Observatoire du Monde Cybernétique
Trimestriel

Septembre 2013

DELEGATION AUX AFFAIRES STRATEGIQUES
MINISTERE DE LA DEFENSE

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

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

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

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

Sommaire

1. Cyberespace et « situational awareness »

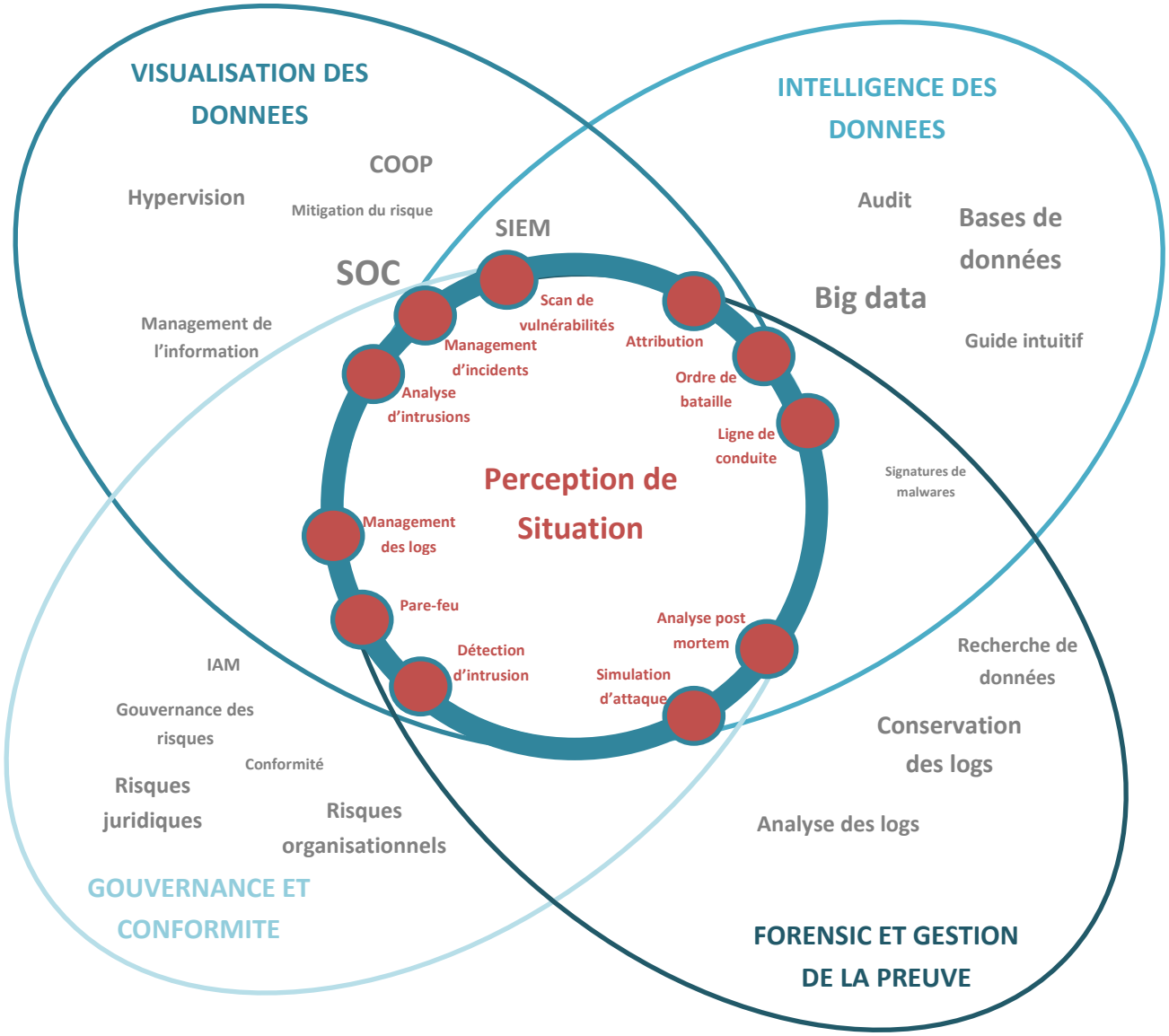
L'un des principaux défis dans la mise en place d'une capacité de cyberdéfense civile ou militaire est d'assurer le « situational awareness » ou « perception de situation », c'est à dire non seulement la capacité de percevoir son environnement, mais également de le comprendre et de s'y projeter.

Et ce à différents niveaux. Au niveau des Etats tout d'abord. Les attaques subies par l'Estonie en 2007 ont montré que le pays avait manqué d'une vision globale et partagée de la situation. Au niveau des forces armées, ensuite : la gestion des opérations « cyber » ou des opérations intégrant des aspects « cyber » passe nécessairement par un suivi permanent de la situation. Au niveau des entreprises, notamment des opérateurs d'infrastructures vitales, enfin : l'efficacité d'un Security Operation Center, voire d'un dispositif global de gestion des risques, dépend de l'appréhension de la situation.

L'établissement de cette vision partagée est cependant complexe en raison des spécificités du cyberespace :

- Niveau d'abstraction des couches logiques et cognitives ;
- Intégration croissante du cyberespace aux environnements physiques ;
- Vitesse de circulation de l'information ;
- Multiplicité des acteurs publics et privés impliqués ;
- Croissance exponentielle des informations et multiplicité des équipements et outils émettant des données utiles à la gestion des risques (système de détection d'intrusion, scanner de vulnérabilité, antivirus, système de corrélation d'événements…) qui sont de plus rarement interopérables.

« Cyber Situational Awareness »



1.1 Point de passage obligé : l'établissement d'une « cyber common operational picture » (CCOP)

L'établissement d'une vision partagée du « champ de bataille » ou « cyber common operational picture » (CCOP) est le préalable indispensable au « situational awareness »[1].

La COOP permet :

- La visualisation du champ de bataille. Elle comprend plusieurs aspects :
    - La connaissance de la situation actuelle : localisation en temps réel des actifs, de leur statut juridique (amis ou ennemis si l'on se situe dans un contexte militaire[2]), de leur statut technique, mais également identification des attaques (type, cible, auteur…) ;
    - Le suivi de cette situation en temps réel et dans la durée,
- La connaissance de l'environnement global : « ordre de bataille » des forces en présence dans le domaine militaire, connaissance et suivi des menaces internes et externes, des vulnérabilités de l'organisation.

Cette CCOP sert aussi de support :

- A l'évaluation des dommages réels et prévisibles en fonction des scénarios ;
- A l'analyse post-incident : recherche de causalité, back tracking, forensic ;
- A l'aide à la décision. La CCOP doit permettre d'anticiper les actions ou réactions ennemies et de dégager plusieurs options possibles, à charge pour l'utilisateur de choisir l'option lui paraissant la plus adaptée ;
- A la planification des opérations (ciblage, analyse de mission, analyse des effets projetés, conformité avec les règles d'engagement…) ;
- A la conduite des opérations elles-mêmes.

[1] Lire à ce propos l'étude intitulée "Toward a Cyber Common Operating Picture » de Gregory Conti, John Nelson, David Raymond : http://www.rumint.org/gregconti/publications/130324_CyCon_CCOP_v28_final.pdf

[2] Il n'existe pas à proprement parler d'IFF « cyber ».

1.2 Quels défis ?

Plusieurs défis sont à relever dans l'établissement de la « Common Operational Picture » :

- ***La fusion de données hétérogènes et en progression constante.*** L'exhaustivité dans le domaine cyber est impossible à obtenir compte tenu de la nature complexe et très changeante de l'environnement. Le point de départ est donc de définir un périmètre d'intérêt, avec la capacité à tout moment de « zoomer » sur une zone ou, au contraire, d'élargir le champ. Autre challenge : prendre en compte les problèmes de classification des données et de coopération entre différents acteurs, notamment dans un contexte « public-privé » ou dans le cadre de coalitions. L'interopérabilité des CCOP suppose ainsi l'utilisation d'un référentiel commun en matière d'information[3] ;

- ***L'analyse prédictive, tant en terme de pertinence que de rapidité.*** Cette analyse implique que l'utilisateur ait confiance dans le système. Au plan technique, l'utilisateur doit donc pouvoir à tout moment remonter aux données brutes. Un outil « boîte noire » ne saurait donc donner pleinement satisfaction ;

- ***Les interactions entre les différentes couches du cyberespace*** et avec l'environnement physique ;

- ***La « scalabilité ».*** Au plan temporel, il s'agira de pouvoir remonter dans le temps ou de se projeter dans l'avenir. Au plan spatial, l'utilisateur pourra à tout moment « zoomer » sur un détail ou explorer une nouvelle zone. Au plan organisationnel, enfin, l'image fournie doit pouvoir s'adapter aux différents niveaux de l'entreprise (expert sécurité, RSSI, risk manager, DG). Même chose dans le monde militaire avec les niveaux tactique, opératif et stratégique. Chaque niveau doit ainsi accéder uniquement à l'information nécessaire pour éviter tout risque de sur-information.

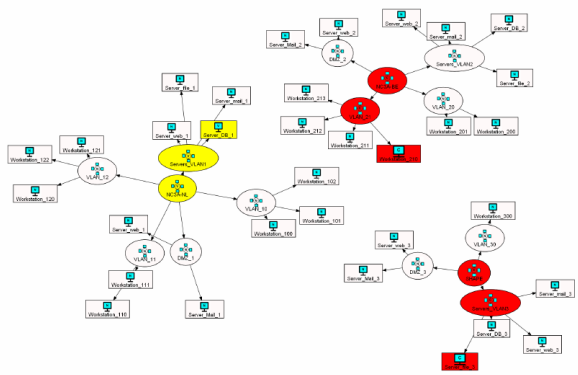
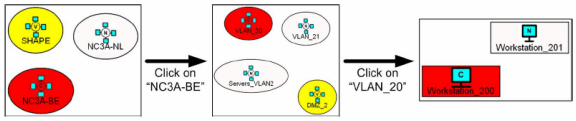
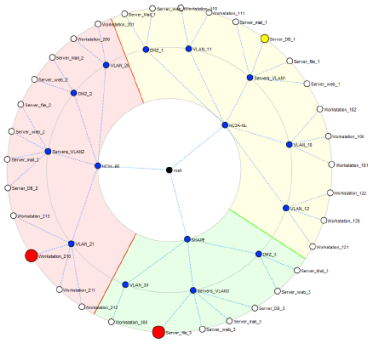
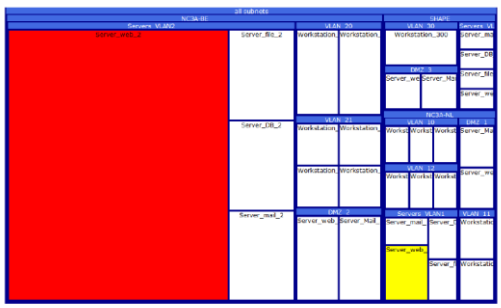
  Plusieurs questions à ce propos : faut-il prévoir un seul système avec des interfaces différentes ou plusieurs systèmes différents ? Le plus réaliste est pour l'instant de s'appuyer sur des systèmes différents mais interopérables. Plus on monte vers les niveaux stratégiques, plus le dispositif doit en effet être « cross domain » et intégrer une vision globale combinant environnement physique et environnement cyber : opérations combinées (artillerie, infanterie…) ou conjointes (air, terre, spatial…). Même constat dans l'entreprise où le dirigeant devra posséder une vision globale combinant IT et processus métiers ;

- ***La visualisation.*** Celle-ci ne saurait reposer que sur des suites de tableaux mais doit intégrer des systèmes interactifs, avec des affichages dynamiques et graphiques. Plusieurs

