Rapport annuel - 2016 - disponible sur omc.ceis.eu

Table des matières

1. ANALYSE REGIONALE

Cette analyse porte sur différentes régions choisies par le pilote de l'étude. Son objectif est de dresser un état des lieux à l'instant t de la région ou du groupement politique, de son niveau de maturité en matière cybernétique, de la coopération régionale et de ses relations avec les autres régions dans le domaine.

1.1 Les BRICS

Le terme BRIC (Brésil, Russie, Inde, Chine) apparaît pour la première fois en 2001 dans une note de Jim O'Neill, économiste de la banque d'investissement Goldman Sachs pour désigner des « pays en forte croissance » dont le PIB serait susceptible d'égaler en 2040 celui du G6 (les États-Unis, l'Allemagne, le Japon, la France, le Royaume-Uni et l'Italie). Mais ce n'est qu'en juillet 2009 que les quatre BRICS décidèrent de s'associer avec la volonté de réformer rapidement le système financier mondial et d'être plus influents ensemble[1], rejoints en 2010 par l'Afrique du Sud. Ce dernier élargissement est principalement politique, d'autres pays comme le Mexique, la Corée du Sud ou encore la Turquie s'étant vus refuser l'accès au groupe. « *Pour être crédible et représenter le Sud sur la scène mondiale, les BRICS avaient besoin d'un membre africain, et le choix de l'Afrique du Sud est très judicieux* », explique Catherine Grant de l'Institut sud-africain pour les affaires internationales (SAIIA)[2] . La décision est également motivée par des raisons économiques : la présence de l'Afrique du Sud permet un accès direct sur le continent africain, présenté comme le futur eldorado commercial de la planète. Selon l'agence Ecofin[3] , agence africaine d'informations basée à Genève, les échanges entre l'Afrique et les BRICS devraient ainsi atteindre 500 milliards de dollars en 2015. Avec 42,1% de la population mondiale, 26,7% de la surface terrestre, 21,8% du PIB mondial (soit 16.900 milliards de dollars)[4], les BRICS sont devenus en 2015 une réalité économique incontestable, encore renforcée par une progression rapide du numérique.
Comme le souligne une contribution russe lors du NetMundial[5], les BRICS représentent 30% des internautes mondiaux. Et la contribution de leurs économies au secteur numérique mondial, qui s'élevait à 500 milliards de dollars en 2013, devrait doubler en 2015. Soutenu par des initiatives gouvernementales, le marché des services et produits numériques au sein des BRICS devrait en effet progresser de 11,72% par an sur la période 2014-2019, estiment les analystes de la société de conseil Technavio.

1.1.1 Une relation de partenariat économique et politique à part entière

Les membres des BRICS ont rapidement mis en place différents accords et partenariats. Ainsi, lors du 6ème sommet BRICS, organisé à Fortaleza au Brésil en juillet 2014, les pays émergents officialisent la création d'une banque de développement basée à Shanghai, dotée de 50 milliards de dollars (*New Development Bank BRICS*), ainsi qu'un fonds d'urgence de réserves de 100 milliards. La Chine devrait y contribuer à hauteur de 41 milliards de dollars, le Brésil, l'Inde et la Russie pour 18 milliards, l'Afrique du Sud pour 5 milliards. L'ambition est claire : contourner le système économique mondial régi par le Fonds monétaire international (FMI) et la Banque Mondiale avec la possibilité d'effectuer des règlements en monnaies nationales. La Nouvelle banque de développement fondée par les membres des BRICS a ainsi officiellement ouverte fin juillet 2015. Selon le ministre russe des finances, Anton Silouanov, cette organisation servira notamment à financer des travaux d'infrastructure et des projets (publics ou privés) de développement durable dans les BRICS et les autres économies émergentes (comme l'Afrique par exemple)[6] . Autre priorité : le renforcement des échanges et investissements croisés entre les pays, avec la création d'un Conseil d'affaires des BRICS présidé par Sergueï

[1] http://www.courrierinternational.com/article/2009/06/18/bresilrussie-inde-chine-l-attaque-des-bric
[2] www.saiia.org.za
[3] http://www.agenceecofin.com/commerce/0209-22481-lesechanges-entre-l-afrique-et-les-brics-sont-projetes-a-500- milliards-de-dollars-en-2015
[4] http://www.worldbank.org/
[5] http://content.netmundial.br/contribution/pir-center-policyproposals-global-internet-governance-as-a-new-commonagenda-for-russia-brazil-and-brics-states/242
[6] http://fr.rbth.com/2015/07/08/la-banque-de-developpementdes-brics-entame-ses-activites_168213

Katyrine, président de la chambre de commerce et d'industrie de Russie. « *Il y a une volonté d'améliorer le climat d'affaires dans les cinq pays sur les questions relatives au régime des visas, les moyens de simplifier la circulation des entrepreneurs, des biens, des services et des finances, ainsi que le rapprochement des normes, des règlements techniques et des régimes d'autorisation* », explique ce dernier. Selon le document adopté le 9 Juillet 2015 et intitulé « La stratégie de partenariat économique des BRICS »[7], les pays membres « *doivent coopérer à travers des mécanismes d'échange et de présentation des informations, des politiques et stratégies dans les domaines des sciences, technologie et de l'innovation, y compris à travers des programmes de long terme destinés à résoudre des problèmes concrets.* » Une liste des axes de coopération prioritaire est également publiée dans ce document[8]. On y retrouve ainsi le calcul haute performance, les télécommunications, les nanotechnologies ou bien encore la coopération entre les différents pays des BRICS.

De même, le volontarisme numérique des BRICS transparait également dans la déclaration d'Iougorsk adoptée le 7 juillet 2015 à Khantys-Mansis en Russie à l'issue du 7ème Forum international des technologies de l'information[9]. Elaboré conjointement par les participants au Forum (2 060 personnes et 38 pays) et par les pays des BRICS et de l'OCS (Organisation de coopération de Shanghai, organisation intergouvernementale régionale asiatique qui regroupe la Chine, le Kazakhstan, le Kirghizistan, l'Ouzbékistan, la Russie et le Tadjikistan, et depuis 2016, le Pakistan et l'Inde), le document souligne tout d'abord la nécessité de mettre en œuvre un plan commun de développement en matière logicielle (serveurs et systèmes d'exploitation mobiles, systèmes de gestion des bases de données, applications bureautiques, logiciels industriels et d'ingénierie). Une volonté d'indépendance qui correspond en tout point aux orientations de la Chine et de la Russie qui ont toutes deux décidé de développer leur propre système d'exploitation (COS pour la Chine[10], et mobile pour la Russie[11]). Signe du rôle clé de la Russie, il a été évoqué lors de la rencontre la possibilité d'ouvrir des représentations permanentes des pays des BRICS et de l'OCS au sein des *Technoparc* et incubateurs informatiques présents en Russie[12]. La déclaration d'Iougorsk appelle également les autorités compétentes à trouver des solutions de substitution aux importations de technologies informatiques et à soutenir le développement d'infrastructures nationales pour que tout citoyen puisse accéder aux outils numériques modernes (de très larges portions du territoire russe sont par exemple non connectées). La déclaration plaide enfin pour l'harmonisation des législations des Etats membres des BRICS et de l'OCS en matière de liaisons électroniques et de gestion numérique des documents.

Au niveau politique, signe de l'émergence d'une stratégie russe coordonnée en direction de l'Eurasie - loin du G7 où la Russie a été exclue suite au conflit en Ukraine - le 7ème sommet des BRICS à Oufa, la capitale de la République de Bachkirie, membre de la Fédération de Russie, a réuni les BRICS, mais aussi l'Organisation de coopération de Shanghai (OCS) et les dirigeants de l'Union économique eurasienne (UEE). Internet et la cybersécurité y ont été au cœur des débats[13]. Un groupe de travail a ainsi été créé sur le développement de normes communes, les meilleures pratiques en cybersécurité et la lutte anti- cybercriminalité. Les BRICS ont en outre réitéré leur appel pour un traité sur la cybercriminalité dans le cadre de l'Organisation des Nations Unies et une « évolution de l'écosystème de la gouvernance de l'Internet, qui devrait être basé sur un processus ouvert et démocratique, libre de l'influence de toute considérations unilatérale. » *[« Evolution of the Internet governance ecosystem, which should be based on an open and democratic process, free from the influence of any unilateral considerations. »]*
Une position qui correspond là aussi en tous points au modèle revendiqué depuis de nombreuses années par certains pays, au premier rang desquels la Chine et la Russie, et qui se traduirait par une reprise en main étatique de la gouvernance de l'Internet, dont le contrôle serait transféré à l'Union internationale des télécommunications (UIT), une agence onusienne dépendant donc des gouvernements des Etats représentés. Dès décembre 2012 à Dubaï, lors du sommet de l'UIT, ces pays demandaient ainsi le transfert de la gestion des DNS sous l'autorité de l'UIT. Ce sujet a été de nouveau évoqué lors du NetMundial, le 23 et 24 avril 2014, conférence internationale sur la gouvernance de l'Internet, organisée par la présidente brésilienne Dilma Rousseff, à la suite de son discours[14] à l'ONU en septembre 2013 où elle accusait le gouvernement américain et l'ICANN (Internet Corporation for Assigned Names and Numbers) d'atteinte à la souveraineté nationale. L'événement a cependant révélé des divergences fortes au sein des BRICS à propos de la gouvernance

[7] http://en.brics2015.ru/load/381830
[8] http://static.kremlin.ru/media/events/files/ru/KT0SBHnlZjOpIuAj2AOXCnszNQA8u7HL.pdf
[9] http://www.itforum2015.admhmao.ru/wps/portal/itf2015/home/vse_novosti/news/280a5c99-8204-47c7-8523-3430985733f5
[10] http://www.lemonde.fr/technologies/article/2010/10/27/larussie-veut-creer-son-propre-systeme-dexploitation_1432068_651865.html
[11] http://www.nextinpact.com/news/94135-la-russie-veut-sonpropre-systeme-dexploitation-base-sur-sailfish.htm
[12] http://www.nakanune.ru/news/2015/7/7/22406594/
[13] http://www.brics.utoronto.ca/docs/150709-ufadeclaration_en.html
[14] http://www.les-crises.fr/discours-a-lonu-de-la-presidentedu-bresil-dilma-rousseff/

d'internet avec, d'un côté, la Chine et la Russie plaidant pour une gouvernance étatique et non commune d'Internet[15], et, de l'autre, le Brésil défendant une évolution de l'ICANN vers une gouvernance neutre, transparente et démocratique. A ces divergences sur la gouvernance Internet s'ajoutent également de fortes tensions politiques entre certains BRICS eux-mêmes. L'exemple le plus flagrant est celui de l'Inde et de la Chine. Ainsi, lorsque Beijing a organisé le « *2012 Internet Roundtable for Emerging Countries* »[16] qui a réuni la Chine, la Russie, l'Afrique du Sud et le Brésil, l'Inde n'était présente qu'en tant qu'observateur au travers d'un fonctionnaire de son ambassade. Les liens forts existant entre l'Inde et les Etats-Unis (notamment dans le domaine de la cybersécurité[17]) et, de façon plus globale, la stratégie américaine de « pivot vers l'Asie » qui vise à utiliser l'Inde pour contenir la Chine n'ont sans doute pas amélioré la situation. L'Inde, « plus grande démocratie du monde », peut enfin avoir quelques préventions à coopérer avec le « plus grand Etat autoritaire du monde ».

1.1.2 Les BRICS et le reste du monde

Depuis leur création, les BRICS ont évolué : au départ simple réalité économique, ils constituent aujourd'hui une force politique à part entière. Suite à son éviction du G7, on observe par exemple que la Russie, en y concentrant désormais ses forces, figurent parmi les grandes puissances du groupe.

Mais sur les sujets « cyber », les pays membres des BRICS ne sont pas tous d'accord entre eux. On a pu l'observer par exemple à propos de la neutralité du net, sujet où les différents membres ont des avis très divergents. De plus, certaines coopérations fortes entre les membres et d'autres pays pèsent dans la balance. Ainsi, l'Inde et les Etats-Unis, qui entretiennent une relation assez forte, arrivent pour l'instant à faire contrepoids sur certains sujets de cyberdéfense. N'arrivant pas à parler d'une seule voix sur les sujets de cyberdéfense, les BRICS n'ont actuellement pas encore réussi à utiliser cette alliance dans les échanges internationaux.

1.2 Asie – Pacifique

1.2.1 Niveau de maturité

L'Asie-Pacifique est la région la plus disparate en matière de développement des technologies de l'information et des communications, d'infrastructures, de capacités cybernétiques, de cadres législatifs et réglementaires, de gouvernance et de sensibilisation aux enjeux de cybersécurité.

Cette disparité s'explique par des niveaux de développement très différents entre Etats. Le rapport de l'*Australian Strategic Policy Institute* (ASPI) sur la cybermaturité en Asie souligne ainsi de fortes inégalités entre les Etats dans tous les domaines (gouvernance, lutte contre la cybercriminalité, cyberdéfense, économie numérique et base industrielle, enjeux sociaux et sociétaux, etc.). Cette étude identifie quatre puissances numériques (l'Australie, la Corée du Sud, le Japon et Singapour) auxquelles on peut cependant ajouter la Chine[18].

