-cybercriminalite (site consulté à plusieurs reprises durant la période de rédaction)
- RTBF.BE. L'UE et les USA renforcent leur coopération en matière de cybercriminalité, 11 janvier 2013, http://www.rtbf.be/info/medias/detail_l-ue-et-les-usa-renforcent-leur-cooperation-en-matiere-de-cybercriminalite?id=7905967 (site consulté à plusieurs reprises durant la période de rédaction)
- AFAPDP. Conseil de l'Europe : coopération contre la cybercriminalité, 10 juin 2012, http://www.afapdp.org/archives/943 (site consulté à plusieurs reprises durant la période de rédaction)
- LACOTE.CH. Microsoft et le FBI lancent une offensive conjointe face à la cybercriminalité, 06 juin 2013, http://www.lacote.ch/fr/societe/multimedia/microsoft-et-le-fbi-lancent-une-offensive-conjointe-face-a-la-cybercriminalite-609-1192235 (site consulté à plusieurs reprises durant la période de rédaction)
- WUILBERCQ E. Comment Facebook s'adapte à l'Afrique, où le mobile est roi, 03 février 2014, http://www.jeuneafrique.com/Article/ARTJAWEB20140203115123/ (site consulté à plusieurs reprises durant la période de rédaction)
- CHEMINAT J. Microsoft se dote d'un centre de lutte contre la cybercriminalité, 15 novembre 2013, http://www.lemondeinformatique.fr/actualites/lire-microsoft-se-dote-d-un-centre-de-lutte-contre-la-cybercriminalite-55685.html (site consulté à plusieurs reprises durant la période de rédaction)
- FILIPPONE D. Les Etats-Unis toilettent leur plan de lutte contre la cybercriminalité, 03 juin 2010, http://www.journaldunet.com/solutions/securite/lutte-contre-le-piratage-aux-etats-unis.shtml (site consulté à plusieurs reprises durant la période de rédaction)
- DUQUESNE M. Microsoft présente son unité de lutte contre la cybercriminalité, 15 novembre 2013, http://www.linformaticien.com/actualites/id/31019/microsoft-presente-son-unite-de-lutte-contre-la-cybercriminalite.aspx (site consulté à plusieurs reprises durant la période de rédaction)
- MEDEF 92. Les marchés noirs de la cybercriminalité, septembre 2012, http://medef.expeert.com/fr/securite-information/blog/1801267-les-marches-noirs-de-la-cybercriminalite (site consulté à plusieurs reprises durant la période de rédaction)

- GHERNAOUTI S. Cyber-guerre : la Suisse n'est pas prête !, 01 mars 2013, http://www.lesobservateurs.ch/2013/03/01/solange-ghernaouti/ (site consulté à plusieurs reprises durant la période de rédaction)
- ZDNET.FR. Un centre européen de lutte contre la cybercriminalité opérationnel en janvier 2013, 29 mars 2012, http://www.zdnet.fr/actualites/un-centre-europeen-de-lutte-contre-la-cybercriminalite-operationnel-en-janvier-2013-39770141.htm (site consulté à plusieurs reprises durant la période de rédaction)
- WALTER F. Les entreprises devraient dépenser 500 milliards de dollars contre la cybercriminalité, 24 mars 2014, http://www.developpez.com/actu/69231/Les-entreprises-devraient-depenser-500-milliards-de-dollars-contre-la-cybercriminalite-selon-une-etude-d-IDC/ (site consulté à plusieurs reprises durant la période de rédaction)
- MLENKOVICH S. Lutte contre la cybercriminalité : un succès international, 29 juillet 2013, https://blog.kaspersky.fr/lutte-contre-la-cybercriminalite-un-succes-international/ (site consulté à plusieurs reprises durant la période de rédaction)
- LAMANDE E. CLUSIF : panorama de la cybercriminalité 2013, janvier 2014, http://www.globalsecuritymag.fr/CLUSIF-panorama-de-la,20140120,42351.html (site consulté à plusieurs reprises durant la période de rédaction)
- DH.BE. La lutte contre la cybercriminalité renforcée, 07 janvier 2014, http://www.dhnet.be/actu/new-tech/la-lutte-contre-la-cybercriminalite-renforcee-52cc1d653570105ef7e6fc89 (site consulté à plusieurs reprises durant la période de rédaction)
- NOCETTI J. & MASSIT-FOLLEA F. Internet se cherche une gouvernance, 23 avril 2014, http://www.lemonde.fr/idees/article/2014/04/23/internet-se-cherche-une-gouvernance_4405625_3232.html (site consulté à plusieurs reprises durant la période de rédaction)