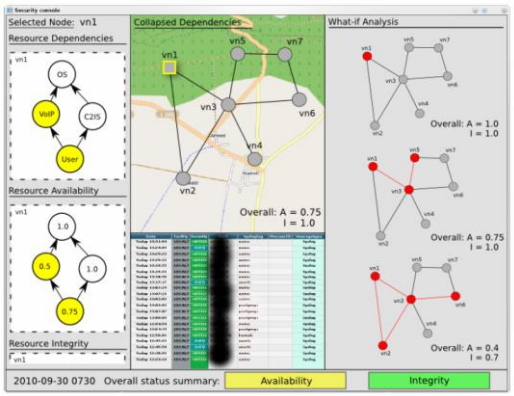
[3] Exemple de référentiel proposé par l'OTAN : http://ftp.rta.nato.int/public//PubFullText/RTO/MP/RTO-MP-IST-091///MP-IST-091-P03.doc.

techniques de visualisation[4] de réseau ont par exemple été présentées lors des journées SSTIC de 2010, l'objectif étant de combiner ces différentes vues dans une même interface de façon à disposer d'une vision à la fois géographique et logique ;

Exemple de techniques de visualisation

<table>
<tr>
<td>Réseau à plat (GraphViz)
  </td>
<td>Vue hiérarchique (GraphViz)
 
</td>
</tr>
<tr>
<td>Vue radiale (radialnet)
  </td>
<td>Vue treemap (thejit.com)
  </td>
</tr>
</table>

[4] https://www.sstic.org/media/SSTIC2010/SSTIC-actes/CyberDefense/SSTIC2010-Article-CyberDefense-lagadec.pdf

Vue géographique	Interface combinée[5]
	

- **L'IHM.** Elle est fondamentale pour assurer une boucle OODA plus rapide que l'adversaire. Il existe malgré tout une limite : les capacités humaines n'évoluent pas, contrairement à la quantité de données disponibles et aux capacités d'affichage informatique. Rien ne sert donc de multiplier les écrans. Il faut plutôt des systèmes qui stimulent l'utilisateur. Les environnements 3D offrent ainsi plusieurs avantages : immersion accrue, possibilité de convergence entre différents capteurs... Les écrans tactiles sont également perçus comme des moyens d'accélérer le tempo des opérations. On observe d'ailleurs que dans certains programmes de R&D américains le clavier est perçu comme un élément retardateur ;

- **L'automatisation.** Avec toutefois deux écueils : le tout automatique déshumanisé et le totalement manuel. Le cyberespace n'est pas qu'un environnement technique. Derrière les ordinateurs, il y a des hommes. Mais en même temps, la spécificité temporelle du cyberespace rend indispensable une automatisation partielle de certains processus. Il y a donc un juste équilibre à trouver dans lequel le système doit fournir des données, proposer des options, que l'analyste doit ensuite analyser et choisir.

[5] http://www.marko-jahnke.de/docs/work/rto-rws10.pdf

1.3 Quels technologies et outils ?

Le « situational awareness » dans le cyberespace suppose le recours à différentes familles d'outils :

- **Les systèmes SIEM.** Exemples : HP ArcSight, IBM Q1 Labs. RSA, Symantec.
- **Les technologies « big data ».** Exemples : Splunk. Palantir.
- **Les outils d'analyse et de visualisation de données.** Exemples : IBM Analyst Notebook, GraphViz.
- **Les centres de commandement ou centres opérationnels.** Ceux-ci sont parfois appelés « hyperviseur », leur objectif étant de passer de la supervision à l'hypervision en intégrant l'ensemble des données et outils sur la même interface et surtout en connectant les événements techniques aux missions de l'organisation considérée et aux risques « métier »). On les retrouve aussi bien dans le monde civil (gestion technique de bâtiments[6], infrastructures physiques, systèmes d'information, sécurité des systèmes d'information…), que dans la sécurité intérieure ou la défense.

Exemples de solutions supportant des centres de commandement « cyber » ou intégrant une dimension « cyber » :

- Sentinel (BlueSpace[7]),
- IC3 (Northrop Grumman[8]),
- CoMotion Cyber (General Dynamics[9]),
- Cybel (Thales[10]),
- TAME Center (IAI[11]),
- Virtual Ops Center (Infosys[12]),
- Visual Command Center (IDV Solutions[13]),
- Nice Situator (Nice Systems[14]),
- NeuralStar (Kratos Defense[15]).

[6] http://www.mesures.com/archives/827-Hypervision.pdf
[7] http://bluespace.com/cyber/
[8] http://www.northropgrumman.com/Capabilities/Cybersecurity/Documents/Assets/IC3_factsheet.pdf
[9] http://www.gdc4s.com/comotion-cyber-product-detail-page.html
[10] http://www2.thalesgroup.com/extras/cybersecurity/
[11] http://www.globes.co.il/serveen/globes/docview.asp?did=1000845458&fid=1725
[12] http://www.infosys.com/industries/aerospace-defense/white-papers/Documents/virtual-ops-center.pdf
[13] http://www.idvsolutions.com/company/releases/2012/Visual-Command-Center-at-ASIS.aspx
[14] http://www.nice.com/situation-management/nice-situator

1.4 Quelques projets de R&D en cours

1.4.1 Le Defense Science and technology Laboratory

Le Defense Science and technology Laboratory du ministère de la Défense britannique a lancé en octobre 2012 dans le cadre de son Cyber & Influence programme un appel à projets intitulé "cyber situational awareness"[16]. Parmi les projets retenus : le N.Guru Cyber Situational Awareness System mené par Northrop Grumman, en partenariat avec les Universités d'Oxford et de Glamorgan[17]. A noter que dans le cadre du même programme, le Ministère de la défense britannique finance également la conception d'un Virtual Cyber Centre of Operation (VCCO) par EADS IW. Objectif de ces programmes : parvenir à une amélioration des capacités opérationnelles en 2015.

1.4.2 Le projet VIS SENSE

Le projet VIS SENSE (Visual Analytic représentation of large datasets for enhancing network security) est financé par le programme cadre européen FP7. Les partenaires français sont Eurecom et Telecom Sud Paris. Objectif : développer de nouvelles technologies et méthodes d'analyse visuelle pour l'identification et l'anticipation de situations à risque en matière de cybersécurité[18].

1.4.3 Le projet Plan X de la DARPA américaine[19].

L'objectif est d'imaginer le cyber warfare « clés en main » de demain afin que le non spécialiste puisse mener des opérations dans le cyberespace grâce à un système intuitif. Une grande priorité est donc accordée à l'IHM et à la représentation du cyberespace. Plusieurs sociétés spécialisées dans le jeu vidéo, l'animation ou le design interviennent ou sont ainsi intervenus sur ce volet comme Frog Design ou Massive Black[20].

---

[15] http://www.kratosdefense.com/solutions/tts/cybersecurity-ia/cybersecurity_situational_awareness
[16] http://www.science.mod.uk/events/event_detail.aspx?eventID=184
[17] http://www.unmannedsystemstechnology.com/2013/09/northrop-grumman-to-develop-cyber-visualisation-tools-as-part-of-uk-research-program/
[18] http://www.vis-sense.eu/
[19] Pour une description détaillée de ce programme : http://www.ceis.eu/fr/management-des-risques/actu/note-strategique-la-nouvelle-initiative-de-defense-strategique
[20] http://www.wired.com/dangerroom/2013/05/pentagon-cyberwar-angry-birds/all/

2. Cybersécurité des pays émergents : état des lieux

> **« *La fracture digitale existante ne doit pas se doubler d'une fracture sécuritaire, encore moins d'une dépendance plus forte à des entités qui contrôleraient [les] besoins et moyens de sécurité des technologies de l'information* ».**
>
> Union Internationale des télécommunications, Guide de la cybersécurité pour les pays en développement, 2006, p. 6

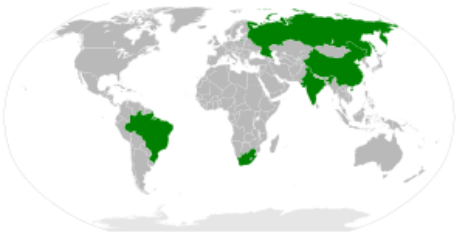
Appréhender la question de la cybersécurité des pays émergent, c'est lever le voile sur des problématiques distinctes, et donc des stratégies variées. Si les préoccupations de certains pays paraissent, de prime abord, très éloignées les unes des autres [rapports de force très présents, sur des territoires pour certains encore novices face à d'autres très développés (exemple des rapports entre la Chine, superpuissance « cyber », et le continent africain faisant l'objet de nombreuses convoitises)], ces pays sont confrontés, pour beaucoup, à des problématiques similaires (développement des services numériques comme levier économique, réduction de la fracture numérique, aménagement du territoire et gestion de l'installation d'infrastructures, mais aussi transfert et développement des compétences, lutte contre la cybercriminalité…).

Mieux connaître les cyberstratégies et les problématiques auxquelles sont confrontés les pays émergents, c'est tenter de mieux appréhender un contexte aux lignes désormais incertaines. La fonction « égalisatrice » du cyberespace bouleverse en effet les définitions traditionnelles. Ainsi, un pays usuellement perçu comme relativement peu avancé, est aujourd'hui susceptible de disposer de hackers patriotes, et de capacités cyber insoupçonnées.

Ces pays, au potentiel de développement plus ou moins rapide, peuvent donc être analysés à des fins d'anticipation, dans un contexte où les rapports de force évoluent rapidement.

Après un point sur la notion de « pays émergent » et sa pertinence dans le milieu « cyber », un rapide état des lieux sera fait sur la question du déploiement des infrastructures IT et des usages numériques dans ces pays (partie 1). Ces mutations, sources d'opportunités de développement, sont accompagnées de risques numériques. Comment les pays émergents gèrent-ils leur écosystème cybercriminel et hacktiviste ? Comment organisent-ils leur cyberdéfense ? (partie 2).

La notion de « pays émergents » comprend les BRICS (Brésil, Russie, Inde, Chine et Afrique du Sud) mais également certains pays du continent africains à l'image du Sénégal.

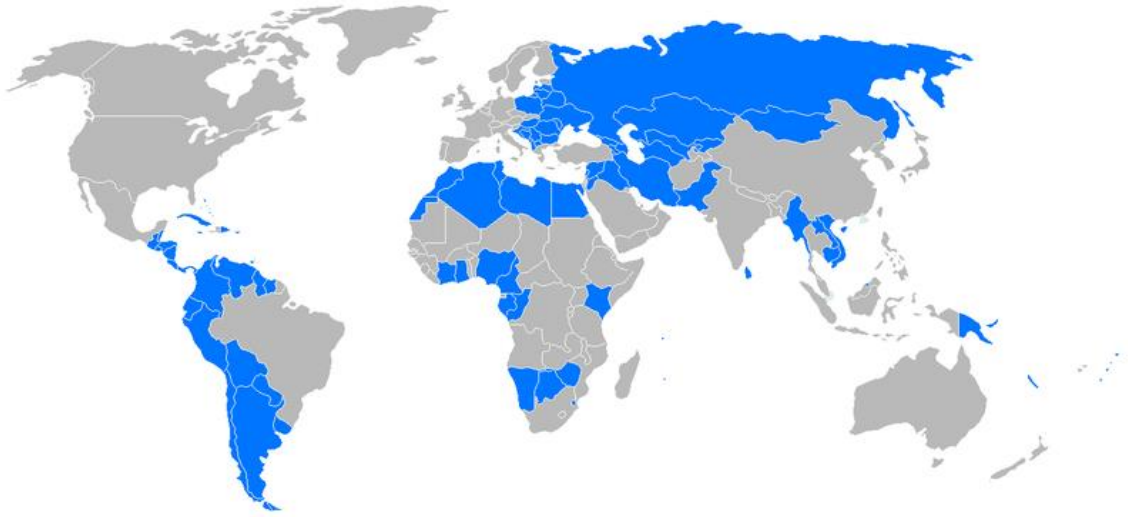


La notion de BRIC est une notion qui a été employée la première fois en 2001 par l'économiste Jim O'NEIL dans une note interne à la banque qui l'employait, Goldman Sachs[21]. Cette note mettait en avant la forte croissance du PIB des BRIC qui égalerait en 2040 celui des Etats membres du G6 (Etats-Unis, Japon, Royaume-Uni, Allemagne, France et Italie). En 2011, l'Afrique du Sud, malgré une puissance économique peu comparable aux pays des BRIC, a obtenu de rejoindre ce groupe, l'acronyme devenant alors BRICS.