En matière d'infrastructure et de connectivité, Singapour (82%), la Corée du Sud (84%), l'Australie (85%) et le Japon (91%) disposent des plus forts taux de pénétration tandis que Corée du Nord (0%), le Myanmar (2%) et le Cambodge (0%) ont les taux de pénétration les plus bas[19]. Ces statistiques se basent sur l'accessibilité à Internet pour les utilisateurs des pays considérés, mais passent cependant à côté des éventuels intranets locaux (on pense notamment à la Corée du Nord). Certains Etats n'ont en outre pas développé de mécanismes

[15] http://reseaux.blog.lemonde.fr/2014/09/19/guerrerhetorique-gouvernance-internet/
[16] http://news.xinhuanet.com/english/sci/2012-09/18/c_131858755.htm
[17] http://www.oneindia.com/international/india-us-to-enhancecyber-security-cooperation-1837954.html
[18] L'étude pénalise la Chine pour son manque de politique de coopération avec les CERT et services de police étrangers.
[19] http://www.internetworldstats.com/stats3.htm#asia

de gouvernance pour assurer le développement des TIC (Myanmar, Corée du Nord, Papouasie Nouvelle-Guinée, Iles Fidji), de législation appropriée (Cambodge, Laos, Corée du Nord) ou de mécanismes de lutte contre la cybercriminalité (Papouasie Nouvelle-Guinée, Cambodge, Laos). A l'inverse, les quatre géants cyber précédemment cités ont un écosystème numérique très développé.

Ces situations très différentes permettent d'expliquer les stratégies des Etats. Pour les pays à faible taux de pénétration, il s'agira avant tout de favoriser le développement des technologies de l'information et des communications et l'accès à Internet. Pour les pays très « numérisés », il s'agira au contraire de renforcer la cybersécurité à tous les niveaux de la société (Corée du Sud, Japon, Australie) ou bien encore l'exportation des produits fabriqués sur le territoire national (Chine, Corée du Sud). Le contrôle de l'information tient également une place importante dans la stratégie de l'OCS (Organisation de coopération de Shanghai), organisation intergouvernementale régionale asiatique. Créée le 14 et 15 juin 2001 à Shanghai, elle est composée de la Russie, la Chine, le Kazakhstan, le Kirghizistan, le Tadjikistan et l'Ouzbékistan.[20]
Parmi ses multiples objectifs, figurent le renforcement de la confiance mutuelle, la facilitation de la coopération entre les Etats parties, la sauvegarde de la paix et de la sécurité. Ce dernier objectif recouvre également la sécurité dans le cyberespace. Ainsi, les membres de l'OCS ont renforcé leur coopération en matière de cybersécurité.[21]

Selon une étude menée par la Chaire Castex de cyberstratégie, *« la vaste majorité des incidents se produisent entre nations voisines, au niveau régional. Les grandes puissances comme les Etats-Unis et la Chine opèrent à l'échelle globale mais les puissances moyennes opèrent principalement au niveau régional »*[22].
Face à l'augmentation des attaques, on note une prise de conscience des Etats qui mettent progressivement en place un cadre réglementaire dont l'effectivité reste à démontrer. Pour continuer à attirer les investisseurs, les pays d'Asie-Pacifique devront en effet nécessairement affirmer leur capacité à faire face aux cyberattaques.

1.2.2 Coopération régionale

Deux facteurs contribuent à renforcer la coopération entre les pays d'Asie Pacifique : l'interconnexion des économies, notamment du secteur numérique, moteur essentiel de la croissance, et le caractère transfrontalier des menaces. Si la coopération régionale en matière de cybersécurité est largement dominée par les facteurs géopolitiques traditionnels, les difficultés d'attribution des attaques et leur complexité constituent aussi des motivations supplémentaires.

Plus de 40 initiatives multilatérales ont émergé dans la région et permettent aux Etats les plus puissants d'affirmer leur puissance et d'influencer les autres. On peut distinguer les coopérations animées par des organisations existantes et celles résultant d'initiatives *ad hoc*.

Pour les premières, les organisations les plus impliquées sont la Coopération économique pour l'Asie-Pacifique (APEC), l'Association des nations de l'Asie du Sud-Est (ASEAN) et le Forum régional de l'Association des nations de l'Asie du Sud-Est (ASEAN Regional Forum).

- L'APEC est un forum économique intergouvernemental qui regroupe 21 Etats et dont l'objectif est de faciliter la croissance, la coopération et les échanges économiques entre les pays de la région. Un groupe de travail sur les technologies de l'information et des communications[23] traitant du développement des infrastructures et des services liés aux TICs, au partage d'informations et à l'élaboration de cadres réglementaires a été créé. Un plan d'action 2016-2020 a été publié en octobre 2015 et un sous-groupe de travail sur la sécurité a été mis en place. Parmi les sujets abordés, la cybersécurité et la cybercriminalité tiennent une place importante. La Thaïlande a ainsi proposé, dans le cadre des travaux de ce sous-groupe, l'élaboration d'une directive sur la sécurité des réseaux. De plus, une équipe (*Mutual recognition Arrangement Task Force*) a été chargée de mettre en place des standards de conformité pour les matériels de télécommunication.

[20] http://www.agoravox.fr/actualites/international/article/la-puissante-organisation-dont-162681
[21] http://french.xinhuanet.com/2016-01/27/c_135050545.htm
[22] Chaire Castex de cyberstratégie, *Géopolitique du Cyber en Asie*, septembre 2014, Etude réalisée avec le soutien de la Direction aux Affaires stratégiques, p.11
[23] http://www.apec.org/Home/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information

- L'ASEAN, qui regroupe 10 pays à vocation économique, sociale et culturelle, vise à encourager la coopération entre ses Etats membres. Si elle a commencé à se saisir du sujet , la cybersécurité ne constitue pas une priorité et les avancées sont encore peu nombreuses. La problématique a cependant été évoquée lors du sommet TELMIN-Chine du 23 janvier 2015 qui a vu l'adoption d'un programme de travail sur les TICs et la proposition par la Chine de mécanismes de coopération entre l'ASEAN et son CERT national. Une rencontre ASEAN-Chine portant sur le crime transnational a d'ailleurs eu lieu en juin 2015[24]. A noter que l'ASEAN et le Japon avaient, dès 2013, présenté une déclaration conjointe dans laquelle ils adoptaient un certain nombre de principes pour promouvoir la cybersécurité[25].
- L'ASEAN Regional Forum est un forum multilatéral traitant des questions de sécurité. Regroupant désormais 51 Etats membres, ce forum s'intéresse depuis 2004 aux questions de cybersécurité dans le cadre de ses travaux sur la sécurité, le terrorisme et la criminalité transfrontière. En 2012, il a adopté un programme de travail sur la sécurité des TICs. Objectif : promouvoir un environnement des TICs pacifique, sûr, ouvert et coopératif afin de prévenir les conflits et crises en développant la confiance entre les Etats[26]. Le plan a été présenté à la fin de l'été 2015 et un projet visant à élaborer des mesures de confiance dans le cyberespace a été lancé fin 2015. Ces projets prennent forme grâce à des réunions de travail organisées par l'ASEAN Regional Forum et ouvertes aux représentants des Etats membres mais également aux acteurs de la société civile. La problématique du « cyberterrorisme » a fait l'objet de plusieurs déclarations et réunions de travail, notamment sous l'angle de la gestion des contenus à caractère terroriste.

Autres organisations actives sur le sujet : l'Organisation de la coopération islamique des CERTs dont la Malaisie est membre, et la Banque asiatique de développement, qui fournit une aide financière importante à certains Etats (Vietnam, Thaïlande, Indonésie et Philippines) qui souhaitent développer des projets liés aux TICs.

En matière de coopération multilatérale ad hoc, l'initiative de coopération la plus aboutie est l'*Asia-Pacific Computer Emergency Response Team* (APCERT[27]) qui regroupe la Corée du Sud, le Japon, Taiwan, la Chine, Brunei, l'Inde, le Vietnam, l'Indonésie, la Malaisie, Singapour, les Philippines, l'Australie, la Thaïlande et Hong-Kong. La coopération est fondée sur l'échange d'informations et la participation à des exercices communs. Une plateforme de surveillance du trafic (TSUBAME) fournit des informations aux pays membres. Cette coopération technique, qui a pour ambition de créer un CERT régional, connaît plus de succès que le projet IMPACT de l'Union internationale des télécommunications dont le rôle est d'aider les pays dans l'évaluation de leurs besoins en matière de cybersécurité et dans la création de CERTs.

Au plan bilatéral, enfin, les accords sont de deux niveaux : il peut s'agir soit d'accords stratégiques classiques entre Etats alliés, soit de coopérations entre les forces de police. A titre d'exemple, la police australienne collabore avec les polices sud-coréenne et indonésienne et le Japon entretient des liens avec l'Indonésie. En août 2014, ce sont également la Chine et la Malaisie qui ont annoncé le développement de leur coopération. On trouve enfin également des accords bilatéraux entre le Vietnam et la Corée du Sud.

1.2.3 L'Asie-Pacifique et le reste du monde

Plusieurs pays asiatiques sont actifs au sein d'autres instances internationales, notamment de l'Organisation des Nations unies. La Chine, le Japon, la Malaisie, le Pakistan et la Corée du Sud ont ainsi participé aux travaux du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité nationale qui a rendu son rapport en juin 2015.

[24] http://www.asean.org/?static_post=overview-asean-china-dialogue-relations
[25] http://www.asean.org/storage/images/Statement/final_joint_statement%20asean-japan%20ministerial%20policy%20meeting.pdf
[26] http://aseanregionalforum.asean.org/files/library/Plan%20of%20Action%20and%20Work%20Plans/ARF%20Work%20Plan%20on%20Security%20of%20and%20in%20the%20Use%20of%20Information%20and%20Communications%20Technologies.pdf
[27] http://www.apcert.org/

La place et le rôle de la Chine dans les relations entre l'Asie et les autres parties du monde est centrale et concentre toutes les attentions. Acteur majeur de la scène internationale, elle cristallise toutes les tensions (nombreuses accusations de cyberattaques et d'espionnage industriel) et sa relation avec les Etats-Unis impacte largement ses stratégies d'influence, y compris sur les sujets cyber, dans la région. Le pivot américain vers l'Asie trouve également à s'exprimer dans ce domaine et les Etats-Unis mène une diplomatie cyber très active dans la région pour promouvoir un Internet pacifique, ouvert et sûr. Leur engagement auprès de certains Etats s'inscrit dans l'objectif de contrer l'influence de la Chine dans cette région.

La Russie s'est également tournée vers l'Asie en se rapprochant de la Chine. Ce rapprochement est également observable à travers l'adhésion des deux pays à l'OCS (Organisation de coopération de Shanghai) qui a pour finalité de renforcer leur coopération notamment en matière de sécurité dans l'espace numérique. La proposition de code de conduite déposé par la Russie, la Chine et d'autres pays de l'Asie centrale à l'ONU illustre bien ce rapprochement. De plus, plusieurs pays asiatiques partagent les inquiétudes russes sur la menace que représente Internet pour la stabilité interne d'un pays et s'accordent, malgré des divergences sur la gestion des contenus et la censure, sur la question de la régulation des activités des Etats dans le cyberespace en temps de paix ou sur la nécessité d'un certain contrôle souverain des Etats du cyberespace.

Sur les relations Asie-Pacifique et Europe, seuls l'Australie et le Japon ont ratifié la Convention de Budapest sur la lutte contre la cybercriminalité.

1.3 Moyen Orient

1.3.1 Niveau de maturité

Si le Moyen-Orient comptait 317.7 millions d'habitants fin novembre 2015, dont 160.8 millions utilisaient Internet, (taux de pénétration de 50,6%), la région ne connait pas un développement uniforme en matière de technologies de l'information et de communication. Cette disparité s'explique par des niveaux de développement très différents mais surtout par des rivalités de pouvoirs et une conflictualité qui freinent le développement du numérique dans certaines parties de la région.
Le taux de pénétration mobile est élevé dans l'ensemble de la zone : 9 pays sur 14 avaient déjà dépassé 100% de taux de pénétration en mars 2015. Les pays membres du Conseil de Coopération du Golfe (CCG) - Arabie Saoudite, Bahreïn, Emirats-Arabes-Unis, Koweït, Oman et le Qatar - sont notamment en avance avec des taux oscillants entre 170% et 200%. En 2014, la région connaissait d'ailleurs la plus importante croissance du trafic mobile du monde. [28] Région meurtrie par la succession des conflits, le Moyen-Orient se trouve aujourd'hui en proie à un déchaînement de violence sans précédent. Ces conflits sont d'ordres politiques, religieux, énergétiques ou stratégiques.

Terre de naissance des trois grandes religions monothéistes, le Moyen-Orient est aujourd'hui non seulement confronté à une tension constante entre celles-ci, mais également à des tensions intra-religieuse croissantes (notamment chiites-sunnites).
En termes de conflits territoriaux, le Moyen-Orient est évidemment marqué par le conflit Israélo-palestinien. Ce conflit est néanmoins loin d'être le seul, l'Iran et les Emirats arabes unis, l'Israël et la Syrie, l'Arabie Saoudite et le Yémen ne parvenant pas à trouver de consensus au sujet de leurs territoires.
Les conflits se poursuivent dans le domaine des hydrocarbures. Principaux fournisseurs d'hydrocarbure de toute la planète et situés dans une zone stratégique au carrefour de l'Europe, l'Afrique et l'Asie, les pays du Moyen-Orient peinent à trouver un accord sur le sort des hydrocarbures. A la suite notamment de la découverte de gaz dans la mer Méditerranée, des tensions ont vu le jour entre le Liban et l'Israël.[29]

Dans ce contexte conflictuel, l'espace numérique apparaît comme un espace stratégique dans lequel les conflits traditionnels n'ont pas tardé à s'y transposer en raison de la multitude d'actions qu'il permet,

[28] http://www.budde.com.au/Research/Middle-East-Mobile-Voice-and-Mobile-Operators-Market.html?r=51
[29] http://www.defense.gouv.fr/content/download/206617/2291582/file/EPS2013-Resume-Utilisation%20strat%20cyber%20MoyenOrient.pdf

anonymement et à faible coût. Parmi ces actions, figurent la communication, le renseignement, le sabotage et l'attaque.
Il ne fait nul doute que les Etats du Moyen-Orient ou les groupes non étatiques usent parfaitement des codes modernes à des fins de protection et de défense de leurs intérêts. En effet, les canaux de communication utilisés par ces acteurs sont très contemporains : à l'instar de la société, ils utilisent les technologies de l'information et de communication pour la diffusion et la protection de leurs intérêts.