Au plan mondial, les BRICS représentent actuellement 18 % du produit intérieur brut (PIB), 40 % de la population, 15 % du commerce et 40 % des réserves monétaires[22]. Forts de ces arguments de poids, les BRICS aspirent à une place importante dans la gouvernance mondiale, notamment dans le domaine économique, dont la récente création d'une banque de développement comme une alternative à la Banque Mondiale[23] témoigne de leur volonté, et en matière diplomatique[24].

Mais se limiter aux pays des BRICS ne permettrait pas de balayer l'ensemble du spectre des pays émergents. Plus largement donc, les pays émergents sont ceux dont le PIB par habitant est inférieur à celui des pays développés mais qui font preuve d'une croissance économique rapide. Et ce concept est d'autant plus vrai en matière de cybersécurité, domaine dans lequel ces pays cherchent à obtenir plus de pouvoir dans la gouvernance du cyberespace ou accueillent sur leur sol des entreprises spécialisées en la matière.

[21] http://www.ladocumentationfrancaise.fr/dossiers/d000534-l-emergence-des-brics-focus-sur-l-afrique-du-sud-et-le-bresil/la-montee-en-puissance-du-groupe-des-brics-bresil-russie-inde-chine-afrique-du-sud
[22] GERVAIS-LAMBONY (P.), *Afrique du Sud. Entre héritages et émergences*, Documentation photographique, 2012, n°8088, 64 p.
[23] http://lecercle.lesechos.fr/economistes-project-syndicate/autres-auteurs/221171835/brics-creent-nouvelle-banque-developpement-no
[24] LAFARGUE (F.), « Des économies émergents aux puissances émergentes » in *A la recherche des Européens*, 2011, 128 p.



By User:AlexCovarrubias - imported by MaCRoEco 12:18, 26 April 2007 (UTC) [Public domain], via Wikimedia Commons

De manière générale, les pays émergents sont confrontés à la nécessité d'intégrer la société de l'information afin de combler la fracture numérique existant vis-à-vis des pays développés. Mais comme le concède l'UIT[25], « *la fracture digitale existante ne doit pas se doubler d'une fracture sécuritaire, encore moins d'une dépendance plus forte à des entités qui contrôleraient leurs besoins et moyens de sécurité des technologies de l'information* ».

Afin de conserver un spectre ciblé, nous incluront dans les pays émergents ceux d'Amérique latine et centrale, d'Asie et d'Afrique. Les pays du Moyen-Orient ayant fait l'objet d'un focus dédié dans une précédente note trimestrielle.

[25] Union Internationale des télécommunications, Guide de la cybersécurité pour les pays en développement, 2006, p. 6

Partie 1 : La croissance des infrastructures numériques et la mutation des usages

Certains pays émergents sont aujourd'hui confrontés à une véritable problématique de dépendance numérique (infrastructures et services Web). Ce qui contraste fortement avec leur avance considérable avance sur les questions d'identité numérique. Etat des lieux.

1.1 Des services numériques en fort développement

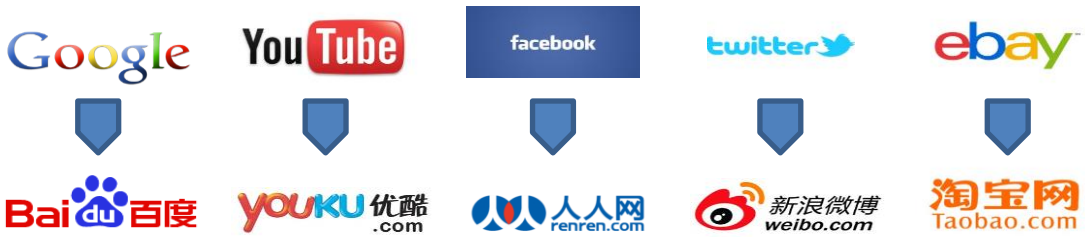
1.1.1 Le numérique, moteur de croissance

Le numérique s'impose comme un véritable moteur de croissance, puisqu'il devrait générer 64% de la croissance mondiale en 2017 pour atteindre 1674 milliards de dollars[26]. Et les pays émergents devraient tirer leur épingle du jeu : les BRICS, mais aussi l'Argentine ou l'Indonésie, génèreront près de 37% de la croissance du secteur du numérique.

Selon l'Institut de l'audiovisuel et des télécoms en Europe (Idate), le marché du numérique a enregistré un ralentissement de sa croissance au niveau mondial en 2012 mais connait cependant une croissance rapide dans les pays émergents : l'Afrique et le Moyen-Orient (+ 8,2%), l'Amérique Latine (+ 5,2%) et l'Asie Pacifique (+ 3,9%) sont en forte croissance alors que l'Europe stagne à 0,1%[27].

1.1.2 Le développement de services numériques « nationaux »

Le numérique prend une telle importance au sein des pays émergents que bien des services que l'on retrouve dans les pays développés ont été créés et adaptés aux pays émergents. L'exemple chinois est à cet égard très explicite[28] :



[26] http://www.pwc.com/gx/en/global-entertainment-media-outlook/index.jhtml
[27] http://www.ecrans.fr/Numerique-le-marche-ralentit-en,16431.html
[28] http://www.relevanceweb.com/blog/item/internet-in-the-bric-countries

Source : Red social

A l'image de la Chine qui propose ses propres services comme une véritable alternative aux géants mondiaux, principalement américain, d'autres pays émergents ont mis en place des services qui leurs sont propres. Cela se vérifie surtout au niveau des réseaux sociaux : le gouvernement cubain a ainsi mis en place son « facebook like » avec Red social[29]. Il en va de même en Afrique où des services dépassant le simple cadre des réseaux sociaux sont apparus[30] :

- **Ushaidi**[31] (Kenya) a permis aux Kenyans de communiquer lors des élections de 2008, notamment sur des soupçons de fraude. L'outil permet aussi de créer son propre blog, d'avoir une boite mail et un service d'envoi/réception de SMS ;
- **Afrigator**[32] (Afrique du Sud) est un agrégateur de contenu destiné à toute l'Afrique ;

Source : Afrigator

- **Zoopy**[33] (Afrique du Sud) permet le partage de vidéos, etc.

Ces services Web interafricains ont néanmoins dû s'adapter à la multitude de langues sur le continent.

Et cette demande en matière de numérique ne fera que croitre : d'ici 2015, le nombre d'utilisateurs Internet pour les BRIC devrait doubler pour atteindre 1,2 milliards d'individus selon un rapport du Boston Consulting Group[34].

[29] http://www.foxcrawl.com/2011/12/03/cuba-released-own-social-network-redsocial-a-copy-of-facebook/
[30] http://terangaweb.com/lafrique-et-les-reseaux-sociaux-virtuels/
[31] http://www.ushahidi.com/
[32] http://www.afrigator.com/
[33] http://www.zoopy.com/
[34] http://www.computerworlduk.com/news/public-sector/3237588/internet-users-in-bric-countries-to-double-by-2015/

1.1.3 Des pays en avance sur l'identité numérique

Autrefois handicapés par des problèmes de recensement de leur population, les pays émergents se sont saisis de ces problématiques et ont acquis une avance considérable en matière de numérisation de l'identité. Cela passe par le déploiement de documents d'identité sécurisés via l'adoption de cartes d'identités biométriques (tandis que des pays comme la France viennent seulement de passer au permis de conduire biométrique)[35], mais aussi par la définition de certaines politiques en matière d'identification sur le Web.

Cette volonté de moderniser, de dématérialiser le système existant se justifie d'abord par la facilitation du recensement et de la délivrance de documents d'identité. Pour autant, si certains pays ont réussi à créer un véritable e-Etat du fait d'une population peu importante, à l'image de l'Estonie et de ses 1,3 million d'habitants[36], d'autres s'attèlent à un travaillent bien plus herculéen au regard du nombre d'habitants qu'ils comptent : quand la Russie compte 143 millions d'habitants, l'Inde ou la Chine en recense plus d'un milliard[37].

Cette dématérialisation du système se justifie ensuite par la volonté dépasser les difficultés de mise en œuvre de prérogatives telles que vote. Dans certains pays venant tout juste de mettre en place un système démocratique, l'organisation d'élections s'avère souvent compliquée, et susceptible de compromettre leur stabilité politique.

1.1.3.1 L'usage croissant de l'enrôlement biométrique

Beaucoup de pays africains se sont penchés ces dernières années sur l'enrôlement biométrique de leurs citoyens, avec comme objectif premier de les recenser et de réduire les risques de fraudes en matière d'usurpation d'identité ou de maîtrise de la population présente sur le territoire. Telle a été l'initiative du Gabon qui a lancé le 30 juillet dernier une opération d'enrôlement biométrique de ses citoyens au plan national[38], notamment dans le but de préparer les listes pour les prochaines élections. Les Philippines utilisent également la biométrie pour réviser les listes électorales et résoudre le problème des enregistrements illégaux qui permettaient la fraude et faussaient le résultat des élections[39].

D'autres pays utilisent la biométrie pour des problématiques sécuritaires. Récemment, une haute juridiction pakistanaise a rendu une décision dans laquelle elle impose aux opérateurs de téléphonie mobile d'instaurer l'identification biométrique comme condition d'utilisation de leurs services par leurs clients[40]. Pour se faire, les opérateurs devront connecter leurs matériels avec la base nationale

[35] http://www.lesechos.fr/economie-politique/politique/actu/0203003974424-le-nouveau-permis-de-conduire-securise-arrive-lundi-en-france-604993.php
[36] Banque mondiale
[37] Banque mondiale
[38] http://www.koaci.com/articles-84256
[39] http://newsinfo.inquirer.net/457283/biometrics-to-weed-out-illegal-registrants
[40] http://www.biometricupdate.com/201305/sindh-high-court-orders-sim-card-sales-to-be-biometrically-verified-in-pakistan/

d'identification nommée NADRA (*National Database and Registration Authority*). Cette initiative tend à se déployer dans tout le pays : la police New Dehli a récemment demandé au ministère de l'Intérieur de rendre obligatoire la vente de cartes SIM biométriques en lieu et places des cartes SIM traditionnelles. Objectif : lutter contre le crime, notamment les escroqueries à la nigériane.[41]

Des pays adoptent également la biométrie pour leur système de santé. L'Assurance maladie ghanéenne vient par exemple de lancer un programme pilote consistant à inscrire les ayants droit dans un registre biométrique[42]. Le but de ce programme est d'éviter la duplication des inscriptions et d'accélérer la chaîne de traitement du domaine médical. A titre de comparaison, la Suisse mettra en place un système similaire seulement à la fin de l'année 2013[43].

1.1.3.2 Le programme Aadhaar en Inde

Depuis 2009, l'Inde a entrepris de mettre en œuvre un projet d'identification unique, le projet Aadhaar[44]. Confié à l'autorité indienne de l'identification unique (UIDAI), son objectif est d'assigner un numéro d'identification à 12 chiffres à chaque citoyen indien de manière permanente, l'Inde comptant tout de même près de 1,2 milliard d'habitants (les cartes d'identité étant alors réservées jusque-là aux classes les plus aisées). Le projet AADHAAR a ainsi été lancé dans le village de Tembbhli le 29 septembre 2010.

La base, qui deviendra à terme la plus importante au monde, enregistrera photo, empreintes digitales et iris des citoyens. Fin 2013, 30% de la population indienne devrait être dotée de la carte Aadhaar, ce chiffre devant 50% à l'horizon 2014[45].

Ce projet doit permettre de lutter contre la corruption du pouvoir, de réduire les inégalités et de favoriser le développement économique du pays : chaque année, l'Inde alloue des milliards de roupies aux programmes de lutte contre la pauvreté, mais 85 % des sommes sont détournées par les fonctionnaires ou les chefs de village[46]. La carte Aadhaar contenant les informations biométriques de son porteur, son utilisation permettrait d'accélérer la demande de passeport[47], la fabrication et la délivrance grâce au gain de temps en matière de vérification d'identité. Encore, cet identifiant unique devrait être utilisé pour l'accès aux distributeurs de billets dans le pays[48].

---

[41] http://www.biometricupdate.com/201306/biometric-verification-for-sim-card-sales-should-be-mandatory-delhi-police-commisioner/
[42] http://findbiometrics.com/ghanas-nhia-launches-pilot-to-issue-biometric-id-cards/?utm_source=rss&utm_medium=rss&utm_campaign=ghanas-nhia-launches-pilot-to-issue-biometric-id-cards
[43] http://www.lavenir.net/article/detail.aspx?articleid=DMF20130604_00319419
[44] http://uidai.gov.in/index.php?option=com_content&view=article&id=57&Itemid=105
[45] http://www.igovernment.in/node/44737
[46] COUVELAIRE (L.), « *Un milliard d'Indiens recensés : émoi, émoi, émoi…* », Le Monde, 24 septembre 2011
[47] http://timesofindia.indiatimes.com/india/Aadhaar-biometric-information-may-be-used-for-passports/articleshow/21926047.cms
[48] http://economictimes.indiatimes.com/news/news-by-industry/banking/finance/banking/aadhaar-or-cards-uidai-and-banks-disagree-on-use-of-biometric-authentication-at-atms/articleshow/21437169.cms

1.1.3.3 L'Afrique du Sud a des cartes d'identité biométriques

Afin de réduire les risques de fraudes et d'usurpations d'identité[49], le ministre de l'Intérieur sud-africain a annoncé en juillet 2013 le prochain lancement du projet de cartes d'identité biométriques[50] qui a essentiellement pour but d'apporter des progrès en matière de sécurité tant pour le secteur public comme le secteur privé. En 2014, une partie de la population sud-africaine utilisera ces nouvelles cartes d'identité électroniques, remplaçant les livrets d'identité existant. Ces nouvelles cartes devraient être utilisées pour les prochaines élections selon le ministre des Affaires intérieures, Nkosazana Dlamini-Suma[51].

Le Ministère de l'Intérieur sud-africain a également annoncé que la nouvelle carte d'identité électronique devrait remplacer les systèmes d'enregistrement civil et d'immigration actuels, qui enregistrent actuellement les informations dans un « green ID book », facile à contrefaire et à falsifier[52]. Chaque carte d'identité contiendra une puce intégrée qui stockera les informations des citoyens et leurs données biométriques.

1.1.3.4 L'exemple chinois : la fin de l'anonymat dans le cyberespace

Le 28 décembre 2012, l'agence de presse Reuters annonçait que la Chine avait adopté une nouvelle réglementation pour gérer les informations en ligne afin de « protéger la vie privée »[53]. Le comité permanent de l'Assemblée nationale populaire chinoise a entre autres légiféré sur l'obligation pour les internautes d'utiliser leur véritable identité pour accéder à Internet et poster des messages publiquement[54]. Cette réglementation a d'ailleurs été suivie de directives permettant de poursuivre au pénal les internautes diffusant de fausses informations sur les réseaux sociaux[55].

[49] http://www.biometricupdate.com/201302/south-african-department-of-home-affairs-to-issue-smart-id-cards-this-year/
[50] http://www.zdnet.com/south-africa-prepares-to-launches-smart-id-card-project-7000017680/
[51] http://www.biometricupdate.com/201303/smart-id-cards-could-be-used-in-next-south-african-general-election-minister/
[52] http://www.secureidnews.com/2012/04/30/south-africa-pilots-smart-card-based-national-id-system
[53] http://www.reuters.com/article/2012/06/07/us-china-internet-idUSBRE8560AM20120607
[54] http://www.01net.com/editorial/583229/l-etat-chinois-met-fin-a-l-anonymat-en-ligne-pour-mieux-controler-internet/
[55] http://abonnes.lemonde.fr/asie-pacifique/article/2013/09/10/la-chine-enverra-en-prison-les-internautes-diffuseurs-de-rumeurs_3475338_3216.html

1.2 Un retard considérable sur les infrastructures : du désenclavement à la dépendance numérique

Dans un contexte de prise de conscience de l'importance de la « souveraineté numérique » (et donc de la souveraineté des données), la situation de certains pays émergents semble préoccupante. De plus en plus dépendant des équipementiers principaux, certains Etats cherchent le désenclavement au prix de leur souveraineté numérique.

1.2.1 Le cas de l'Afrique

Le continent africain est en pleine mutation en raison d'investissements issus principalement de l'extérieur. Si d'un côté les Chinois participent activement au développement de l'Afrique, d'autres sociétés étrangères ne sont pas en reste.

La Chine investit massivement dans l'Afrique : en 2000, les échanges entre Pékin et le continent africain s'élevaient à 6,5 milliards de dollars contre plus de 166 milliards de dollars en 2011[56]. Souvent critiquée sur sa politique commerciale en Afrique, la Chine a comme stratégie de multiplier les accords commerciaux afin de s'implanter de manière progressive dans les pays africains en construisant des infrastructures jusque-là inexistantes. Tel a été le cas avec le contrat passé entre la Chine et le Kenya en 2013 pour un montant de 5 milliards de dollars, qui prévoit notamment la mise en place de réseaux de télécommunication et des projets liés aux technologies de l'information[57].

La Chine a d'ailleurs inscrit l'objectif de dépasser le seuil de 200 milliards de dollars d'échanges commerciaux avec l'Afrique en 2013[58] dans son Livre blanc sur la coopération économique et commerciale sino-africaine. Ce Livre blanc est d'ailleurs l'occasion pour la Chine de rappeler que cette coopération a permis l'installation de réseaux de fibre optique, de lignes téléphoniques, d'infrastructures de téléphonie mobile, favorisant ainsi l'accès à Internet aux Africains[59].

ZTE et Huawei sont en train de bouleverser le secteur des télécoms en Afrique en fournissant des équipements à MTN, Safaricom, en partenariat avec des banques chinoises comme la China Development Bank ou Exim Bank[60]. Ces entreprises chinoises sont aussi les partenaires privilégiés des Gouvernements africains pour la création des systèmes d'informations nationaux, à l'image du projet de mise en place d'un e-gouvernement au Ghana par Huawei[61] ou d'un service d'e-justice en Tanzanie par ZTE[62]. Huawei attaque même sur le front des terminaux qui utiliseront les

[56] http://www.lemonde.fr/idees/article/2013/08/14/quand-l-afrique-s-eveillera-contre-la-chine_3461702_3232.html
[57] http://www.afrik.com/le-kenya-miroir-de-l-expansion-chinoise-en-afrique
[58] http://economie.jeuneafrique.com/regions/international-panafricain/19280-la-chine-presente-sa-nouvelle-strategie-pour-lafrique.html
[59] http://www.china.org.cn/government/whitepaper/2013-08/29/content_29861255.htm
[60] http://www.lesafriques.com/actualite/asie-afrique-comment-les-grands-groupes-chinois-conquierent-des-ma.html?Itemid=89
[61] http://afriqueitnews.com/2013/03/18/ghana-le-projet-e-government-lance-avec-huawei/
[62] http://afriqueitnews.com/2013/05/27/zte-et-huawei-accuses-despionnage-un-risque-pour-lafrique/

infrastructures que l'entreprise aura elle-même installées : au début de l'année 2013, Microsoft et Huawei ont annoncé le lancement conjoint d'un smartphone à destination du continent africain[63].

Cela soulève aussi quelques questions sur le rôle de ces équipementiers dans le cyber espionnage[64] opéré par le Gouvernement chinois, ces derniers ayant été notamment soupçonnés de complicité aux Etats-Unis dans un rapport du Congrès américain en date du 8 octobre 2012[65] et depuis écartés de la mise en place de certaines infrastructures. L'Afrique ne serait-elle pas ainsi dans une position à risque à son tour ?

Câble sous-marin ACE - Source : ACE

Mais les entreprises chinoises ne sont pas les seules à profiter du sous-développement du continent africain en matière d'infrastructures de télécommunications. Récemment élue *« entreprise télécom de l'année 2013 »* en Afrique par Frost & Sullivan pour *« la mise en œuvre de stratégies de croissance audacieuses »* et *« l'engagement du Groupe à offrir à ses clients des services et des produits de qualité à valeur ajoutée »*[66], Orange tire son épingle du jeu.

Outre sa forte activité d'opérateur de téléphonie mobile (carte ci-dessus) Orange, a mis en service le 19 décembre 2012 le câble sous-marin ACE (Africa Coast to Europe) qui relie dans un premier temps Sao Tomé à la France. Ce câble doit à terme relier plusieurs pays : l'Afrique du Sud, l'Angola, le Bénin,

[63] http://www.latribune.fr/technos-medias/20130206trib000747240/microsoft-et-huawei-partent-a-l-assaut-de-l-afrique-avec-un-smartphone-a-bas-prix.html
[64] http://www.osiris.sn/ZTE-et-Huawei-accuses-d-espionnage.html
[65] http://intelligence.house.gov/sites/intelligence.house.gov/files/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf
[66] http://www.boursier.com/actions/actualites/news/orange-elue-entreprise-telecom-de-l-annee-2013-en-afrique-546512.html

le Cameroun, la République démocratique du Congo, la Côte d'Ivoire, l'Espagne, la France, le Gabon, la Gambie, le Ghana, la Guinée, le Libéria, le Mali, la Mauritanie, la Namibie, le Niger, le Nigéria, le Portugal, le Sénégal, la Sierra Leone et Sao Tomé & Principe[67]. D'un investissement de 700 millions de dollars et d'une longueur finale de 17 000 kilomètres, ce câble est présenté avant tout comme un levier au développement économique, mais permet aussi aux entreprises françaises d'accéder à de nouveaux marchés à l'image d'Alcatel-Lucent qui a procédé à la pose du câble[68].

1.2.2 La problématique du désenclavement

1.2.2.1 L'internet mobile : outil de désenclavement et d'ouverture vers le monde

Le taux de pénétration Internet est un bon indicateur concernant le développement d'un pays en matière de TIC.

Alors que les Etats d'Amérique du Nord sont ceux qui connaissent le plus fort taux de pénétration internet avec 78,6% de la population ayant accès à internet[69], suivis par l'Europe qui affiche un taux de 63,2%, les pays émergents connaissent une forte progression de leur taux de pénétration Internet :

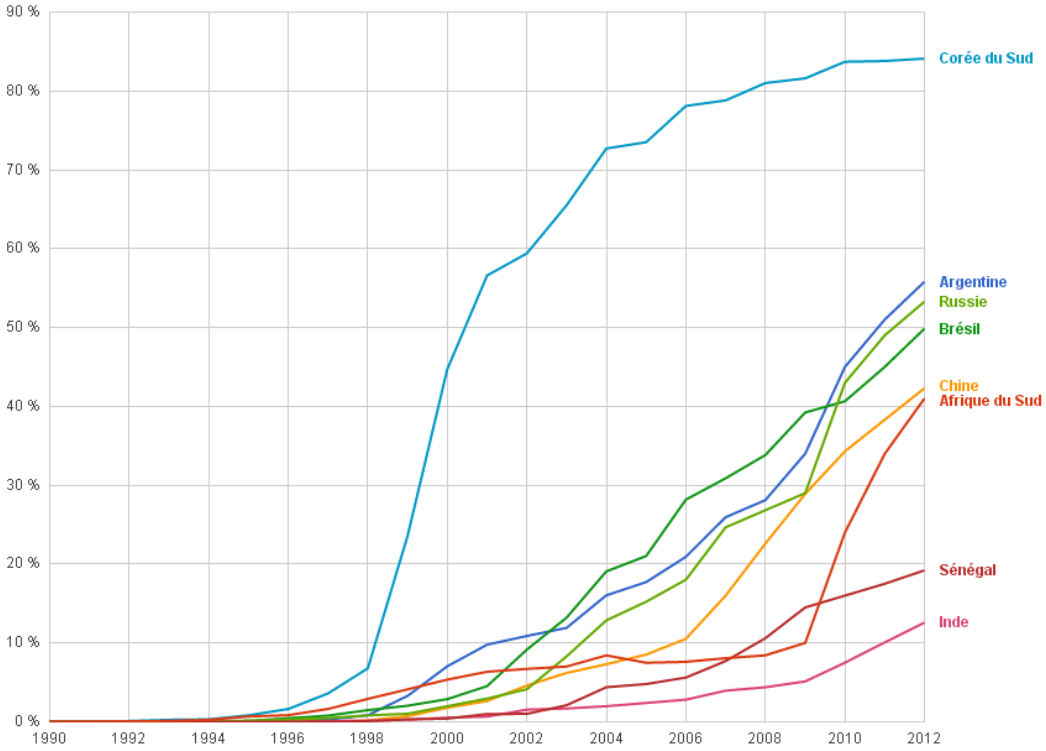
Pays	Utilisateurs internet	Taux de pénétration
Afrique du Sud	6 800 000	13.9 %
Argentine	28 000 000	67,0%
Brésil	81 798 000	42.2%
Chine	513 100 000	38.3 %
Corée du Sud	40 329 660	82,7%