Cependant, les capacités et les points de vue à l'égard des stratégies dans le cyberespace divergent selon les pays. Ainsi, quand la cyberstratégie est élevée au rang de priorité nationale dans certains pays, elle ne représente qu'une préoccupation quasi-anodine pour d'autres.

Israël accorde une importance croissante aux questions cyber notamment depuis l'arrivée du Premier ministre Benjamin Netanyahou en 2009. Ce dernier a mis en place une commission d'experts chargée de travailler sur la cybersécurité, elle-même à l'origine de l'institution centrale « Israel National Cyber Bureau » pour la coordination, le soutien, la règlementation et la coopération internationale sur les questions cyber. La sensibilisation de la population aux risques du cyberespace est une priorité fondamentale pour l'Israël.[30]
Pour une défense optimale contre toute cyberattaque de grande ampleur envers les infrastructures critiques de l'Etats, un ancien commandant de l'armée de l'air d'Israël, Eitan Ben Eliyahou, propose la mise en place de systèmes de secours parallèles permettant de maintenir le fonctionnement des systèmes informatiques de ces infrastructures dans l'hypothèse où ces dernières seraient cibles de cyberattaque. Ainsi, cette stratégie permettrait d'empêcher toute perturbation des systèmes informatiques et un fonctionnement ininterrompu garanti.[31]

Quant à l'Iran, sa sensibilité à la cybersécurité existait bien avant la survenance de cyberattaques de grande ampleur telle que l'attaque du virus *Stuxnet* dont il a été victime. Afin de pallier ses lacunes en la matière, l'Etat iranien a, depuis 2011, pris la décision de perfectionner ses infrastructures et ses équipements au point d'élever la sécurité numérique au rang de priorité nationale.
L'Iran dispose par exemple d'une cyberpolice ayant pour mission la répression de la cybercriminalité. En 2014, l'Iran a été placé 19ème sur 194 dans le classement des pays en fonction du niveau de leur cybersécurité.[32]
De façon non officielle, l'Iran soutient le groupe non étatique de hackers nommé Hezbollah. Ce groupe dynamique a particulièrement été aux côtés du pouvoir lors des contestations par le peuple en 2009 et organise souvent des conférences pour rassembler les partisans du gouvernement et parler des stratégies à mettre en place pour le cyber djihad.

En Syrie, le régime de Bachar Al-Assad n'a pas eu d'autre choix que de développer ses compétences et de mettre en place des infrastructures de cyberdéfense à partir des soulèvements de mars 2011. Depuis cette date, des cyberattaques visent le gouvernement de manière presque quotidienne. Le modèle de cybersécurité de l'Iran, faisant preuve de progrès considérables en matière cyber ces dernières années, a incontestablement été une source d'inspiration pour la stratégie syrienne, d'autant que ces deux Etats entretiennent des relations bilatérales privilégiées.
Le gouvernement syrien soutient activement des groupes de hackers travaillant officieusement à son service.

Suite à la prolifération des cyberattaques de grande ampleur dont la région a été victime depuis 2011, la péninsule arabique a naturellement abordé la problématique numérique, dans un premier temps, du seul point de vue de la cybercriminalité, et n'a pas tardé à l'encadrer strictement. Aujourd'hui, elle a pris conscience de la nécessité de l'élaboration de politiques de cyberdéfense. Dans cette perspective, de par leurs rapports étroits, la péninsule arabique profite du savoir-faire, des compétences et de l'expérience des entreprises et des autorités américaines en matière de stratégie de cyberdéfense.
L'originalité de cette péninsule par rapport au reste de la région demeure dans l'attribution de la sécurité des infrastructures à des CERT (Computer Emergency Response Team) contrairement à Israël ou l'Iran, où cette responsabilité est confiée à des organisations centrales.

[30] Ibidem.
[31] Ibidem
[32] http://iranfr.com/place-liran-cybersecurite/

Du côté du Yémen, les capacités intrinsèques en matière de cybersécurité et de cyberdéfense sont très faibles, voire inexistantes. Le pays est en proie à une guerre civile depuis 2011, le conflit opposant les Comités Révolutionnaires Houthi, soutenus par l'Iran et le Hezbollah, au gouvernement Hadi, dont le principal soutien est l'Arabie Saoudite. Le gouvernement Hadi se contente de faire appel au gouvernement américain pour la protection et la défense de ses systèmes d'information[33]. De l'autre côté du spectre, le groupe Yemen Cyber Army, qui semble être en réalité basé en Iran, est responsable de campagnes massives de défacement à l'encontre de l'Arabie Saoudite, ainsi qu'à la fuite de données du Ministère des Affaires Etrangères en mai 2015 (dont les données ont par la suite été publiées sur Wikilieak).

Concernant les organisations non étatiques du Moyen-Orient, elles ne dépendent d'aucune structure, sont multiples et ont des finalités diverses. Certaines d'entre elles ont de forts liens avec les Etats. Bien que le groupe Anonymous soit présent au Moyen-Orient, il ne représente pas un groupe majeur, à la différence d'Al-Quaïda, du Hezbollah ou encore du Hamas. Ces groupes ont parfaitement saisi les enjeux de l'espace numérique et tentent de perfectionner leur stratégie offensive en acquérant des compétences techniques pointues.

La lutte contre ces cyberattaques passe nécessairement par une lutte contre l'idéologie de ces groupes non étatiques et donc par une bataille sur le plan numérique. La forte diffusion numérique de leurs idéologies met la lutte contre la cybercriminalité au centre des préoccupations sécuritaires du Moyen-Orient.
Les capacités d'attaques cybernétiques de l'Iran sont une source d'inquiétude majeure pour les Etats du Golfe, tout comme celles d'Israël. Les cyberattaques peuvent avoir de graves répercussions sur la production pétrolière et donc avoir des conséquences sur l'économie mondiale.
La montée en puissance de l'Iran et d'Israël en matière de capacités cybernétiques bouscule les six pétromonarchies du golfe arabique, membres du Gulf Cooperation Council (GCC) : l'Arabie saoudite, Bahreïn, le Koweït, les Émirats arabes unis, Oman, et le Qatar, qui ne possèdent pas de capacités similaires, même si l'attaque iranienne sur l'Arabie Saoudite en 2012 résonna comme le *wake-up call* dans la région.[34] Depuis, les Etats-Unis ont soutenu les pays du Golfe dans l'amélioration de leurs capacités de cyberdéfense.
Les conflits géopolitiques se traduisent par un hacktivisme très actif au Moyen-Orient. Cet hacktivisme résulte en général de groupes de hackers patriotiques, dont la plupart sont a minima tolérés, voire contrôlés par les Etats ou factions qu'ils défendent comme la Syrian Electronic Army (SEA) ou encore la Yemen Cyber Army[35], en ce qu'ils sont la traduction dans le cyberespace de conflits interétatiques. L'Etat islamique a également développé des capacités d'action dans le cyberespace, notamment en termes de communication offensive, ce qui a suscité la création d'une mouvance hacktiviste anti-Daesh.
L'organisation a en effet su utiliser le cyberespace pour déployer une propagande portée par la démocratisation de l'Internet et le développement des réseaux sociaux, ainsi qu'une excellente maîtrise des codes de la communication occidentale qui en ont fait une stratégie médiatique redoutable. La lutte contre cette propagande est devenue un enjeu primordial pour les démocraties occidentales.[36]

1.3.2 Coopération régionale

Le Moyen-Orient compte un certain nombre d'alliances régionales dont plusieurs en matière de cybersécurité. Branche de l'ITU (International Telecommunication Union) des Nations Unies, l'IMPACT (International Multilareal Parnership Against Cyber Threat) composée de l'Iran, la Syrie, l'Israël, le Liban, l'Arabie Saoudite, le Yémen et l'Oman, est l'une des alliances les plus importantes du Moyen-Orient en terme de cybersécurité. Le but de cette alliance est de contribuer à la protection des systèmes informatiques de l'ONU et de mettre à la disposition des Etats parties, des experts et des ressources en cybersécurité.
L'IMPACT s'est elle-même alliée à l'ATI (Autorité des technologies de l'information omanaise chargée de perfectionner la connectivité des autorités étatiques, des entreprises et des citoyens omanais) pour la création du CRCS (Centre régional de cyber sécurité) à Oman. Son objectif est de soutenir les Etats arabes dans la création de centres nationaux de cybersécurité et, de façon générale, de les assister et les entraîner à la sécurisation de leurs infrastructures.

[33] http://www.defense.gouv.fr/content/download/206617/2291582/file/EPS2013-Resume-Utilisation%20strat%20cyber%20MoyenOrient.pdf
[34] http://csis.org/publication/cybersecurity-and-stability-gulf
[35] http://www.crowdstrike.com/global-threat-report-2015/
[36] http://www.cyberstrategie.org/sites/default/files/utilisationcyberespacedaesh_bbonifait.pdf

La localisation de ce centre à Oman est source de débats car une possible mutation du centre en véritable organisation de cyberdéfense n'est pas à exclure, ce qui ne ferait que confirmer les craintes des acteurs écartés du projet (Israël et Iran).
D'autant qu'il existait d'ores et déjà une coopération multilatérale ad hoc via l'*Organisation of The Islamic Cooperation - Computer Emergency Response Teams* (OIC-CERT) dont tous les pays de la région sont membres hormis l'Etat d'Israël. La coopération est fondée sur l'échange d'informations et la participation à des exercices communs, entre membres, mais aussi en partenariat avec l'APCERT, l'*Asia-Pacific Computer Emergency Response Team* qui regroupe l'Australie, Brunei, la Chine, la Corée du Sud, Hong-Kong, l'Inde, l'Indonésie, le Japon, la Malaisie, les Philippines, Singapour, Taiwan, la Thaïlande et le Vietnam, et l'*African forum of computer incident response teams* (AfricaCERT) qui regroupe le Burkina-Faso, le Cameroun, la Côte d'Ivoire, l'Egypte, le Ghana, le Kenya, l'île Maurice, le Maroc, l'Afrique du Sud, le Soudan et la Tunisie. Alors que des pays tels que l'Arabie Saoudite et les Emirats arabes unis sont moyennement intéressés par des exercices de protection contre les cyberattaques organisés par l'OIC-CERT, certains, tel que le Qatar, ne figurent même pas parmi membres de cette organisation.
Concernant la Turquie, bien qu'elle fasse partie de l'OIC-CERT, elle s'implique essentiellement dans les actions de l'OTAN. Il faut à cet endroit rappeler que la Turquie est le seul pays du Moyen-Orient à être membre de l'OTAN.[37] Elle a intégré le Centre d'excellence de cyberdéfense de l'OTAN (NATO Cooperative Cyber Defense Centre of Excellence) le 3 novembre 2015.[38]
Le Centre d'excellence de cyberdéfense de l'OTAN est un organisme militaire de coopération international, crée en 2008 en Estonie, ayant vocation à améliorer les capacités de cyberdéfense de ses adhérents, par la formation des responsables et des spécialistes des Etats membres de l'OTAN ou des Etats partenaires.[39] Il contribue à la création de doctrines dans le domaine de la cybersécurité et améliore l'interopérabilité et les capacités. En outre, il procède au test et à la validation des stratégies à l'aide d'expérimentations.[40] L'expertise et l'expérience de ce centre permettent aux adhérents d'être plus opérationnels face aux attaques numériques.[41] Ce centre, composé de vingt membres, s'élargit constamment. Les prochains adhérents seront la Belgique et la Suède. Il représente le centre d'excellence le plus important de l'OTAN, tant au regard de la quantité des membres que de l'importance des sujets de cybersécurité.[42]
Au niveau local, la Turquie a introduit en 2012 le « Cyber Defense Command » dans ses forces armées. Cette entité a pour mission de contribuer à la cybersécurité du pays tout en coordonnant le TUBITAK (Conseil de la recherche scientifique et technologique turque), le Ministère des transports maritimes et des communications turque et l'OTAN.

Au terme de l'analyse, il apparaît que les Etats du Moyen-Orient sont membres de multiples accords de coopération en matière de cybersécurité tant bilatéraux, régionaux qu'internationaux. Il ressort toutefois que la meilleure échelle de lutte demeure malgré tout l'échelle nationale. Les stratégies les plus efficientes émergent à l'initiative du gouvernement national avec la contribution du monde académique et industriel.
Eu égard à l'intensité des rivalités au Moyen-Orient, un tel constat n'est pas étonnant.