[67] http://www.orange.com/fr/actualites/2012/decembre/mise-en-service-du-cable-sous-marin-ACE-dans-les-13-premiers-pays
[68] http://economie.jeuneafrique.com/regions/international-panafricain/14296-le-cable-sous-marin-ace-entre-en-service-dans-13-pays.html
[69] http://www.internetworldstats.com/stats.htm

Inde	121 000 000	10.2%
Russie	67 982 547	47,7%
Sénégal	1 989 396	15,7%

Taux de pénétration Internet - Source : Internet World Statistics

Et cette tendance ne fait que croitre ces dernières années avec une forte augmentation :



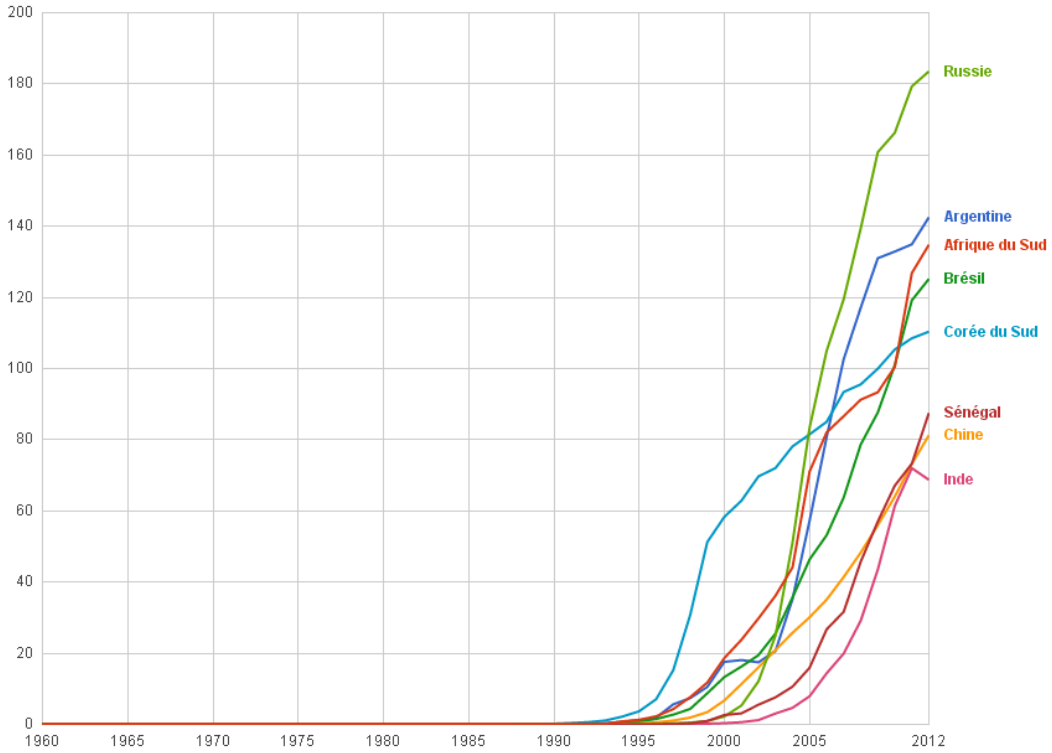
Evolution du taux de pénétration Internet - Source : Banque mondiale

L'augmentation rapide de l'accès à Internet dans les pays émergents s'explique non seulement par le développement des infrastructures, qui a entraîné une baisse des coûts d'utilisation et d'accès[70], mais aussi par la démocratisation de la téléphonique mobile, qui permet un accès à Internet plus flexible, moins lourd, nécessitant l'installation de structures moins importantes. Le continent africain est l'exemple type en la matière puisque l'on ne recense pas loin de 550 millions d'utilisateurs de téléphone mobiles en 2013[71]. L'Internet mobile haut débit est donc parti à la conquête du continent africain peu à peu. Ce qui a notamment ouvert la voie à la création de relais de croissance[72].

Même si la possession d'un iPhone à Dakar n'était pas forcément évidente il y a quelques années (les utilisateurs de l'époque mettant de longs moments à charger leurs mails ou à consulter la moindre page web), celle-ci s'est aujourd'hui démocratisée. Désormais, tous les opérateurs offrent (ou souhaitent offrir) l'accès à Internet par la 3G, bien que l'UIT estime que seulement 3,2 % des utilisateurs 3G dans le monde résident dans les pays émergents.

Car même dans les régions où la 3G est disponible, l'accès à ce type de connexion reste relativement cher. L'arrivée de plusieurs câbles sous-marins près des côtes ouest-africaines dans les prochains mois devrait faire évoluer cette situation dans les pays francophones, qui accusent un certain retard sur leurs voisins anglophones de l'Est et du Sud du continent. Le surplus de bande passante apporté par ces nouvelles infrastructures devant entraîner une baisse des prix de la connexion Internet pour les opérateurs et donc les utilisateurs.

[70] http://businesstech.co.za/news/internet/13358/brics-internet-penetration-sa-lagging-behind/
[71] http://www.jeuneafrique.com/Article/ARTJAJA2523p068-069.xml3/-telephonie-mobile-technologies-marche-380-millions-d-Africains-au-telephone.html
[72] http://www.jeuneafrique.com/Articles/Dossier/ARTJAJA2600p091-093.xml0/internet-facebook-millicom-applele-reveil-de-l-internet-mobile-ou-la-course-a-la-3g.html



Taux de pénétration de la téléphonie mobile en 2012 - source : Banque mondiale

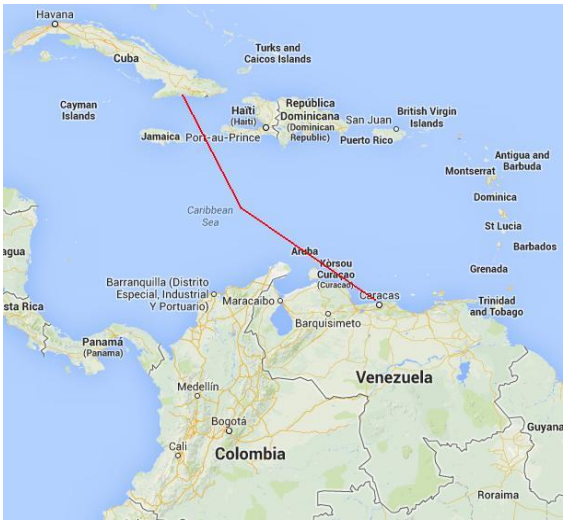
Par ailleurs, lorsque l'arrivée des câbles sous-marins ou l'installation de nouvelles infrastructures demeurent encore impossibles eu égard aux conditions géographiques, d'autres solutions sont expérimentées. A l'image du projet « Loon » (pour « balloon ») de Google qui permet d'établir des connexions au sol en provenance d'une trentaine de ballons flottant à une vingtaine de kilomètres d'altitude : des signaux sont envoyés vers les ballons qui les renvoient vers le sol en direction d'antennes disposées sur le sol[73].

Les débits proposés sont équivalents à de la 3G et chaque ballon permet une connexion sur 40 kilomètres autour de lui selon les responsables du projet[74]. Actuellement expérimentés en Nouvelle-

[73] http://www.liberation.fr/economie/2013/06/15/google-experimente-l-acces-au-net-via-des-ballons_911095
[74] http://www.lemondeinformatique.fr/actualites/lire-google-loon-des-ballons-internet-pour-desenclaver-les-regions-isolees-54001.html

Zélande, le but est de fournir à terme une connexion internet à des pays comme l'Afrique du sud, l'Uruguay, l'Australie ou le Chili. Le projet reste toutefois critiqué, car vu comme une manifestation supplémentaire de la domination et de l'omniprésence numérique de Google.

1.2.2.2 Le cas de Cuba, récemment désenclavé



Câble sous-marin Alba-1 - Source : Google maps

Jusqu'à lors enclavé par l'embargo américain depuis le 7 février 1962, l'accès à Internet pour les Cubains était réservé aux classes supérieures ou aux touristes résidants dans de grands hôtels et se faisait par l'intermédiaire d'une connexion satellite[75].

Le ministère cubain des Communications a toujours soutenu que seules des raisons « technologiques et financières » justifiaient ces restrictions. Mais, en réalité, les autorités cubaines opéraient ces restrictions par crainte de manœuvres de déstabilisation du pouvoir pouvant être orchestrées entre autres par les Etats-Unis via les réseaux sociaux[76]. Cette interprétation a été confirmée par une vidéo mise en ligne montrant un expert en informatique cubain exposer les dangers du cyberespace et des blogueurs indépendants à un parterre de responsables du ministère de l'Intérieur[77].

En 2011, la société Alcatel-Lucent a procédé à la pose d'un câble sous-marin nommé Alba-1. Ce câble reliant Cuba à Internet depuis le Venezuela n'avait jusque-là pas été mis en service. Le 14 janvier

[75] http://www.renesys.com/blog/2013/01/cuban-fiber-completo.shtml
[76] http://www.rfi.fr/ameriques/20130605-cuba-web-salle-navigation-censure
[77] http://www.courrierinternational.com/article/2011/12/21/les-fruits-defendus-d-internet

2013, un changement dans la structure du trafic Internet cubain a conduit les analystes de la société Renesys à penser que le câble Alba-1 aurait été mis en service[78].

Depuis la mise en service supposée de ce câble sous-marin, le Gouvernement cubain a annoncé la possibilité d'obtenir une connexion Internet à domicile à partir de 2014 par l'intermédiaire l'opérateur étatique ETECSA (Empresa de Telecomunicaciones de Cuba S.A) [79] qui détient le monopole de la fourniture des services de télécommunication sur l'île.

Dans la même logique d'ouverture sur le monde, le régime cubain a autorisé l'ouverture de 118 salles Internet[80] (à distinguer des cybercafés qui restent sous le contrôle des autorités). Depuis, plus de 100 000 Cubains y ont souscrit un abonnement. Malgré tout, l'accès à Internet demeure à un prix relativement élevé puisque le coût de la connexion est de 4,5 dollars de l'heure, de 1,5 dollar pour le courrier électronique et de 0,60 dollar pour la navigation sur l'intranet national[81], alors que le salaire mensuel avoisine les 20 dollars[82]. Parallèlement, les autorités cubaines ont lancé un équivalent de « Facebook » national, très verrouillé.

En 2012, plus de 2,5 millions des habitants de l'île ont bénéficié un accès à Internet sur une population atteignant 11 millions d'individus, soit un taux de pénétration de 23,2%[83]. L'Office national des statistiques (ONE) a en outre indiqué qu'à la fin de l'année 2012, 834 000 ordinateurs avaient été comptabilisés sur l'île, dont 500 000 connectés à Internet[84].