1.3.3 Le Moyen-Orient et le reste du monde

Plusieurs pays de la région sont actifs au sein des instances internationales. Israël a ainsi participé aux travaux du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité informatique qui a rendu son rapport en juin 2015. Les places et rôles de l'Iran, d'Israël et de l'Arabie Saoudite dans les relations entre le Moyen-Orient et les autres parties du monde sont centraux et concentrent toutes les attentions. Acteurs majeurs de la scène internationale, ils cristallisent toutes les tensions (nombreuses accusations de cyberattaques et d'espionnage industriel). Les relations avec les Etats-Unis influencent largement les stratégies d'influence, y compris sur les sujets cyber, dans la région.
L'Union internationale des communications (UIT) est un des moteurs du développement des TICs dans le monde arabe. La Ligue des Etats arabes travaille en partenariat avec l'UIT depuis le Sommet « Connecter le monde arabe » tenu à Doha, au Qatar, en mars 2012. Ainsi, un projet sur la gestion du spectre est mené à titre

[37] http://www.nato.int/cps/fr/natohq/topics_52044.htm
[38] http://www.postimees.ee/3385113/nato-kuberkaitsekeskusega-liitusid-kreeka-turgi-ja-soome
[3939] https://fr.sputniknews.com/international/20130111197197027/
[40] http://www.nato.int/cps/fr/natohq/topics_68372.htm
[41] https://ccdcoe.org/
[42] http://www.mil.be/fr/article/le-chef-de-la-defense-visite-le-centre-dexcellence-en-cyber-securite-de-lotan

consultatif par l'UIT depuis plus de dix ans auprès de l'Arabie Saoudite en collaboration avec le Programme des Nations Unies pour le Développement et a été prolongé en 2013 pour une période supplémentaire de trois ans, jusqu'à la fin 2016. En outre, l'UIT et le Partenariat multilatéral international de lutte contre les cybermenaces (IMPACT) ont conclu un accord en décembre 2012 avec l'Etat d'Oman (représenté par l'Autorité des technologies de l'information, ITA) pour établir un centre régional d'innovation en matière de cybersécurité afin de répondre aux besoins de la région arabe. Ce centre est officiellement entré en activité en mars 2013 et a pour mission de renforcer le rôle de l'UIT visant à instaurer une confiance vis-à-vis des TIC et à garantir la sécurité de celles-ci dans la région.[43] Entre 2015 et 2017, l'UIT focalise ses initiatives sur 5 piliers : le développement de la bande passante, la confiance et la sécurité, le développement des TICs au profit du développement durable, l'accès pour tous et une formation sur mesure.[44]
A propos des relations entre le Moyen-Orient et l'Europe, notons que seuls la Turquie, qui est membre du Conseil de l'Europe, et Israël ont ratifié la Convention de Budapest sur la lutte contre la cybercriminalité.

Il n'existe pas d'unité régionale tant au plan géopolitique traditionnel que sur les sujets d'intérêt cyber. La fragmentation de la région se répercute ainsi dans le cyberespace et les disparités engendrent une multiplicité des stratégies, les nombreux conflits traditionnels de la région ayant naturellement trouvé une continuité dans le cyberespace.

1.4 Europe

1.4.1 Niveau de maturité

Le taux de pénétration d'Internet reste relativement disparate, notamment entre Europe de l'Est et Europe de l'Ouest. Ainsi l'Europe de l'Est regroupe les pays dont les taux de pénétration sont les plus bas de la région, notamment l'Ukraine (avec un taux de pénétration de 43,4%), la Moldavie (49,2%), la Bulgarie (56,7%), alors que les plus hauts taux de pénétration de l'Europe de l'Ouest dépassent les 90%, avec notamment l'Islande (98,2%), la Norvège (96,3%) et le Danemark (96,3%). De la même manière, là où les grandes puissances européennes (Royaume-Uni, Allemagne et France) ont massivement investi dans le domaine de la cybersécurité et de la cyberdéfense, que ce soit en matière législative (encadrement de la protection des infrastructures critiques), ou en matière de certification des produits, les « petits » pays européens, ne disposant pas des moyens techniques et législatifs nécessaires, ne sont pas toujours en mesure de fournir les éléments requis lors d'une coopération et demeurent en conséquent fragiles, ce qui constitue un facteur de blocage en matière de coopération multilatérale.

Même si l'intégration européenne souffre des soubresauts nationaux (menaces de Brexit et de Grexit, processus d'intégration ukrainien et turc), l'Union européenne permet cependant d'améliorer le niveau de maturité des Etats les plus faibles dans le domaine grâce à l'uniformisation législative et réglementaire qu'elle entraine. Les dispositions (stratégies, conventions, règlements, directives) adoptées au niveau européen permettent en effet de tirer les pays les plus fragiles vers le haut. A titre d'exemple, la directive NIST qui devrait rentrer en vigueur en 2018 va contribuer à renforcer les niveaux de protection des Opérateurs d'Importance Vitale (OIV) face aux cybermenaces dans chaque pays européen.

1.4.2 Coopération régionale

Le cadre européen reste, malgré les disparités des niveaux d'évolution, le cadre de référence dans le domaine numérique.

[43] https://itunews.itu.int/fr/5000-LES-ETATS-ARABES-BR-La-connectivite-numerique-gagne-du-terrain-dans-le-monde-arabe.note.aspx
[44] http://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Pages/Regional_Initiatives_Projects.aspx

Les actions au plan législatif

Au plan législatif, il faut évoquer la Directive NIS (Network Security and Information).[45] Cette directive a été proposée par la Commission européenne en février 2013, puis a été approuvée en décembre 2015. Son entrée en vigueur est prévue pour l'année 2018. L'objectif de cette directive est d'assurer la mise en place d'un niveau élevé de sécurité pour les systèmes de réseaux et d'information des infrastructures critiques, telles que l'énergie, la santé, les transports, situées à l'intérieur de l'Union européenne.[46]

Plus récemment, à l'issue d'une longue période de travail et de négociations de quatre ans, le Parlement européen a adopté le 14 avril 2016, un règlement sur la protection des données personnelles prenant en compte la numérisation croissante de la société. Il remplacera la directive 95/46/CE du 24 octobre 1995 sur la protection des données personnelles, adoptée lorsque l'internet n'en était qu'à ses prémices et qui semblait définitivement obsolète. Applicable à partir de 2018 sur l'ensemble du territoire des Etats membres de l'Union européenne, il représente une avancée remarquable dans l'histoire de la protection européenne des données personnelles.

En parallèle, tendant vers un modèle de protection efficient dans le transfert transatlantique des données personnelles, surtout à la suite de l'invalidation du *Safe Harbor* par la Cour de Justice de l'Union européenne le 29 février 2016, la Commission européenne et les Etats-Unis ont établi un nouveau projet de décision d'adéquation nommé *EU-U.S. Privacy Shield*. Ce nouvel accord a pour objectif de préserver les droits fondamentaux des personnes tout en maintenant la sécurité juridique des opérateurs dans le cadre des transferts transatlantiques de données personnelles des citoyens européens.

Les avancées législatives semblent donc notables, en dépit de certaines incertitudes subsistantes quant à l'application effective des dispositions de ces nouveaux textes.

Le renforcement de l'ENISA

Au plan organisationnel, il faut souligner que l'European Network Information Security Agency (ENISA) - qui gère la protection des systèmes d'information de l'Union et l'élaboration d'une politique européenne de SSI, commune aux Etats membres - dispose aujourd'hui de réelles capacités en matière de formation, d'entrainement, d'expertise technique, d'études et de veille. Bien que son mandat de 5 ans reste relativement restreint et qu'elle n'ait jamais eu de pouvoir de décision contraignant, elle entend combler le fossé qui existe entre le politique et l'opérationnel en développant une plateforme européenne pour l'échange et le partage d'informations[47]. Elle organise en outre régulièrement des exercices de crise baptisés Cyber Europe[48]. A noter que l'OTAN organise également les exercice de défense cyber Cyber Coalition (dont la dernière édition s'est tenue en novembre 2015[49]) et Locked Shields (dont la dernière édition s'est tenue en avril 2015)[50].

Recherche & Technologie

En matière de Recherche & Technologie, enfin, l'Union européenne a lancé plusieurs appels à projet sur la cybersécurité dans le cadre de son programme Horizon 2020. Ce programme-cadre novateur est un programme de recherche de 2014 à 2020, regroupant les programmes de recherche et d'innovation européens. Il soutient et favorise la croissance de ces programmes et leurs facilite l'accès aux financements européens. Les trois priorités du programme Horizon 2020 sont : élever le niveau d'excellence scientifique de l'Europe, améliorer la compétitivité des entreprises européennes, et, concentrer la recherche et l'innovation vers la réponse aux grands défis sociétaux. Parmi les programmes participants figurent notamment, le P.C.R.D.T et Euratom.[51]

Le rôle de l'OTAN

[45] http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security
[46] http://www.village-justice.com/articles/Les-obligations-matiere-securite,21341.html
[47] Laboratoire de l'IRSEM N°16, « La coopération internationale et bilatérale en matière de cybersécurité : enjeux et rivalités », Alix Desforges, consultable en ligne : http://www.defense.gouv.fr/actualites/operations/laboratoire
[48] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce
[49] http://www.aco.nato.int/cyber-exercise-challenges-defense
[50] http://www.nato.int/cps/en/natohq/news_118855.htm
[51] http://www.horizon2020.gouv.fr/cid73300/comprendre-horizon-2020.html

L'OTAN a de son côté lancé un partenariat avec l'industrie de cyberdéfense (Nato Industry Cyber Partnership).[52]

Ces différentes actions contribuent à renforcer la coopération intra-européenne et favorisent le *capacity building*. Néanmoins, la coopération européenne en matière de cybersécurité se heurte très rapidement à ce que les Etats considèrent être leurs zones de souveraineté respectives. Si le *capacity building* ne soulève que peu de difficultés, il n'en va pas de même pour la mutualisation ou le partage capacitaire.

Vincent Joubert et Jean-Loup Samaan, dans leur article « L'intergouvernementalité dans le cyberespace : étude comparée des initiatives de l'Otan et de l'UE »[53] reviennent ainsi sur un domaine dans lequel la coopération est particulièrement compliquée : la cyberdéfense. Que ce soit au niveau de l'Union européenne, ou de l'OTAN, ils démontrent les limites de l'approche multilatérale, malgré des efforts pour mettre en œuvre des politiques intergouvernementales. Ces limites tiennent principalement à des divergences de vues entre les « petits » Etats européens qui profiteraient d'une mutualisation des forces, et les « grands » Etats comme le Royaume-Uni, la France ou l'Allemagne qui *« ont massivement investi dans le domaine, ont produit un vaste corpus doctrinal en matière de lutte informatique et ont parfois même constitué des Cyber Commandements »*[54] dès lors que toute mutualisation pourrait porter atteinte à leur souveraineté.

En outre, la question des capacités offensives divise, notamment d'un point de vue juridique. Par ailleurs, dès lors que l'OTAN ne possède aucun levier sur le secteur privé (qui contrôle majoritairement le cyberespace), les capacités réelles d'action de l'organisation en matière de défense cyber sont limitées, principalement à ses propres réseaux. Comme le souligne Florence Mangin, ancienne ambassadrice de la France au groupe des experts gouvernementaux (GGE) sur la cybersécurité, *« la France estime que l'OTAN n'a pas vocation à être un parapluie cyber pour les alliés à un niveau supranational. Elle doit avant tout permettre une montée en compétence de ses membres »*[55].

Toute coopération sur des domaines stratégiques, qui plus est touchant au renseignement, est *de facto* compliquée à un niveau multilatéral et se gère principalement dans un cadre bilatéral. La cybersécurité reste donc essentiellement l'objet d'une coopération volontaire entre nations et avec le secteur privé. L'ANSSI et le BSI allemand ont ainsi développé deux projets communs en matière de standards pour le Cloud et de cryptographie pour les emails. A l'instar du rôle moteur qu'il joue au plan global, le couple franco-allemand se cherche clairement un rôle au plan numérique, comme en témoignent les initiatives communes engagées récemment par les deux pays. Le 27 octobre 2015, une conférence numérique franco-allemande réunissait ainsi les ministres Sigmar Gabriel et Emmanuel Macron. Objectif : mettre en œuvre une coopération bilatérale destinée à accélérer la transformation numérique de l'économie. Conscients du dynamisme des secteurs numériques, les deux gouvernements entendent renforcer la coopération entre les écosystèmes numériques et les plateformes industrielles, mais aussi promouvoir une stratégie globale pour le marché unique du numérique au sein de l'Union européenne.[56]

Notons enfin que la coopération passe aussi par des regroupements d'autorités administratives consultatives et indépendantes, comme le G29 pour les autorités de protection des données personnelles ou encore l'Organe des régulateurs européens des communications électroniques (ORECE ou BEREC en anglais) pour ce qui est des régulateurs télécoms. Le BEREC est une instance européenne indépendante créée par le Conseil de l'Union européenne et le Parlement européen rassemblant les 28 Etats de l'UE ainsi que 9 régulateurs observateurs qui conseille les institutions européennes et permet de renforcer la coopération entre régulateurs des communications électroniques et ces mêmes institutions.[57]

1.4.3 L'Europe et le reste du monde

[52] http://www.nicp.nato.int/fr/index.html
[53] Vincent Joubert, Jean-Loup Samaan ,« L'intergouvernmentalité dans le cyberespace : étude comparée des initiatives de l'Otan et de l'UE »*Hérodote*, 2014/1 n°152-153, p.276-295.
[54] Ibidem.
[55] http://www.alliancy.fr/a-laffiche/securite/2015/07/08/cybersecurite-la-diplomatie-francaise-a-la-manoeuvre
[56] http://www.economie.gouv.fr/conference-numerique-franco-allemande-transformation-numerique-economie
[57] http://www.arcep.fr/index.php?id=12961#c92940

La coopération bilatérale entre les pays européens et le reste du monde est très poussée, en témoigne l'intérêt de la Chine et de l'Allemagne pour la finalisation d'un accord relatif à la cybersécurité.[58] Mais les pays européens et l'Union entendent aussi jouer un rôle important au sein des instances internationales.

Ainsi, l'Allemagne, l'Espagne, l'Estonie, la France et le Royaume-Uni ont participé aux travaux du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité nationale qui a rendu son rapport en juin 2015. Les trois principales puissances européennes (Royaume-Uni, France et Allemagne) étaient présentes pour porter les revendications européennes sur la scène internationale. Ce rapport met en exergue une réalité prosaïque et incite fortement les Etats parties à mettre en œuvre des dispositifs efficients afin de réduire les utilisations controversées des technologies de l'information et de la communication constatées depuis leurs territoires.[59]

Qui plus est, la Convention de Budapest du 23 novembre 2001, œuvre du Conseil de l'Europe, est encore à ce jour le seul grand texte international existant en matière de lutte contre la cybercriminalité. Ainsi, hormis les pays membres du Conseil de l'Europe, Afrique du Sud, Australie, Canada, Etats-Unis, Japon, Maurice, Panama, République dominicaine et le Sri Lanka ont signé ou ratifié la Convention.
Plus récemment, le 30 mars 2016, le Sénégal a adopté le projet de loi autorisant la ratification de la Convention de Budapest.[60]

Il faut observer que la Convention de Malabo du 27 juin 2014, convention africaine relative à la cybersécurité et la protection des données à caractère personnel, ouverte exclusivement aux pays africains, a été établie sur le modèle de la Convention de Budapest.[61] Cette convention représente une avancée considérable en termes de lutte contre la cybercriminalité en Afrique. Elle s'articule autour de trois axes principaux : la lutte contre la cybercriminalité, la protection des données à caractère personnel et, enfin, l'encadrement des transactions électroniques.

Concernant les relations Europe - Etats-Unis, l'analyse démontre l'existence d'un certain nombre de désaccords notamment sur les questions de protection des données personnelles, de liberté d'expression, ou encore de propriété intellectuelle.
L'un des désaccords les plus importants entre l'Europe et les Etats-Unis concerne la gouvernance de l'internet et le statut de l'ICANN (Internet Corporation for Assigned Names and Numbers) qui est le « régulateur de l'internet ». Afin de donner à l'ICANN une indépendance vis-à-vis du gouvernement américain, un projet de réforme de cette dernière a été examiné le 10 mars 2016 à Marrakech. Théoriquement, il consiste en l'abandon de la tutelle américaine de l'ICANN laissant la place à une gouvernance multipartite internationale.
Néanmoins, le Ministère des affaires étrangères français a récemment fait savoir qu'il n'était pas satisfait de l'organisation future prévue pour l'ICANN et signale l'influence des géants de l'internet américains sur cette organisation. En effet, selon le Ministère des affaires étrangères, lors des discussions dudit projet de réforme, par un fort lobbying, les GAFA ont réussi à obtenir une diminution des pouvoirs des Etats au sein de l'ICANN.[62]
Le projet de réforme doit à ce stade être étudié par les Etats-Unis. Le gouvernement Français demande aux Etats-Unis de tenir compte des préoccupations des Etats concernant l'organisation future de l'ICANN.[63]

La fin de l'année 2015 aura été marquée par un coup de force européen lorsque la Cour de justice de l'Union européenne (CJUE) a invalidé, le 6 octobre 2015, l'accord, dit « Sphère de sécurité », qui encadrait les transferts de données personnelles de citoyens européens vers les Etats-Unis. Si un "Safe Harbor 2.0", baptisé Privacy Shield, a été annoncé, ce dernier est d'ores-et-déjà contesté, au nom de la défense de la souveraineté des Européens sur leurs données

Qu'il s'agisse de souveraineté sur les données, ou de façon plus globale, dans le cyberespace, le débat sur la souveraineté est très présent en Europe. Certains pays européens ont même adopté des positions assez dures vis-à-vis d'entreprises américaines afin de les soumettre à leur juridiction et de faire appliquer leurs décisions de façon extraterritoriale. Pour exemples[64], en France, en juin 2015, la CNIL a demandé à Google d'appliquer le droit au déréférencement partout, et plus seulement en Europe, comme la plateforme le faisait pour

[58] http://www.ibtimes.com/cybersecurity-deal-between-china-germany-works-report-2162901
[59] http://www.un.org/press/fr/2015/agdsi3537.doc.htm
[60] http://www.observatoire-fic.com/un-pas-decisif-du-senegal-vers-ladhesion-et-la-ratification-des-conventions-de-budapest-et-de-malabo/
[61] http://www.afapdp.org/wp-content/uploads/2014/07/CONV-UA-CYBER-PDP-2014.pdf#sthash.ETVa2dtR.dpuf
[62] http://www.lemonde.fr/economie/article/2016/03/24/icann-paris-denonce-une-privatisation-de-la-gouvernance-d-internet_4889567_3234.html
[63] http://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/evenements/article/gouvernenance-de-l-internet-reforme-de-l-icann-10-03-16
[64] Rapport 2015 Internet & Jurisdiction disponible sur internet : http://www.internetjurisdiction.net/observatory/retrospect/archive2015/

contourner le droit à l'oubli. Enfin aux Pays-Bas, en octobre 2015, un tribunal hollandais a ordonné à Google de communiquer des informations sur des utilisateurs même si ceux-ci vivaient en dehors de l'Union européenne. Tout l'enjeu de ces décisions repose sur la prévention des phénomènes de *forum-shopping* et de *law-shopping* de la part des géants de l'internet, consistant à choisir une juridiction ou une législation qui leurs serait plus favorable. En d'autres termes, l'objectif est d'éviter que ces entreprises échappent au droit national qui leur impose un certain nombre de contraintes. Dans le même temps, les propositions en faveur d'une souveraineté technologique se sont multipliées en Europe depuis les révélations Snowden de 2013. Tim Maurer, Robert Morgus, Isabel Skierka, Mirko Hohmann dans leur article "Technological Sovereignty: Missing the Point? An Analysis of European Proposals after June 5, 2013" ne recensaient pas moins de 18 propositions dans ce sens, émanant de 12 pays européens différents, Allemagne et France en tête. Ces propositions concernaient aussi bien la question des câbles sous-marins, de la localisation des données, de la gouvernance, de la protection des données personnelles, que du comportement des agences de surveillance ou encore du chiffrement.[65]

En 2014, l'Allemagne a proposé aux Etats-Unis de signer un accord bilatéral concernant le non espionnage réciproque. Les Etats-Unis ont refusé de signer cet accord. Ce refus suspicieux aux yeux de l'Allemagne a brisé la confiance des administrations allemandes à l'égard des acteurs numériques américains. Cette méfiance a été corroborée par l'écoute du téléphone d'Angela Merkel la même année par la NSA.[66] Ces phénomènes ont poussé les autorités allemandes à vouloir mettre un terme à leurs relations commerciales avec les entreprises informatiques américaines. De ce fait, l'Allemagne a rompu son contrat de fourniture d'infrastructures de réseaux de télécommunications avec l'entreprise américaine Verizon et l'a confié à une entreprise allemande Deutsche Telekom.[67]
Le 12 juin 2015, le gouvernement allemand a voté une nouvelle loi visant à améliorer la sécurité des réseaux des administrations et des infrastructures essentielles à l'Allemagne. Cette loi comporte des dispositions permettant à l'Etat allemand de contrôler les produits de sécurité informatique, proposés aux administrations ou aux infrastructures essentielles, afin de vérifier qu'aucune porte ouverte ne permette un espionnage extérieur. Elle oblige également les infrastructures essentielles à signaler les cyberattaques dont elles seront victimes.[68]
A ce débat sur la souveraineté numérique s'ajoute également un différend concernant les règles applicables en matière de propriété intellectuelle. Les grands groupes européens (Airbus, Ericsson, Orange, Alstom, etc.) s'élèvent en effet contre une décision de l'Institut des ingénieurs électriciens et électroniciens (IEEE). L'Institut a pris la décision - validée par le département américain de la justice – de modifier les méthodes de rémunération des innovations brevetées, en se basant, non plus sur la valeur ajoutée apportée à un produit par une innovation, mais plutôt sur le moins onéreux des composants intégrés au produit fini servant de support à ladite innovation. Les coûts s'en trouvent diminués en faveur des Géants du net américains, tout en fragilisant la chaîne de financement de l'innovation, selon l'alliance « IP Europe » (Intellectual property Europe) créée à la suite de cette décision par une vingtaine de sociétés innovantes européennes[69].

Pour l'Europe, qui se veut « terre de droit », le levier juridique est ainsi un outil primordial pour tenter de faire valoir ses intérêts. Outre la protection de la vie privée ou la propriété intellectuelle, cette approche se vérifie aussi en matière de neutralité du net : par l'adoption du règlement européen 2015/2120 du 25 novembre 2015 établissant des mesures relatives à l'accès à un internet ouvert, l'Union européenne a officiellement instauré un traitement égal et non-discriminatoire du trafic internet, d'une part, et un droit de diffusion et d'accès aux informations et contenus de son choix pour tous d'autre part.[70]

[65] Tim Maurer, Robert Morgus, Isabel Skierka, Mirko Hohmann, "Technological Sovereignty: Missing the Point? An Analysis of European Proposals after June 5, 2013", Novembre 2014, consultable en ligne : https://www.newamerica.org/downloads/Technological_Sovereignty_Report.pdf
[66] http://www.lemonde.fr/pixels/article/2014/11/10/espionnage-les-entreprises-americaines-face-a-une-suspicion-grandissante-en-allemagne_4521458_4408996.html
[67] http://www.lemonde.fr/international/article/2014/06/27/ecoutes-de-la-nsa-berlin-se-passe-de-verizon_4446486_3210.html
[68] http://www.dw.com/en/germany-tightens-it-security-laws/av-18513902
[69] http://www.lesechos.fr/idees-debats/sciences-prospective/021646198495-innovation-les-etats-unis-inquietent-les-europeens-1195126.php
[70] http://www.arcep.fr/fileadmin/reprise/dossiers/net-neutralite/reglement-2015-2120_fr_NN.pdf

1.5 Afrique

1.5.1 Niveau de maturité

Si le continent africain comptait fin novembre 2015, 330,9 millions d'internautes, équivalents à un taux de pénétration de 28,6%, l'Afrique n'en reste pas moins, à bien des égards, aussi disparate que la région asiatique en matière de développement des technologies de l'information et des communications. Ceci peut s'expliquer par des niveaux de développement fort différents entre les Etats, mais aussi par le niveau de priorité accordé selon les pays au développement d'un Internet de qualité.

Le taux de pénétration mobile est très hétérogène en Afrique, il varie d'un pays à l'autre de 9 à 129%. Le marché africain de la téléphonie représente tout de même 13% du marché mondial. Les cinq premiers marchés d'Afrique - Nigeria, Egypte, Afrique du Sud, Ethiopie et République Démocratique du Congo - représentent 44% du marché total, alors que les 30 derniers pays n'atteignent même pas les 10% du total. Seuls quatre pays font état d'une pénétration supérieure à 100% : Mali (124%), Gabon (118%), Botswana (112%) et Gambie (104%).[71]
Si le continent s'est bien lancé dans le développement des technologies du numérique en développant rapidement la fibre optique et la téléphonie mobile, la réalité du numérique reste clairsemée et une véritable « fracture numérique »[72] existe entre les pays africains.
En effet, si des pays comme le Maroc, l'Egypte, l'Afrique du Sud, la Tunisie, le Ghana, la Namibie, le Bostwana, le Zimbabwe, le Nigéria, le Sénégal, la Côte d'Ivoire, le Gabon, le Lesotho ou encore le Kenya connaissent un important développement numérique, le reste de l'Afrique n'est pas encore pleinement tourné vers le numérique.
Sur une échelle mondiale, les utilisateurs africains représentent 9,8% en dépit des utilisateurs. L'observation de ces statistiques impose un constat immédiat : nombre d'utilisateurs internet africains reste faible au regard de l'importance de la taille du continent et de la population, soit 1,15 milliards[73] d'habitants en Afrique contre 7,2 milliards d'habitants dans le monde en 2015.[74]

Ces constats trouvent leur justification dans la faiblesse, voire l'absence, d'infrastructures et d'équipements en ordinateurs et en connexion internet fixe.
A titre d'illustration, au Sénégal, les statistiques démontrent que pour l'année 2014, seuls 7,8% des ménages disposaient d'un ordinateur fixe, d'autant que parmi eux, seuls 1,5% disposaient d'une connexion internet ADSL. [75] Toutefois, avant même d'évoquer le problème de l'important retard infrastructurel, il est nécessaire de mettre l'accent sur l'absence de réseaux d'électricité dans certaines régions d'Afrique, handicapant naturellement l'installation de réseaux informatiques.
En effet, l'installation d'infrastructures et de réseaux de connexion est étroitement liée à l'installation de réseaux d'électricité, car il va de soi que sans électricité, la connexion internet est impossible.
Bien que l'émergence des cybercafés a eu, et continue d'avoir, pour effet de favoriser le taux de pénétration africain, cette alternative de connexion est loin d'être la panacée.

La connectivité semble se diriger vers une mutation majeure qui passe inéluctablement par le mobile : c'est l'expansion du mobile qui a changé la conjoncture en démocratisant l'accès au réseau internet, même si de fortes disparités subsistent encore selon les pays. Ainsi, afin de remédier au défaut d'équipements fixes, les Africains se sont rabattus sur la connexion internet mobile.
Les statistiques font transparaître un essor phénoménal du mobile en Afrique, avec notamment, un taux de pénétration passant de 2% en 2000 à 82% en 2015 pour l'Afrique sub-saharienne. L'Afrique est donc un continent en pleine mutation numérique.