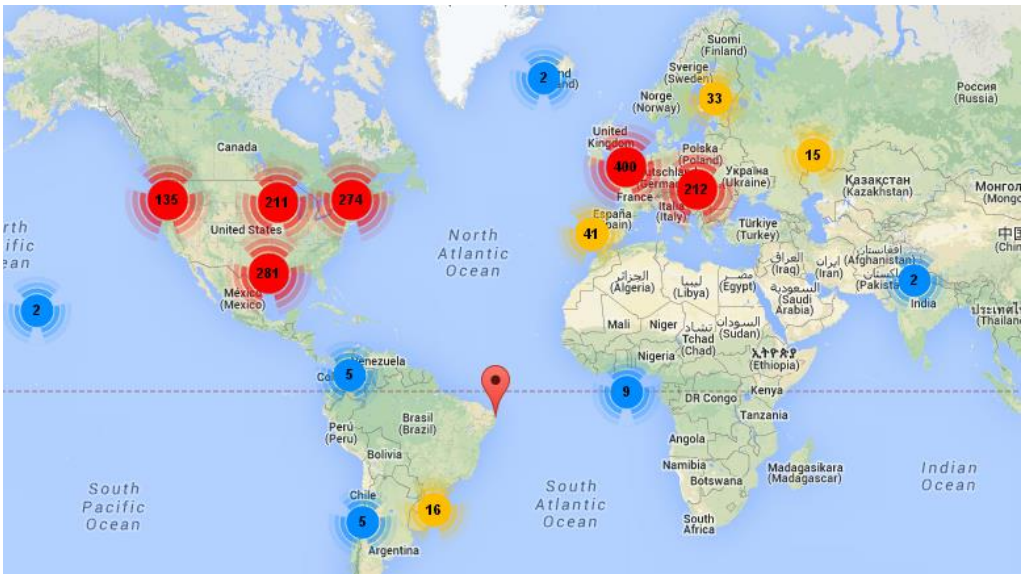
1.2.2.3 Cartographie : où se situent les data centers ?

Sur les infrastructures également, les pays émergents témoignent d'un retard important sur le cloud computing et l'hébergement des données : l'association Business Software Alliance (BSA), qui regroupe les principaux éditeurs de logiciels mondiaux, affirme dans son rapport 2013 intitulé « BSA Global Cloud Computing Scorecard » que les pays des BRICS ont une politique publique à la traîne en matière cloud tout en étant très demandeurs[85].

C'est ainsi que la plupart des data centers sont situés sur le continent américain et en Europe. Et les pays émergents souffrent d'une réelle faiblesse en la matière : quand les Etats-Unis (890), le Royaume-Uni (138), l'Allemagne (116) ou la France (101) en accueillent des centaines, la Russie n'héberge que 23 data center sur son territoire, suivie par le Brésil (10), l'Argentine (6) et l'Inde (2).

---

[78] http://tech.slashdot.org/story/13/01/21/0432210/cuba-turns-on-submarine-internet-cable?utm_source=rss1.0mainlinkanon&utm_medium=feed
[79] http://www.renesys.com/2013/08/cuban-internet/
[80] http://www.rfi.fr/ameriques/20130605-cuba-web-salle-navigation-censure
[81] http://abonnes.lemonde.fr/ameriques/article/2013/08/29/en-deux-mois-100-000-cubains-s-abonnent-a-internet_3468679_3222.html
[82] http://www.lefigaro.fr/flash-actu/2012/06/04/97001-20120604FILWWW00738-le-salaire-moyen-a-19-dollars-a-cuba.php
[83] http://www.internetworldstats.com/stats2.htm
[84]
[85] http://www.lemagit.fr/actualites/2240200130/Pour-la-BSA-les-BRIC-sont-en-retard-sur-le-Cloud-Computing



Répartition mondiale des data centers - Source : MapLink

Partie 2 : Cyberdéfense et lutte contre la cybercriminalité : des menaces de plus en plus présentes

Sous-partie 1 : La cybercriminalité et le hacktivisme

Phénomène mondial, il est courant de rappeler que la cybercriminalité se joue des frontières. Mais force est de constater que certaines frontières attirent plus que d'autres les cybercriminels, et ce pour plusieurs raisons. D'une part parce que certains Etats constituent, du fait de leur mauvaise gestion et prévention des risques, des cibles idéales. D'autre part, parce que d'autres constituent, du fait de leur laxisme ou tolérance, des paradis numériques relativement accueillants pour les cybercriminels. Les Etats émergents se sont saisi de cette problématique menaçant leur économie et affirment désormais leur volonté ferme d'enrayer la cybercriminalité.

1.1 Des cibles privilégiées car vulnérables

Comme tous les pays, les pays émergents sont vulnérables aux cyberattaques. Mais la jeunesse de leurs infrastructures IT fait d'eux des cibles privilégiées.

Source : Norton

D'après une étude de PandaLabs menée d'avril à juin 2012, si la Corée du Sud compte 57,3% d'ordinateurs infectés, suivent très rapidement la Chine à 52%, et Taïwan à 42%. La Bolivie, le Honduras, la Turquie, l'Équateur, la Russie, la Slovaquie, et la Pologne se trouvent également parmi les pays les plus infectés, tandis les pays les mieux protégés sont la Suisse (18,4%), la Suède (19%), la Norvège, le Royaume-Uni, l'Uruguay, l'Allemagne, l'Irelande, la Finlande, la Hongrie, et les Pays-Bas.

Selon le directeur technique de PandaLabs Luis Corron, cette nette tendance à l'infection par des troyens témoignerait des motifs économiques de la génération de programmes malveillants[86].

1.2 Des pays « accueillants » pour les activités cybercriminelles et hacktivistes

Les pays émergents sont confrontés au fléau grandissant de la cybercriminalité, tant comme cible que territoire « accueillant » pour ces cybercriminels. Véritables paradis numériques pour certains (en raison d'un manque de législation efficiente, ou de forces de l'ordre formées, voire d'une véritable politique pénale de lutte et de prévention), ces Etats sont aujourd'hui dans une dynamique de prise de conscience. Nombreuses sont désormais les initiatives ayant pour objectif de reprendre la main, et d'enfin pouvoir imposer un certain ordre public sur Internet.

[86] http://threatpost.com/en_us/blogs/south-korea-leads-nations-pc-infections-according-pandalabs-q2-report-080712

1.2.1 Les pays émergents : de véritables paradis numériques ?

Certains Etats peuvent, en raison de leur niveau de développement faible en matière de technologies de l'information et de la communication et, par conséquent, du faible développement de leur législation à ce sujet, être perçus de fait comme des Paradis numériques. C'est ce qu'a rappelé Hamadoun Touré, secrétaire général de l'UIT, dans un article d'Africa News en 2007[87]. Les pays émergents sont-ils pour autant des « paradis numériques » ?

1.2.1.1 La notion de Paradis numérique

Face au phénomène de la cybercriminalité, les acteurs publics se sont mobilisés en adoptant un corpus législatif permettant de sanctionner les actes de cybercriminalité. Mais la seule présence d'un corpus législatif national s'est révélée insuffisante, face à une criminalité transverse, se jouant des frontières. La coopération internationale s'est alors imposée comme un axe majeur de la lutte contre la cybercriminalité. Mais cette thèse est largement battue en brèche en raison de l'absence de coopération – délibérée ou non – de certains acteurs ; de l'absence de législation efficace ; d'une volontaire opacité sur les activités hébergées par certains acteurs. Qualifiées de « cyberparadis », de « paradis numériques » ou, en anglais, de « data heaven », ces entités – rattachées à une réalité physique ou virtuelle, sont de véritables assises du cybercrime international et constituent à ce titre des freins importants dans la lutte contre la cybercriminalité. En fournissant ainsi structures, hébergements et législation laxiste, ils assurent par exemple de ne donner suite à aucune demande de coopération internationale, et, à l'image des paradis fiscaux, favorisent ainsi la prolifération d'actes cybercriminels à l'abri de toute poursuite, réduisant ainsi fortement les effets des efforts de la communauté internationale.

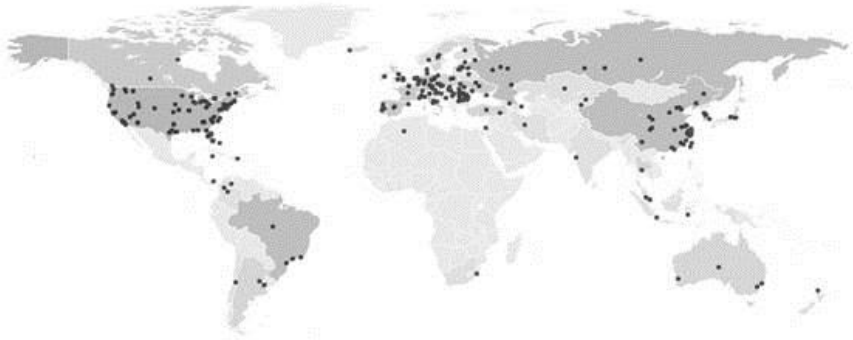
Certains ouvrages dédiés à l'informatique, comme « Sécurité informatique et réseaux – 3ème édition » de Solange Ghernaouti-Hélie, en donnent une définition. Selon l'auteure, les paradis numériques sont des lieux où « un malfaiteur peut agir ou héberger des serveurs et des contenus illicites en toute impunité ». Cette définition, bien que restreinte aux Paradis Numériques localisés géographiquement (certains évoquant des paradis numériques virtuels), reste relativement pertinente. Certains appréhendent les Paradis Numériques comme favorisant le développement de la cybercriminalité à grande échelle : pédopornographie, jeu illégal, fraude à la carte bancaire, hébergement de botnets permettant de lancer des attaques par déni de service, hébergement de malwares, etc.

Les éléments ci-dessous viennent cependant tempérer l'affirmation selon laquelle les pays émergents seraient responsables de la majorité des cyberattaques.

Tout d'abord, les hébergeurs « bulletproof » ou peu conciliant avec les autorités judiciaires sont principalement localisés dans des pays très développés au niveau de leurs infrastructures Internet.

---

87 http://books.google.fr/books?id=dIixW8q1J58C&pg=PA165&lpg=PA165&dq=%22safe+haven%22+cybercriminal&source=bl&ots=7hcyGR4WRr&sig=FQ-OVCtPPuCZZI__LkN-SFreNfo&hl=fr#v=onepage&q=%22safe%20haven%22%20cybercriminal&f=false



Localisation des serveurs malveillants identifiés par Malware Domain List sur avril 2011

Il est également intéressant d'analyser les sources géographiques des attaques recensées.

Rank			Source	Percentage		
2010 EMEA	2009 EMEA	2010 Global		2010 EMEA	2009 EMEA	2010 Global
1	1	1	United States	36%	36%	22%
2	2	4	United Kingdom	11%	14%	6%
3	4	2	China	9%	5%	13%
4	26	16	Turkey	6%	< 1%	2%
5	13	20	Sweden	5%	1%	1%
6	7	3	Germany	3%	3%	6%
7	8	8	Russia	3%	2%	3%
8	10	2	Canada	2%	2%	2%
9	3	5	France	2%	6%	3%
10	6	21	Netherlands	2%	3%	1%

Principales attaques par pays dans la zone EMEA, 2009-2010 - Source : Symantec

L'exemple du continent africain

Les Etats africains ne constituent pas des paradis numériques. En effet, on assiste à un véritable mouvement afin de mieux sanctionner les actes de cybercriminalité. Mais quelques exemples de laxisme peuvent être cités : les infractions punissant les intrusions au sein de banques de données ainsi que la législation sur la protection des données personnelles ne seraient pas appliquées au Maroc. On assisterait alors à une prolifération des actes cybercriminels dans ce pays[88]. De plus, de nombreuses raisons d'ordre géopolitique, sociologique ou historique ont parfois un impact négatif sur la mise en place d'un corpus législatif et de mesures de lutte contre la cybercriminalité. Certains Etats africains seraient en effet réticents à adopter des règles, principes, programmes, conventions européens, ou américains. Certains parlent de « colonisation » cybernétique qui serait imposée par les Etats occidentaux[89]. S'en suit alors un véritable morcellement des initiatives, évoquant une « régionalisation » du cyberespace.