[71] http://www.journaldunet.com/ebusiness/expert/61063/le-potentiel-de-la-telephonie-mobile-en-afrique-est-encore-consequent.shtml
[72] http://www.geopolitique-africaine.com/la-grande-fracture-numerique_988898.html
[73] http://www.statistiques-mondiales.com/afrique.htm
[74] http://www.statistiques-mondiales.com/population_par_pays.htm
[75] L'essor du numérique en Afrique de l'Ouest : entre opportunités économiques et cybermenaces, Les notes stratégiques CEIS, Charlotte Gonzales, Julien Dechanet, Novembre 2015.

Cette transformation numérique se fait cependant de façon anarchique (« *Far West* »), avec tous les problèmes que cela peut susciter. L'émergence de nouveaux usages à destination du peuple africain ayant vu le jour, la connexion via mobile constitue un nouveau terrain de « jeu » pour les cybercriminels. Si « Internet multiplie les accès au monde » il multiplie aussi « les possibles déviances » [76]. La cybercriminalité s'est ainsi considérablement développée. Un rapport publié par la société Trend Micro en 2012, indiquait que les cybercrimes en provenance de l'Afrique étaient classés « parmi les dix principales menaces qui pèseront sur les entreprises et le grand public dans les années à venir, car comme le cyberespace, la cyberescroquerie n'a pas de frontières ». Ainsi, les Etats-Unis, inquiets des attaques venant d'Afrique, dressaient un classement des dix premières sources mondiales de cyberarnaques qui voyait le Nigéria se hisser à la 3ème position, le Ghana 7ème, et le Cameroun à la 9ème place du classement[77].

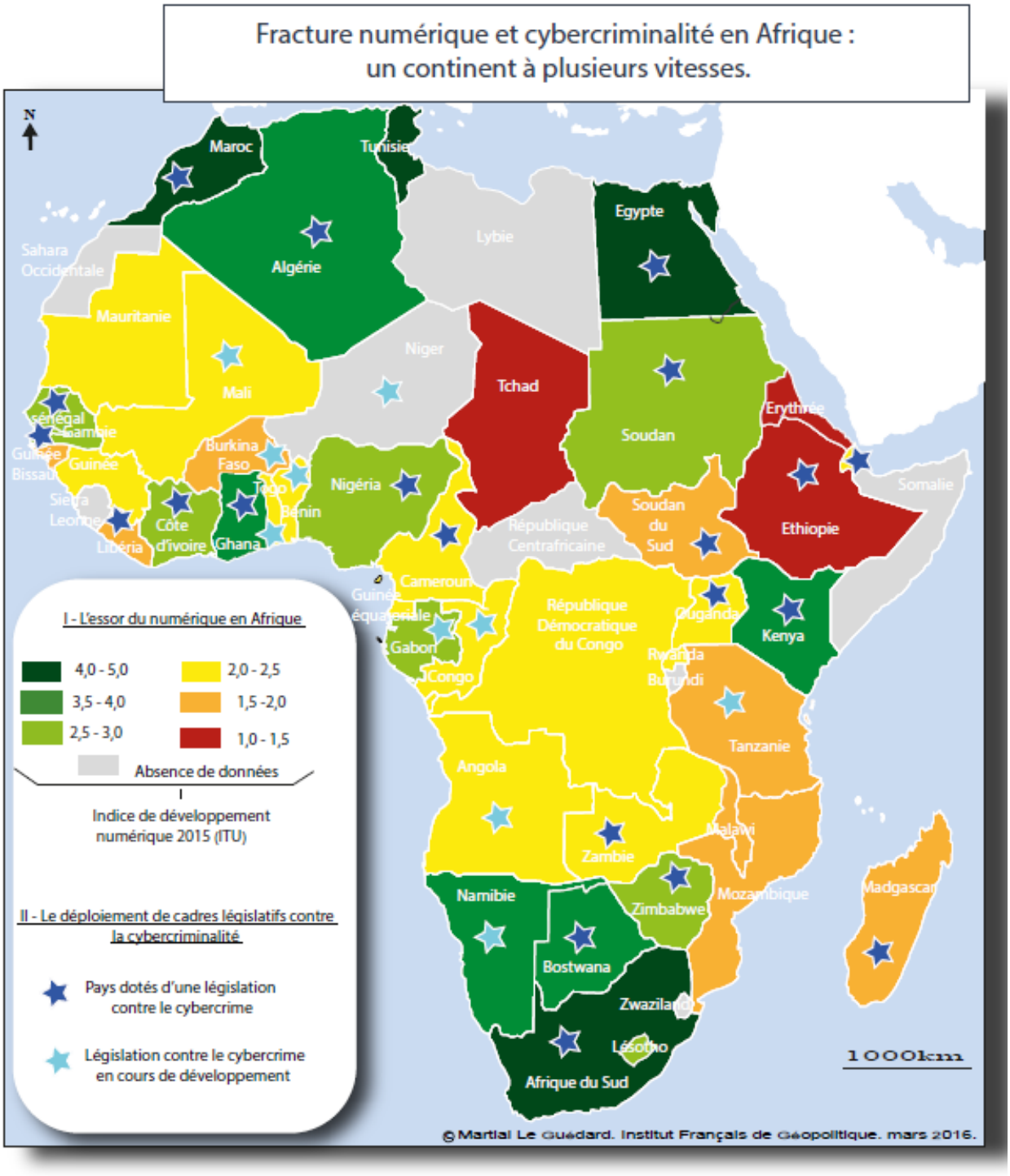
Pour l'Afrique, le défi est donc de faire face aux abus dans l'usage de cette connexion internet. L'escroquerie (ex. l'arnaque à la nigériane), les menaces terroristes (ex. Mauritania attacker), le cyberhacktivisme (ex. Anonymous Côte d'Ivoire, Anonymous Sénégal, Anonymous Africa ou Nigerian Cyber Army), la cyber contrefaçon ou encore l'usage d'internet pour porter atteinte à des valeurs supérieures (les contenus peuvent en effet être racistes, xénophobes, négationnistes ou bien encore des supports de pédopornographie), constituent autant d'exemples de risques inhérents à l'usage d'internet.

D'où un fort besoin de régulation notamment par la prévention et la répression en matière de cybersécurité. C'est aux Etats africains qu'il revient de circonscrire ces risques et de poursuivre les auteurs de cyberattaques. La dépendance croissante de l'Afrique à la « toile » rend l'intervention du législateur et la sensibilisation de la population à la sécurité informatique indispensables. Or, il ressort que la population africaine est peu sensibilisée à la sécurité et à l'hygiène informatiques. De manière générale, les réseaux informatiques utilisés ne disposent pas d'un niveau de sécurité raisonnable. Du côté des administrations, l'intranet utilisé dispose d'une ouverture sur internet et d'une sécurité moindre.

Conscients de ces problématiques croissantes, les gouvernements africains s'attèlent à renforcer leurs législations. Si le cyberespace est un espace de liberté, il ne saurait être un espace hors du champ de la loi. Dans cette optique, l'Union Africaine a créé la Convention de Malabo le 27 juin 2014. Cette convention africaine relative à la cybersécurité et la protection des données à caractère personnel, est ouverte exclusivement aux pays africains.[78] Elle représente une avancée considérable en termes de lutte contre la cybercriminalité en Afrique. Elle met en place des dispositions concernant trois grands sujets numériques : la lutte contre la cybercriminalité, la protection des données à caractère personnel et l'encadrement des transactions électroniques. Plus récemment, et à juste titre, le Sénégal a, le 30 mars 2016, par l'adoption du projet de loi autorisant la ratification de la Convention de Budapest (unique texte international de référence sur la cybercriminalité), témoigné d'une prise de conscience du caractère transfrontalier de la cybercriminalité.[79]

Au terme de l'analyse, il résulte que les politiques actuelles de cybersécurité des Etats d'Afrique sont mouvantes et en constante quête d'efficacité face à une connectivité mobile en plein essor favorisant l'émergence de nouvelles criminalités.

[76] L'essor du numérique en Afrique de l'Ouest : entre opportunités économiques et cybermenaces, Les notes stratégiques CEIS, Charlotte Gonzales, Julien Dechanet, Novembre 2015.
[77] https://www.sifaris.fr/cybercriminalite-lafrique-nouveau-far-west/
[78] http://www.afapdp.org/wp-content/uploads/2014/07/CONV-UA-CYBER-PDP-2014.pdf#sthash.ETVa2dtR.dpuf
[79] http://www.observatoire-fic.com/un-pas-decisif-du-senegal-vers-ladhesion-et-la-ratification-des-conventions-de-budapest-et-de-malabo/



Source : ICT Development Index 2015 ; UNCTAD/PRESS/PR/2015/004

1.5.2 Coopération régionale

Au niveau bilatéral, la coopération dans le domaine cyber reste insuffisante et le Ministre de l'économie numérique et de la poste ivoirien, Bruno Nabagné soulignait « la nécessité d'approfondir les coopérations bilatérales et multilatérales entre les pays pour une lutte efficiente »[80] lors de la 6ème édition de l'IT Forum Dakar du Sénégal.

[80] http://fr.allafrica.com/stories/201602260589.html

Au plan multilatéral, deux types de coopération ont émergé : d'une part des initiatives ad hoc permettant une prise de conscience des enjeux relatifs au numérique et à l'opportunité qu'il représente pour le continent, et d'autre part, des initiatives au sein d'enceintes existantes.
Suite à l'organisation par l'UNESCO, l'UIT, la Commission économique des Nations Unies pour l'Afrique (CEA), le CRDI et le Bellanet International, d'un colloque sur le thème du numérique et du développement en 1995, était lancée en 1996 « l'initiative Société africaine à l'ère de l'information (AISI) ». Des plans stratégiques au niveau national avaient vu le jour dans plus de 44 pays en 2011 afin de renforcer la capacité des pays africains à informatiser leurs sociétés et à proposer des services électroniques aux citoyens. Cependant la réussite de ces plans est évidemment liée à la volonté politique des Etats, ce qui explique encore les disparités africaines.[81]

Cette initiative AISI fut adoptée par l'Organisation de l'unité africaine (OUA), aujourd'hui Union africaine (UA). L'Union Africaine est le principal moteur du développement numérique en Afrique sur un spectre thématique bien plus large que le simple développement d'infrastructures puisqu'elle est aujourd'hui le moteur de réflexion et d'implantation de solutions de lutte contre la cybercriminalité, comme l'implantation de cadres législatifs et de CERT. Elle encourage fortement la coopération entre ses membres. L'UA est l'organisation la plus impliquée dans le développement du numérique et de cadres législatifs appropriés en partenariat avec d'autres organisations comme la Communauté économique des Etats de l'Afrique de l'Ouest (CEDEAO), ou encore la Communauté de développement d'Afrique australe (SADC), sous-régions dans lesquelles le numérique est en plein essor.

L'Union africaine s'appuie sur un cadre stratégique visant le développement socio-économique du continent : le Nouveau Partenariat pour le Développement de l'Afrique (NEPAD), qui a fait des technologies de l'information et de la communication une priorité dans son Plan d'action 2010-2015.[82] C'est dans ce cadre que l'Afrique de l'Ouest a vu s'accroître la coopération via l'Union Economique et Monétaire Ouest-Africaine (UEMOA) et la CEDEAO, qui ont adopté une législation harmonisée en matière de télécommunications et de technologies de l'information et de la communication. On peut noter que le Sénégal, pays moteur pour la région, est aussi en charge du volet Technologies de l'Information et de la Communication du NEPAD.

L'Afrique de l'Est et du Sud (COMESA) et la SADC ont également amorcé des efforts dans ce sens.[83] Cependant, si l'Union Africaine englobe 53 pays sur les 54 qui composent l'Afrique, puisque seul le Maroc n'en fait pas partie, elle ne possède pas de pouvoir de coercition : elle engendre de la *Soft Law*, des normes n'ayant pas de caractère obligatoire et reposant sur une base volontaire et non-contraignante. Les Etats restent donc maîtres de leur politique numérique. Ainsi, si l'UA a adopté une convention sur la cybercriminalité, pour *Géopolitique Africaine*, « l'harmonisation des sanctions pénales se heurte à la souveraineté des États ; les dispositifs de coopération pèchent par des lacunes »[84].
En matière de coopération multilatérale ad hoc, le continent dispose de l'*African Forum of Computer Incident Response Teams* (AfricaCERT) qui regroupe le Burkina-Faso, le Cameroun, la Côte d'Ivoire, l'Egypte, le Ghana, le Kenya, l'île Maurice, le Maroc, l'Afrique du Sud, le Soudan et la Tunisie. La coopération est fondée sur l'échange d'informations et la participation à des exercices communs, entre membres, mais aussi en partenariat avec l'APCERT, l'*Asia-Pacific Computer Emergency Response Team* qui regroupe l'Australie, Brunei, la Chine, la Corée du Sud, Hong Kong, l'Inde, l'Indonésie, le Japon, la Malaisie, les Philippines, Singapour, Taiwan, la Thaïlande, et le Vietnam. L'Organisation de la coopération islamique des CERTs regroupe quant à elle 27 pays d'Afrique.
Enfin, la Banque Africaine de Développement fournit une aide financière importante à certains Etats (Algérie, Burkina-Faso, Cameroun, Côte d'Ivoire, Lesotho, Mali, Tunisie, Afrique du Sud) souhaitant développer des projets liés aux TICs.