[88] http://www.actuel.ma/Societe/Le_Maroc_cyberparadis_des_hackers/172.html
[89] http://www.e-juristes.org/reflexion-sur-les-accords-internationaux-actuels-en-matiere-de-cybercriminalite/

1.2.1.2 Quelques chiffres

Les experts de SophosLabs[90] ont publié un classement des pays ayant relayé le plus de spams entre janvier et mars 2012. Pour la première fois, l'Inde passe devant les États-Unis, avec 9,3% du total des spams relayés par son territoire, contre 8,3% pour les États-Unis. Suivent la Corée du Sud, l'Indonésie, la Russie, l'Italie, le Brésil, la Pologne, le Pakistan, le Vietnam, Taïwan et le Pérou. Le nombre de pays émergents présents en tête de liste vient confirmer l'importance de ces Etats dans le relai et l'hébergement de la cybercriminalité. Tendance confirmée par une étude de l'éditeur antivirus MacAfee décrivant le Cameroun comme détenant les sites webs les plus dangereux au monde d'un point de vue cybercriminel. Le pays a d'ailleurs réagit très vite, en annonçant se doter d'une infrastructure à clé publique. Celle-ci permettra d'identifier les utilisateurs de manière vérifiée et de sécuriser le commerce en ligne. La Corée du Sud participe à 50% à la mise en place du projet[91].

Autre exemple, celui du Bénin où les cybercriminels multiplient les cyberattaques, raison pour laquelle en décembre le gouvernement a lancé un vaste plan de lutte. La plupart des infractions sont commises depuis des cybercafés, mais peu de données d'analyse sont aujourd'hui disponibles, malgré la création d'une cellule de lutte contre la cybercriminalité en 2009. Seules 421 plaintes ont été enregistrées entre 2011 et 2012 pour 53 personnes déférées. L'absence de cadre juridique est ici un problème récurrent. Un autre réside dans la difficulté à identifier les cybercriminels, malgré la publication, par une agence américaine, d'une liste de 200 présumés cybercriminels béninois[92].

Toujours sur le continent africain, la croissance financière de la Tanzanie au cours de ces dernières années a entraîné une hausse des activités cybercriminelles. Le rapport statistique de la Bank of Tanzania révèle que plus de 615 198 $ ont été volés au cours de ces dernières années[93].

1.2.2 Les cyber-conflits : nouvelles manifestations des conflits géopolitiques au sein des pays émergents

Le hacktivisme, exploitant les mêmes outils que les cybercriminels, mais à des fins de contestation politique et sociale, est très présent dans les pays émergents. Outil de pression facile d'accès et bénéficiant d'un écho maximal via Internet, la cyberattaque de type « défacement » ou piratage de site Internet est une manifestation récurrente du hacktivisme. Et désormais, la plupart des conflits géopolitiques dispose d'un volet « cyber ». Affirmation qui touche aussi bien les grandes puissances « cyber » que les pays émergents.

Exemple récent : plusieurs sites du gouvernement du Venezuela ont été la cible d'une cyber-attaque massive lancée par la branche vénézuélienne du groupe Anonymous. Les pirates souhaitent exprimer

---

[90] http://nakedsecurity.sophos.com/2012/04/23/india-becomes-the-king-of-the-spammers-stealing-americas-crown/?utm_source=feedburner
[91] http://www.africareview.com/Business+++Finance/Cameroon+tightens+Internet+trade+/-/979184/1607988/-/4me2x2z/-/index.html
[92] http://herboko.blog.lemonde.fr/2013/01/07/au-benin-la-lutte-contre-la-cybercriminalite-reste-encore-fragile/
[93] http://www.techmissus.com/securite-2/tanzanie-la-cybercriminalite-se-developpe-plus-de-615-000-dollars-voles/

leur rejet des résultats des élections présidentielles du 14 avril et leur demande de démission du Président Nicolas Maduro. Les sites des ministères, des collectivités locales et universités sont ainsi restés indisponibles durant plusieurs heures[94].

1.3 La volonté affirmée d'enrayer la cybercriminalité

Les initiatives de lutte contre la cybercriminalité sont aujourd'hui nombreuses. Des initiatives qui s'inscrivent souvent dans le cadre d'accords de coopération, soit avec de grandes puissances « cyber », soit avec d'autres Etats de la région proche. Plusieurs axes de renforcement de la lutte sont envisagés : les alliances politiques, le renforcement des unités judiciaires, de la législation, et l'amélioration des défenses d'un point de vue plus technique cette fois.

1.3.1 L'exemple Brésilien

Les révélations de l'affaire Snowden ont d'ailleurs permis un véritable renouveau de ces accords de coopération. Les ministères de la Défense d'Argentine et du Brésil ont par exemple noué une alliance pour améliorer mutuellement leurs capacités de cyberdéfense, suite aux révélations sur les activités d'espionnage des Etats-Unis en direction des pays d'Amérique latine. Un sommet bilatéral de cybersécurité sera d'ailleurs tenu avant la fin de l'année 2013, et le Brésil formera en 2014 des officiers argentins à la cyberdéfense[95]. Les 30 et 31 octobre 2012, Brasilia accueillait déjà le premier forum brésilien concernant les problématiques de cybersécurité et de cyberdéfense[96]. Toujours au Brésil, deux lois ont été votées par les chambres législatives : "PL Azeredo" et "Lei Dieckmann". La première permet la création d'unités spéciales de lutte contre le cybercrime. La deuxième punit l'intrusion, le vol d'informations et la dissémination de malwares. Un troisième projet de loi en cours de discussion examine les responsabilités et droits des utilisateurs et fournisseurs d'accès[97].

1.3.2 Le dynamisme du continent africain

Le continent africain tente enfin de reprendre la main sur sa cybersécurité. Longtemps connu pour des fraudes typiques (arnaque dite « nigériane » ou « fraude 419 par exemple), le continent est aujourd'hui l'un des plus actifs, voire hyperactif, en matière d'initiatives de lutte contre la cybercriminalité.

L'Afrique accueille aujourd'hui divers évènements, témoignant du dynamisme et des ambitions de la région, notamment quant à son positionnement au sein de la gouvernance Internet. A titre

[94] http://www.mag-securs.com/News/tabid/62/id/33150/Venezuela-cyber-attaque-massive-contre-le-gouvernement.aspx
[95] http://rt.com/news/brazil-argentina-cyber-defense-879/
[96] Plus d'informations sont disponibles sur le site officiel de l'évènement : http://www.cyberdefensebrazil.com
[97] Enfin, une réforme du droit du copyright est à l'étude. http://www.linhadefensiva.com/2012/11/after-13-years-brazil-approves-two-cybercrime-laws-at-once/

d'exemple, le président du Burkina Faso, Blaise Compaoré, a présidé la réunion à Dubaï du Conseil Consultatif International du Partenariat multilatéral contre les cyber menaces (IMPACT). Le gouvernement burkinabè travaille en effet avec l'UIT pour assurer le bon développement des réseaux informatiques du pays[98]. A Nairobi, plus de 300 représentants venus du monde entier étaient présents les 6 et 7 septembre pour le second sommet mondial sur la liberté sur Internet. Celui-ci s'est tenu pour la première fois sur le continent africain, symbolisant ainsi le rôle croissant des TIC en Afrique[99].

Plusieurs Etats du continent proposent de renforcer leur législation, et de former leurs unités. A l'image des services de police ghanéens qui souhaitent sensibiliser leurs agents à la cybercriminalité, et les former à la lutte contre les cybercriminels. Pour ce faire, 43 policiers de tout le pays ont été choisis pour suivre une formation visant à améliorer les capacités de lutte contre la cybercriminalité du Ghana. Cette démarche a été initiée en raison d'un très faible taux d'élucidation des plaintes déposées pour des cybercrimes[100]. Au Burkina Faso encore, deux projets de lois visent à modifier le code pénal pour prendre en compte les nouvelles problématiques de lutte contre la cybercriminalité[101]. Aussi, la commission des Affaires Economiques et Financières de l'Assemblée Nationale ivoirienne a adopté le 13 Juin 2013 le Projet de loi relatif aux transactions électroniques. Cette loi, qui vise à donner un cadre juridique à la lutte contre la cybercriminalité, prévoit notamment de lutter contre le phénomène des « brouteurs », ces cyberescrocs qui forcent des individus à se dénuder devant leur webcam pour ensuite les faire chanter[102]. Depuis 2008, le **Sénégal** s'est également engagé sur la voie de la lutte contre la cybercriminalité[103].

Ces initiatives s'accompagnent de la volonté de renforcer la cybersécurité, en assurant une meilleure maîtrise des menaces. C'est le cas du Burkina Faso, exemplaire, qui ouvre une Computer Incident Response Team (CIRT) à Ouagadougou. Ce centre dédié à la lutte contre la cybercriminalité a été présenté par le ministère de l'économie numérique. Objectif : lutter contre la cybercriminalité en constante hausse au Burkina Faso mais également dans toute l'Afrique de l'Ouest[104].

Nombreux enfin, sont les Etats africains à envisager une meilleure prévention et formation des citoyens. Des initiatives visant à assurer une prise de conscience. Le Kenya s'est doté d'une stratégie de cybersécurité et d'un plan directeur, qui s'inscrivent dans le plan directeur des Technologies de l'Information et des Communications qui sera lancé le 14 février. Le gouvernement kenyan souhaite élaborer un guide de procédures à destination des administrations et des entreprises en cas de

---

[98] http://news.aouaga.com/h/1594.html
[99] http://www.freedomonlinekenya.org/related-news/kenyatohost1stafricanconferenceoninternetfreedom

[100] http://www.spyghana.com/cyber-crime-training-for-43-detectives/
[101] http://news.aouaga.com/h/1594.html
[102] http://www.koaci.com/articles-83058
[103] Voir textes de loi : **loi n° 2008-11 du 25 janvier 2008 sur la cybercriminalité** (loi n° 2008-11 du 25 janvier 2008 sur la cybercriminalité) et jurisprudence : http://www.pressafrik.com/La-lutte-contre-la-cybercriminalite-les-premieres-decisions-de-la-justice-senegalaise_a40664.html
[104] Le CIRT ne se limitera pas à un travail d'enquête et de résolution d'incidents, mais disposera également d'un volet informatif pour sensibiliser les burkinabés aux enjeux de cybersécurité. http://www.legriot.info/8713-lutte-contre-la-cybercriminalite-au-burkina/

cyberattaques. Cette stratégie a été développée afin d'anticiper l'augmentation des cybermenaces inhérente à l'amélioration des capacités des infrastructures numériques kenyanes[105]. Le gouvernement du Rwanda a quant à lui lancé une campagne de sensibilisation des populations. Près de 6,7 millions € ont été alloués pour cette opération de sensibilisation pour l'année 2013/2014[106].

En Tanzanie cette fois, la Banque principale travaillerait avec le gouvernement à la préparation d'une nouvelle loi pour créer un cadre légal pour les transactions financières électroniques et pour pouvoir lutter contre la cybercriminalité[107].

1.3.3 La coopération régionale : vers un morcellement des initiatives de lutte contre la cybercriminalité[108]

La tendance est, à première vue, au morcellement des initiatives. Se dresse ainsi une liste conséquente de démarches informelles ou d'accords signés, strictement bilatéraux, régionaux ou internationaux.

La Convention de Budapest est aujourd'hui un modèle pour l'adoption de législations locales. Une Convention, signée le 21 décembre 2010 au Caire dans le cadre du sommet de l'Union africaine[109], vise à renforcer la coopération entre les pays arabes en matière de lutte contre la cybercriminalité[110]. En matière de cybercriminalité, elle règlemente la conservation des données à caractère personnel. Elle contraint également les Etats signataires à adopter des dispositions de droit interne pénalisant des actes de cyberdélinquance. La Convention enjoint également aux parties de renforcer leurs infrastructures nationales afin de sécuriser la circulation des informations. De plus, les membres de la Convention devront permettre à des autorités spécialisées de procéder à des expertises visant à retrouver les auteurs des infractions. L'accord précise également que la remise des auteurs sera effectuée conformément à la législation du territoire dont il relève.

Les Etats membres de l'EAC (East African Community ou Communauté d'Afrique de l'Est) ont lancé[111], lors d'une conférence tenue entre le 25 et le 27 juillet 2011 à Nairobi, au Kenya, les bases d'une structure transnationale de cyberprotection. Les Etats membres avaient déjà, en mai 2010, projeté une harmonisation normative, notamment dans le domaine de la cybercriminalité, en accord avec les principes de la Convention de Budapest. Les articles 98 et 99 du traité[112] pour

---

[105] http://www.agenceecofin.com/securite/1302-8937-le-kenya-lance-sa-strategie-nationale-de-cyber-securite
[106] http://www.agenceecofin.com/securite/0107-12085-rwanda-le-gouvernement-a-demarre-la-sensibilisation-sur-la-cybercriminalite
[107] http://allafrica.com/stories/201309110118.html
[108] Issu de la note trimestrielle de septembre 2011, de l'Observatoire de la Guerre Informatique.
[109] http://www.africa-union.org/root/ua/index/index.htm
[110] http://www.echoroukonline.com/fra/actualite/7557-lutte-contre-le-blanchiment-d-argent-terrorisme-corruption-et-cybercriminalite-les-pays-arabes-unifient-leurs-efforts.html
[111] http://allafrica.com/stories/201108040622.html
Et site officiel de l'EAC ; recherche avec les mots clé « cyber crime ».
[112] https://docs.google.com/viewer?a=v&q=cache:wPmDIjUMoIEJ:www.malango-actualite.fr/documents/1976.pdf+Communaut%C3%A9+d'Afrique+de+l'Est+trait%C3%A9&hl=fr&gl=fr&pid=bl&srcid=ADGEESgJ5pkxLCGo9DT4Ow2smlwqFUidJ8mkFLWNOPE8c-O0QIzj7NblmFLIw7MpvlWDmGejLCKVkwi9oYUiW1i1NU-AfY27Nw4D4-gsP3pNcjK-m-hdIIlzCO21eFYVcgdeXDdjR2UP&sig=AHIEtbQmsNpjCQK04SnBWuJ2MYbR33OSyg&pli=1

l'établissement de la Communauté d'Afrique de l'Est incitent les Etats partenaires à coopérer en matière de développement d'infrastructures et services de haute technologies, dans tous les domaines des technologies de l'information et de la communication, et à créer un organe supranational spécialisé dans la lutte contre la cybercriminalité.

Les Etats asiatiques opèrent quant à eux au sein d'organisations régionales comme l'ASEAN, l'Organisation de Coopération de Shanghai ou encore l'Association des nations de l'Asie du Sud-Est (ANASE). La proposition la plus marquante, issue de l'OCS, est le code de bonne conduite sur la sécurité de l'information (2011), à mi-chemin entre la cybercriminalité et la cyberdéfense.

Sous-partie 2 : La cyberdéfense et les pays émergents

Le cyberespace, par sa nature, bouleverse les rapports du fort au faible et redistribue les cartes. Les pays émergents l'ont bien compris et, malgré une apparence d'ambitions disparates, nombreux sont ceux à envisager le cyberespace comme un investissement stratégique. Des ambitions qui doivent être mises en perspective avec la volonté de ces Etats de peser toujours plus dans la gouvernance d'Internet, aujourd'hui monopolisée par certains acteurs.

1.1 La cybersécurité : un investissement stratégique pour les pays émergents

Internet souvent considéré comme un « facteur égalisateur »[113] au sein de conflits. C'est en effet un terrain d'affrontement favorable au développement, avec de faibles moyens, de capacités de lutte importantes[114]. Le développement de cyberarmes est loin d'être l'apanage des seules puissances cyber. Comme le précise le blog cyber-defense.fr, « la découverte isolée d'exploits par n'importe quel amateur éclairé ne peut être empêchée »[115]. Les blackmarkets (ou marchés noirs) sont accessibles à tous, et les exploits et autres outils offensifs sont en libre accès. Le déséquilibre de moyens ne semble donc plus être si évident dans le cyberespace. Même si, face à un attaquant aux faibles moyens, le fort a toujours les capacités d'élever son niveau de défense. Si bien que certains observateurs jugent inutile la distinction entre conflit symétrique, asymétrique et dissymétrique[116].

[113] http://www.egeablog.net/dotclear/index.php?post/2012/06/13/Resym%C3%A9trisation-du-cyber
[114] « Nouvelles guerres de l'information, le cas de la Syrie », CEIS.
[115] http://cyber-defense.fr/blog/index.php?post/2013/04/09/Le-march%C3%A9-des-cyber-armes%3A-un-march%C3%A9-gris
[116] Etienne Durand (IFRI), mentionné par http://mars-attaque.blogspot.fr/2011_12_04_archive.html

La cybersécurité constitue donc un investissement stratégique, l'occasion pour de nombreux Etats de se positionner sur un sujet encore « jeune », favorable à l'émergence de nouveaux acteurs clés et de nouveaux rapports de force.

1.2 Des initiatives et des ambitions disparates

Les pays émergents ne présentent pas de ligne commune de cyberdéfense. Tantôt alignés sur une grande puissance telle que les Etats-Unis, tantôt appuyés sur une coopération à l'échelle régionale, ils font preuve d'ambitions disparates.

Il semble toutefois que les dernières révélations concernant le programme américain d'espionnage à grande échelle, aient précipité et renforcé une coopération régionale encore plus importante (entre le Brésil et l'Argentine, par exemple), et bouleversé les relations pourtant jusque-là bien entretenues par les Etats-Unis avec de nombreux pays émergents ou BRICS.

1.2.1 Le géant Chinois[117]

Le pays affirme une volonté très forte d'autonomie en matière d'infrastructure et de contrôle de son Internet. Cette volonté de l'Etat chinois s'illustre notamment en positionnant de grandes entreprises de hautes technologies (comme Huawei) et menant une forte politique de normalisation. Surtout, les chinois ont cherché leur réhabilitation aux yeux de la scène internationale en réfutant les accusations de cyberattaques, ainsi que celles portées à l'encontre de leurs multinationales Huawei et ZTE. Malgré le fort contrôle exercé sur les contenus sur Internet, la cybercriminalité explose en Chine. En parallèle de ce phénomène, à l'instar de la Russie, la Chine dispose d'un écosystème d'hacker patriotique très important et très actif. En matière de cyberdéfense, la Chine semble très avancée. L'armée chinoise dispose notamment d'unités spécialisées dans la lutte informatique offensive et n'hésiterait pas en faire l'usage selon des rapports américains.

1.2.2 L'Amérique Latine et les Caraïbes ambitieuses[118]

Comme indiqué dans la lettre mensuelle de l'OMC du mois de juillet, les pays d'Amérique latine et des Caraïbes ont des approches variées, mais cohérentes de la lutte contre la cybercriminalité. Tandis que certains avancent des raisons de sécurité et de défense nationale, d'autres justifient leur démarche de cybersécurité par la crainte des risques pour le développement et économique et la compétitivité des Etats. Deux approches différentes mais complémentaires. Beaucoup de pays ont adopté un cadre législatif portant sur la cybercriminalité, créant ainsi des procédures spécifiques qui n'existaient pas jusque-là. De même, la plupart des pays membres ont entamé la création d'un CERT

[117] https://omc.ceis.eu/_layouts/OwlOmc/Dashboard.aspx?c=46#mapanchor
[118] Lettre n°19 – Juillet 2013, Observatoire du Monde Cybernétique, DAS.

national. De récentes révélations sur les vulnérabilités d'infrastructures critiques ont en effet poussé les Etats à prendre de nouvelles initiatives, à l'image du Panama qui a développé une stratégie de protection des infrastructures critiques.

Les Etats membres de l'OAS font preuve d'une mise en commun des efforts dans la lutte contre la cybercriminalité : alors que l'Union européenne vient d'adopter une stratégie en la matière, l'OAS s'est dotée dès 2004 d'une stratégie interaméricaine unifiée en matière de cybersécurité. Cette dernière a été complétée par une déclaration en mars 2012 portant sur le renforcement de la cybersécurité en Amérique. En outre, d'un point de vue opérationnel, le Secrétariat général de l'OAS fournit aux Etats membres une assistance technique et participe à l'amélioration du niveau de cybersécurité des Etats de l'OAS. Des accords bilatéraux concernant la cyberdéfense existent, à l'exemple du Brésil[119] ou du Chili[120] qui ont renforcé leur coopération militaire avec les Etats-Unis en avril 2012. La collaboration entre les pays de l'OAS a également permis à un groupe de pays (Brésil, Argentine, Chili, Pérou et Uruguay) d'empêcher le géant du web Amazon à obtenir le nom de domaine ".amazon" auprès de l'ICANN au motif que le terme « amazon » représente un large territoire qui s'étend sur plusieurs pays[121].

1.2.3 Au cœur de l'Amérique latine, la puissance montante brésilienne

Le Brésil a pour ambition de devenir une puissance influente sur la scène internationale en matière de cyberdéfense. Le pays espère en effet profiter de « l'effet » Coupe du Monde de 2014 et des jeux Olympiques de 2016 afin de devenir, d'ici 2022, le 3ème marché des TIC au monde. Une dynamique suivie également par un renforcement de la législation brésilienne en matière de lutte contre la cybercriminalité. L'armée brésilienne a par exemple annoncé le développement d'un nouveau logiciel pour la sécurité et la prévention des cyberattaques. Cette démarche s'inscrit nettement dans la volonté du gouvernement brésilien de développer la cyberdéfense du pays en particulier concernant les informations sensibles. Le général Antonio Santos, directeur du centre de communication des forces armées et de la guerre électronique (Ccomgex) estime en ce sens que le Brésil n'est que faiblement préparé à faire face à des cyberattaques[122]. Le Brésil soigne également sa coopération. Au cours d'une rencontre au sommet entre les ministres de la Défense brésilien et américain, la cybersécurité a pris une place importante dans les échanges. Leon Panetta a, à l'époque, estimé que la collaboration dans ce domaine serait profitable pour les deux nations. Cependant, aucune mesure concrète de partenariat n'avait été développée[123]. Les récentes affirmations selon lesquelles le Brésil a été une des cibles privilégiées du programme américain PRISM ont cependant remis en cause ces perspectives de coopération.

[119] http://www.defense.gov//news/newsarticle.aspx?id=116075
[120] http://www.defense.gov//news/newsarticle.aspx?id=116102
[121] http://bits.blogs.nytimes.com/2013/07/18/amazon-rejected-as-domain-name-after-south-american-objections/?ref=technology
[122] http://cyberwarzone.com/cyberwarfare/brazil-prepares-cyber-war
[123] http://www.defense.gov//news/newsarticle.aspx?id=116075

Conclusion

Si le paragraphe sur la cyberdéfense des pays émergents semble court, c'est bien parce que ceux-ci semblent bien plus préoccupés par l'enrayement de la cybercriminalité, premier pas vers une cyberdéfense efficiente.

L'affaire PRISM et, plus globalement, les activités d'espionnage des Etats-Unis révélées au grand jour ont remis en cause la confiance régnant entre certains pays émergents et la puissance américaine, les encourageant à renforcer une coopération plus locale et régionale. Les pays dits « sous influence » américaine affichent donc une volonté de s'émanciper, et se tournent vers les puissances que constituent les BRICS.

Le développement des infrastructures IT est un enjeu crucial de développement économique pour ces pays. Le corolaire est l'apparition de menaces. Ces Etats l'ont compris et se saisissent de la problématique. Cette prise de conscience permet le développement d'un marché considérable, avec le développement d'offres à destination des BRICS et pays émergents.

L'affirmation des pays émergents dans le cyberespace passe aussi par leur influence au sein de la gouvernance Internet. L'issue mitigée de la Conférence mondiale des télécommunications internationales de Dubaï a cependant illustré la difficulté de concilier les intérêts de toutes les forces en présence.

Le fait qu'un groupe de pays sud-américains (Brésil, Argentine, Chili, Pérou et Uruguay) ait réussi à empêcher le géant américain du Web Amazon à obtenir le nom de domaine ".amazon" auprès de l'ICANN (au motif que le terme « amazon » représente un large territoire qui s'étend sur plusieurs pays), constitue en soi une victoire symbolique[124].

[124] http://bits.blogs.nytimes.com/2013/07/18/amazon-rejected-as-domain-name-after-south-american-objections/?ref=technology