1.5.3 L'Afrique et le reste du monde

En décembre 2015, le Président chinois Xi Jinping, en visite en Afrique, faisait part de sa volonté d'opérer un rapprochement entre la Chine et l'Afrique et annonçait une aide chinoise de 60 milliards de dollars,

[81] Destiny Tchehouali. Les politiques et actions internationales de solidarité numérique à l'épreuve de la diffusion des TIC en Afrique de l'Ouest : bilan et perspectives. Histoire. Université Toulouse le Mirail - Toulouse II, 2013. Français. <NNT : 2013TOU20020>. <tel-00879871>
[82] http://www.nepad.org/fr/about
[83] Destiny Tchehouali. Les politiques et actions internationales de solidarité numérique à l'épreuve de la diffusion des TIC en Afrique de l'Ouest : bilan et perspectives. Histoire. Université Toulouse le Mirail - Toulouse II, 2013. Français. <NNT : 2013TOU20020>. <tel-00879871>
[84] http://www.geopolitique-africaine.com/la-cooperation-une-necessite-absolue-pour-lutter-contre-la-cybercriminalite_987789.html

notamment sous la forme de prêt sur trois ans, afin de développer le continent, via le financement d'infrastructures et l'éducation. Le plan d'action de Johannesburg 2016-2018 qui en résulte doit permettre d'encourager les « entreprises et institutions financières chinoises à élargir l'investissement sous forme de partenariats public-privé (PPP) ou de Build-Operate-Transfer (BOT) pour soutenir les pays africains et les projets pilotes, notamment le Programme de Développement des Infrastructures en Afrique (PIDA) et l'Initiative Présidentielle pour Promouvoir l'Infrastructure (PICI) »[85]. Il s'agit aussi de travailler en partenariat avec les organisations internationales comme l'Union internationale des Télécommunications pour «réduire le fossé numérique en Afrique et y promouvoir la construction de la société de l'information »[86].
Dans le même temps, la Chine et les Etats africains s'engagent à «se soutenir mutuellement dans les enceintes internationales et à renforcer la coopération »[87]

Plusieurs pays africains sont actifs au sein d'autres instances internationales, notamment de l'Organisation des Nations-Unies. Ainsi, l'Egypte, le Ghana et le Kenya ont participé aux travaux du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité nationale qui a rendu son rapport en juin 2015.
Le Sénégal, qui se veut être un pays moteur en Afrique de l'Ouest dans la promotion des technologies numériques, a intégré le conseil de l'Union Internationale des Télécommunications (UIT) en 2014 avant d'être désigné comme coordinateur et porte-parole du groupe Afrique en 2015, et ce jusqu'en 2018. L'UIT collabore par ailleurs avec l'Union africaine pour l'instauration d'une Convention sur la cybersécurité via le projet d'Appui à l'Harmonisation des Politiques sur les TICs en Afrique Subsaharienne (HIPSSA) qui vise au rapprochement des législations. L'UIT travaille également à la mise en place de CERT (Computer Emergency Response Team) : 15 pays sur 54 disposent actuellement d'un CERT opérationnel.[88]

A propos des relations entre l'Afrique et l'Europe, notons que peu de pays du continent africain ont ratifié la Convention de Budapest sur la lutte contre la cybercriminalité : l'Afrique du Sud, le Maroc et le Sénégal uniquement. Les positions de plusieurs pays africains et européens se rejoignent, notamment sur la question de la régulation des activités des Etats dans le cyberespace en temps de paix ou sur la nécessité d'un certain contrôle souverain des Etats du cyberespace. Dans le second cas, d'importantes divergences existent néanmoins, notamment sur la question de la gestion des contenus et de la censure.
Il n'existe pas d'unité régionale forte tant au plan géopolitique traditionnel que sur les sujets d'intérêt cyber, même si les organisations internationales poussent les Etats à une prise de conscience. Cette incitation semble aujourd'hui porter ses fruits à l'image du dynamisme que l'on peut observer notamment en Afrique de l'Ouest.

1.6 Amérique du Nord

1.6.1 Niveau de maturité

Les taux de pénétration Internet varient largement selon les pays. Sont logiquement en tête les pays à hauts revenus, tels que les Etats-Unis (87.4%) et le Canada (92.5%)[89]. Arrivent ensuite les pays à revenus intermédiaires comme le Mexique (49.3%) et le Panama (52.0%). Le groupe de queue comprend enfin les pays possédant des infrastructures de télécommunication peu développées, et donc un taux de pénétration relativement faibles comme le Guatemala (31,5%), le Honduras (27.4%), le Nicaragua (27.1%) ou Cuba (28%).
Le Costa Rica, pays à revenus intermédiaire, fait figure d'exception avec un fort taux de pénétration Internet de 88%.
L'Amérique du Nord a le privilège d'abriter sur son sol un acteur majeur de l'internet dont le statut est régulièrement remis en question au niveau mondial: l'ICANN (Internet Corporation for Assigned Names and Numbers), autorité de régulation de l'internet ayant son siège en Californie.[90]

[85] http://www.fmprc.gov.cn/fra/wjdt/gb/t1323180.shtml
[86] http://www.fmprc.gov.cn/fra/wjdt/gb/t1323180.shtml
[87] Ibidem.
[88] L'essor du numérique en Afrique de l'Ouest : entre opportunités économiques et cybermenaces, Les notes stratégiques CEIS, Charlotte Gonzales, Julien Dechanet, Novembre 2015.
[89] http://data.worldbank.org/about/country-and-lending-groups#North_America
[90] https://www.icann.org/fr

1.6.2 Coopération régionale

La coopération régionale est principalement le fait des Etats les plus développés, Etats-Unis et Canada, qui ont signé de nombreux d'accords relatifs à la cyberdéfense. Outre les échanges traditionnels entre membres des « Fives Eyes », le NORAD (North American Aerospace Defense Command), organisme militaire binational créé officiellement en 1958 par les deux pays pour surveiller et défendre l'espace aérien nord-américain,[91] joue aujourd'hui un rôle en matière de cyberdéfense[92]. Il s'appuie pour cela sur le Centre Commun Cyber (*Joint Cyber Centre*)[93] mis en place en mai 2012 et dont les 3 principales missions sont[94] :

- Améliorer "la perception situationnelle" du domaine cybernétique afin de mieux l'intégrer dans les missions des états-majors ;
- Améliorer la protection et la défense des réseaux informatiques des différents commandements ;
- Renforcer les capacités collectives afin de fournir un soutien rapide, efficace et approprié aux autorités civiles.

Les autres pays n'ont que peu de relations sur les thèmes de la cyberdéfense en raison de leur faible maturité sur le sujet. Mais la situation change progressivement. Le président mexicain Enrique Peña Nieto a ainsi lancé fin 2014 le *National Security Program (2014-2018)*[95]. Objectif : développer une véritable politique de cybersécurité afin de protéger et défendre les intérêts nationaux, ou développer d'autres structures gouvernementales ces dernières années. L'Organisation des Etats américains (*Organization of American States*) essaye aussi de jouer un rôle important dans la promotion de la cybersécurité pour les pays membres. Un accord a par exemple été signé en 2015 entre l'OAS et FIRST (*Forum of Incident Response and Security Teams*) pour coopérer sur la promotion de la culture « cybersécurité » et la mise en place de mesures pour améliorer les réponses aux incidents dans les pays membres. Des études sont aussi réalisées par l'OAS sur la prise en compte de la cybersécurité par les Etats membres[96].

Par ailleurs, les Etats-Unis, le Canada et le Mexique font partie d'un accord de coopération trilatérale de défense (Trilateral Defense Cooperation), comportant un volet cyberdéfense. Ils coopèrent notamment sur l'amélioration de l'évaluation de la cybercriminalité et le partage d'informations concernant les défis de cyberdéfense.[97]

Du côté de la coopération public/privé, il faut noter qu'en mai 2014, Microsoft et la police fédérale mexicaine ont signé un accord de coopération commerciale afin d'adopter des mesures de lutte contre la cybercriminalité en Mexique.[98]

1.6.3 Relations Amérique du Nord / reste du monde

Outre la coopération traditionnelle avec les autres pays membres des *Five Eyes* (Canada, Australie, Nouvelle-Zélande, Royaume-Uni), les Etats-Unis contrôlent aujourd'hui les organes chargés de la gestion d'Internet comme l'ICANN et sont très présents dans les comités internationaux de normalisation de l'Organisation Internationale de Normalisation (ISO). De leur côté, les autres pays de la Région cherchent de plus en plus à faire appel à des pays extérieurs pour s'affranchir du parapluie « cyber » américain. Le Mexique a ainsi lancé différents projets avec le Royaume-Uni pour améliorer ses capacités et lancer des programmes de recherche conjointe[99].
Une grande partie des pays d'Amérique du nord ont signé la Convention de Budapest du 23 novembre 2001 relative à la lutte contre la cybercriminalité qui prévoit des dispositions pour le renforcement de la coopération entre les pays signataires. Ainsi, l'adhésion à cette Convention de Budapest représente une avancée importante de la part notamment des pays émergents de l'Amérique du Nord tel que le Mexique en termes de volonté de coopération avec le reste du monde. Cette Convention a mis en place des programmes d'aide à destination des pays émergents ne disposant pas d'infrastructures adéquats à la lutte contre la cybercriminalité

[91] https://www.hsaj.org/articles/8038
[92] http://blogs.wsj.com/washwire/2014/12/24/u-s-prepared-to-defend-santa-tracker-from-cyber-attacks/
[93] http://www.northcom.mil/Newsroom/tabid/3104/Article/563711/norad-usnorthcom-joint-cyber-center-stands-up.aspx
[94] http://si-vis.blogspot.fr/2012/06/creation-du-joint-cyber-center-jcc-nord.html
[95] https://www.pwc.com/mx/es/knowledge-center/archivo/20150917-kc-cybersecurity.pdf
[96] http://www.iadb.org/en/news/news-releases/2016-03-14/cybersecurity-in-latin-america-and-the-caribbean,11420.html
[97] http://www.globalresearch.ca/the-north-american-security-framework-expanded-trilateral-defense-cooperation/5383285
[98] https://www.pwc.com/mx/es/knowledge-center/archivo/20150917-kc-cybersecurity.pdf
[99] https://www.gov.uk/government/world-location-news/cyber-security-capacity-building-programme-2015-16

afin de contribuer à l'amélioration des capacités d'enquête sur la cybercriminalité et d'accroître en parallèle la coopération entre les pays signataires.[100]
Par ailleurs, le Mexique est membre de l'OEA (Organisation des Etats Américains), organisation qui rassemble l'ensemble des Etats américains afin de fixer des politiques sur des grands sujets tel que cybersécurité. En effet, en avance par rapport à d'autres ensembles de pays (notamment l'Union européenne), les Etats membres de l'OEA ont mis en place une politique de cybersécurité en 2004. Cette organisation a également élaboré une déclaration sur « Le renforcement de la cybersécurité aux Etats-Unis » en mars 2012, preuve de la volonté des Etats membres de contribuer à faciliter la coopération et le partage d'informations au sein de l'OEA.[101]

1.7 Amérique du Sud

1.7.1 Niveau de maturité

Le Brésil s'impose comme la puissance dominante de la région, y compris sur les questions numériques alors que le pays est loin d'être le mieux connecté avec un taux de pénétration de 57,6%. Arrivent en tête l'Equateur (84,9%), l'Argentine (80,1%) et le Chili (72,3%). Le peloton de queue est constitué par la Bolivie (39%), le Suriname (41,4%) et le Paraguay (43%). Il convient cependant de relativiser l'importance de ces données au regard de la population du Brésil qui représente à elle seule la moitié de la population d'Amérique du Sud.
Malgré la forte disparité des taux de pénétration, la plupart des pays ont développé des mécanismes de gouvernance pour assurer le développement des TIC, de législations appropriées ou de mécanismes de lutte contre la cybercriminalité. Un volontarisme qui s'est nettement accentué à la suite des révélations Snowden qui ont entrainé un véritable rejet de l'Internet américano-centré en Amérique du Sud, plus particulièrement au Brésil.
Le Brésil est à la fois la première victime et le premier acteur de la cybercriminalité dans la région, avec un écosystème criminel qui est l'un des plus virulents de la planète et qui a longtemps profité d'une législation défaillante sur le sujet.
Au-delà de la cybercriminalité, les cybermenaces sont cependant multiples (espionnage, conflits interétatiques, hacktivisme politique…) et ne se cantonnent pas qu'au Brésil. En février 2014, les experts de Kaspersky Lab découvraient une vaste campagne mondiale de cyberespionnage, baptisée The Mask (« Careto » en espagnol), qui ciblait des institutions gouvernementales, des bureaux diplomatiques et des ambassades, des compagnies pétrolières et gazières, des organismes de recherche et des militants. Si de nombreux pays furent infectés par le malware multiplateforme Careto qui fut actif pendant 7 ans, les soupçons portent encore aujourd'hui sur une origine étatique.[102]
La région a donc encore fort à faire pour relever les nombreux défis lui permettant d'assurer le développement de son cyberspace.

1.7.2 Coopération régionale

La coopération entre les pays d'Amérique du Sud est largement dominée par des facteurs géopolitiques traditionnels, mais aussi par la volonté de se donner les moyens de faire face à la dépendance technologique de la région. Plus de 90% du trafic Internet de la région passe en effet par des opérateurs nord-américains et 85% des contenus digitaux de la région sont stockés aux Etats-Unis, ce qui en fait la région la plus dépendante des Etats-Unis pour son accès au cyberespace[103].
La coopération dans le domaine de la cybersécurité se traduit par, d'une part, par des accords stratégiques traditionnels entre Etats alliés. C'est notamment le cas de l'Argentine et du Brésil, qui cherchent depuis les révélations Snowden à améliorer conjointement leurs capacités de cyberdéfense, et, d'autre part, par des accords entre les autorités judiciaires et les forces de police. Ces accords bilatéraux sont principalement fondés

[100] https://www.pwc.com/mx/es/knowledge-center/archivo/20150917-kc-cybersecurity.pdf
[101] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends-and-government-responses.pdf
[102] http://www.kaspersky.com/about/news/virus/2014/Kaspersky-Lab-Uncovers-The-Mask-One-of-the-Most-Advanced-Global-Cyber-espionage-Operations-to-Date-Due-to-the-Complexity-of-the-Toolset-Used-by-the-Attackers
[103] http://www.cubadebate.cu/opinion/2015/06/06/es-urgente-integrarnos/#.VyCs8XrXh1Q

sur les relations traditionnelles entre Etats. Ainsi, la *Comunidad de Policias de América* (AMERIPOL) a mis en place depuis août 2014 un *Centro de Ciberseguridad* pour renforcer la coopération entre les différentes polices sud-américaines, notamment par le partage d'information entre agences de renseignements. Ces échanges se révèlent cependant difficiles dans la pratique et l'action du Centre est encore limitée.[104]
Au plan multilatéral, les organisations les plus impliquées sont l'Union des Nations Sud-américaines (UNASUR) et l'Organisation des Etats Américains (OEA). L'UNASUR, organisation intergouvernementale regroupant les deux unions douanières que sont le Marché commun du Sud (Mercosur) et la Communauté andine (CAN), s'est construite en s'inspirant de l'Union européenne. Son objectif principal est la construction « d'une identité et d'une citoyenneté sud-américaine et le développement d'un espace régional intégré »[105]. Elle regroupe 12 pays (Argentine, Bolivie, Brésil, Chili, Colombie, Equateur, Guyane, Paraguay, Pérou, Suriname, Uruguay, Vénézuela) et a lancé en 2012 une initiative visant à promouvoir la cybersécurité entre les Etats membres. Un projet d'amélioration de la connectivité via la fibre optique a également été lancé en 2014[106].
L'Organisation des Etats Américains (OEA) est une organisation régionale qui regroupe les 35 pays indépendants des Amériques. En 2004, dans le cadre du *Programa de Seguridad Cibernética* a été adoptée une résolution pour l'élaboration d'une stratégie de cybersécurité pour combattre les cybermenaces. Cette dernière a été complétée par une déclaration de mars 2012 portant sur le renforcement de la cybersécurité en Amérique du Sud.
Une stratégie qui est portée par le *Comité Interamericano contra el Terrorismo* (CICTE) dont l'objectif est le développement capacitaire, mais aussi la reconnaissance d'une responsabilité à l'échelle nationale comme régionale en matière de cybersécurité. L'OEA entend ainsi promouvoir le développement de stratégies nationales de cybersécurité et d'une culture forte en matière de cybersécurité. L'un des objectifs était notamment la mise en place de CERT et la région compte aujourd'hui 10 pays (Argentine, Bolivie, Brésil, Chili, Colombie, Equateur, Guyane, Paraguay, Pérou, Venezuela) doté d'au moins un centre.[107] Le département de la coopération judiciaire de l'institution a ainsi développé un portail de coopération en matière de délit cybernétique pour faciliter et renforcer la coopération judiciaire grâce au partage d'information entre gouvernements.[108] Un observatoire de la cybersécurité en Amérique Latine et aux caraïbes[109] permettant d'évaluer la maturité des pays de la région en matière de cybersécurité a également été mis en place. La Banque Interaméricaine de Développement (BID) est le partenaire officiel de l'OEA dans son action en faveur de la cybersécurité dans la région. Dans un rapport de 2016, l'OEA et la BID mettent l'accent sur les vulnérabilités « potentiellement dévastatrices » des pays de l'Amérique latine avec quatre pays sur les cinq qui ne disposent pas de stratégie de cybersécurité. Ils encouragent les pays d'Amérique latine et les Caraïbes à intensifier leurs efforts en matière de cybersécurité.[110]

On peut enfin souligner le rôle du Latin America and Carribean Network Centre (LACNIC) qui collabore avec l'OEA et les CERTs nationaux de la région pour la sécurité du réseau.

1.7.3 L'Amérique du Sud et le reste du monde

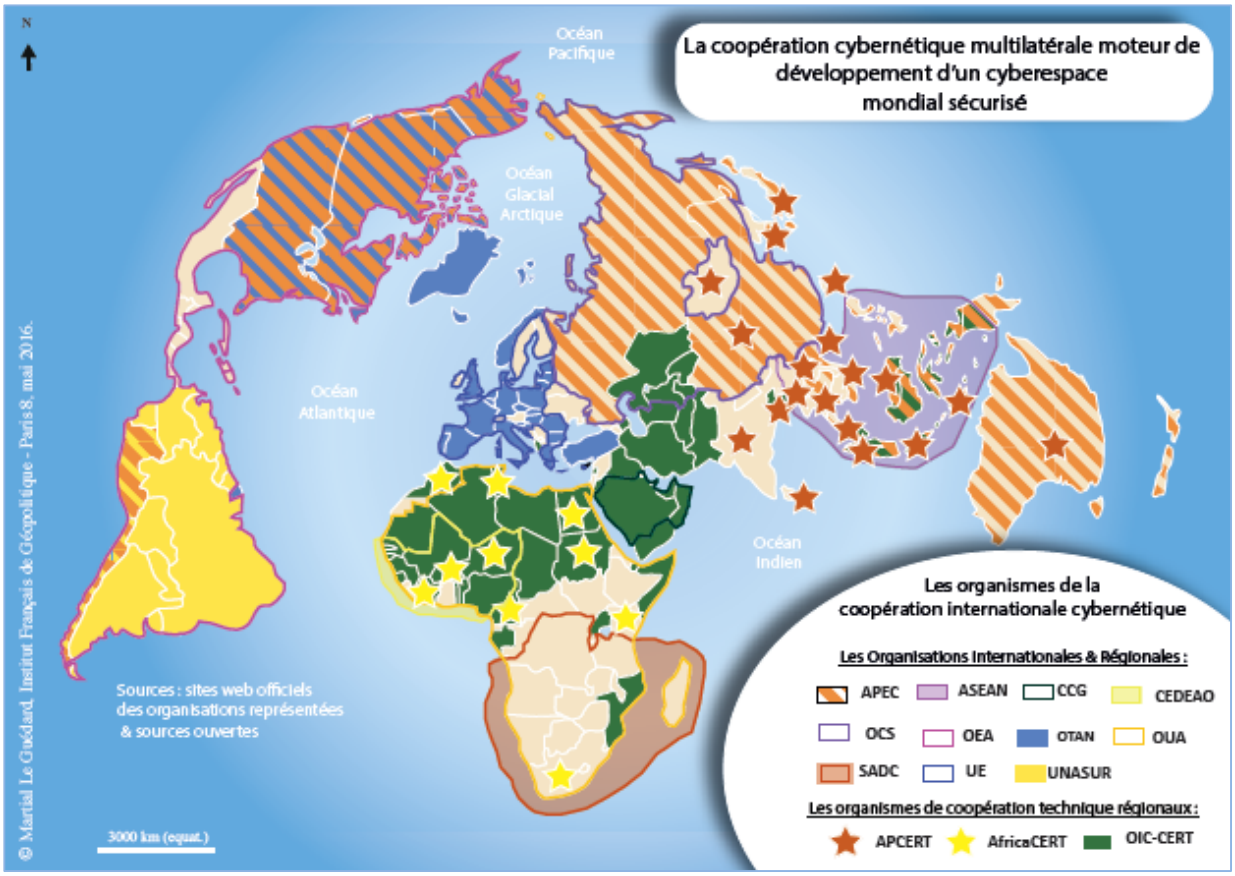
Différents accords bilatéraux relatifs à la cyberdéfense ont également été signés, à l'exemple du Brésil ou du Chili qui ont renforcé leur coopération militaire avec les Etats-Unis en avril 2012, c'est à dire avant que les révélations Snowden ne viennent bouleverser la donne et réorienter cette coopération vers les autres pays du « Sud ».
Concernant les relations Amérique du Sud/Europe, notons qu'aucun pays d'Amérique du Sud n'a ratifié la Convention de Budapest sur la lutte contre la cybercriminalité, bien que les positions de certains pays d'Amérique du Sud et d'Europe se rejoignent sur certains sujets, notamment sur la nécessité d'un certain contrôle souverain des Etats du cyberespace. Cela n'a pas empêché AMEROPOL et EUROPOL de renforcer depuis 2014 leur coopération afin de lutter contre le crime organisé, et notamment le cybercrime.[111] De plus, le Brésil, qui a rapidement pris des mesures suite aux révélations sur la surveillance de masse exercée par la NSA, a obtenu l'appui de certains Etats européens : l'Allemagne a ainsi soutenu aux côtés du Brésil une motion en faveur de la défense de la vie privée en ligne fin 2013. Les projets de câbles sous-marins Sud-Sud se

[104] Paul-Edouard Martin, *Inseguridad cibernética en América Latina : lineas de reflexion para la evaluacion de riesgos*, Instituto Espanol de Estudios Estratégicos, 2015.
[105] http://www.comunidadandina.org/unasur/tratado_constitutivo.htm
[106] David Ramírez Morán, *La Vision internacional de la ciberseguridad*, Instituto Espanol de Estudios Estratégicos, 2015.
[107] https://www.sites.oas.org/cyber/Es/Paginas/default.aspx
[108] http://www.oas.org/juridico/spanish/cybersp.htm
[109] http://observatoriociberseguridad.com/graph/countries/selected/0/dimensions/1-2-3-4-5
[110] http://www.iadb.org/en/news/news-releases/2016-03-14/cybersecurity-in-latin-america-and-the-caribbean,11420.html
[111] https://www.europol.europa.eu/newsletter/europol-and-ameripol-strengthen-cooperation-against-organised-crime

multiplient en effet même si la crise économique qui a frappé les Etats de la Région a conduit à leur suspension, voire à leur annulation comme celui du câble BRICS.

Sur la scène internationale, plusieurs pays d'Amérique du Sud sont actifs au sein d'autres instances internationales, notamment de l'Organisation des Nations unies. Le Brésil et la Colombie ont ainsi participé aux travaux du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité nationale qui a rendu son rapport en juin 2015. La place et le rôle du Brésil dans les relations entre l'Amérique du Sud et les autres parties du monde est primordiale pour la région. Le pays a en effet su faire entendre sa voix sur la scène internationale et représente véritablement la position des pays émergents du Sud face aux Etats-Unis.

1.8 Cartographie des organismes internationaux engagés dans la promotion et la sécurisation du cyberespace



2 ANALYSE PAYS

Dans la seconde partie du rapport, une analyse a été réalisée sur cinq pays définis par le pilote de l'étude. Pour chaque pays, l'analyse se divise en deux parties :

- *Une présentation des différentes données du pays. Elles sont basées sur le portail de l'Observatoire du Monde Cybernétique, qui est mis à jour toute l'année selon les rapports, déclarations officielles ou actualité ;*
- *Basée sur ces données, une analyse sur le pays est réalisée sur différents thèmes : perception des menaces globales et cybernétiques, enjeux numériques du point de vue technologique, politique, économique et militaire.*

2.1 CHINE

L'Australian Strategic Policy Institute émet chaque année un classement[112] en fonction de la maturité cybernétique des pays de la région Asie-Pacifique. La Chine arrive à la huitième place en 2015. Avec une population d'environ 1,37 milliard, la Chine est le pays le plus peuplé au monde. Elle occupe depuis 2010 le 2ème rang mondial par son PIB. Malgré un taux de connectivité de seulement 42%, la place de la Chine dans le monde numérique est critique.

2.1.1 Perception des menaces globales et cyber

Vues côté chinois, les menaces cybernétiques sont intimement liées aux menaces plus traditionnelles bien qu'elles s'expriment différemment. La menace en matière informationnelle est à la fois intérieure et extérieure. Dès l'arrivée d'Internet sur son territoire, le régime a détecté les menaces que pouvait représenter le développement d'Internet via l'accès à l'information qu'il procure et les moyens de communication qu'il offre. Le gouvernement chinois s'est donc saisi très tôt de cette question en adoptant plusieurs mesures dont le développement de réseaux et plateformes de communications nationaux (Baidu, Weibo, WeChat, QQ). L'objectif était que les citoyens utilisent des réseaux et plateformes chinois, plus faciles à surveiller et à contrôler, plutôt que des outils étrangers, principalement américains. Des patrouilles du net ont également été créées pour traquer les comportements jugés contraires à l'ordre public sur Internet. De plus, l'arsenal juridique a été adapté pour ériger en infraction les comportements non-souhaités par le parti communiste chinois. La censure a donc pour objectif d'empêcher les actions collectives en supprimant les messages qui pourraient mener à une mobilisation sociale, quelle que soit la thématique choisie[113]. La menace est également externe par les tentatives répétées de certains Etats, notamment occidentaux, de recourir à Internet pour influencer les populations. Pour y faire face, les autorités chinoises ont mis en place une véritable muraille du net grâce à des techniques de filtrage avancées.

La deuxième cybermenace perçue par la Chine concerne la sécurité de ses réseaux et systèmes d'informations. La Chine est extrêmement vulnérable aux cyberattaques en raison de la multiplication de ses réseaux (et de leur place dans son économie) et de leur faible protection. Elle affirme ainsi régulièrement qu'elle est la première victime des cyberattaques. On dispose cependant de peu d'informations sur ces attaques, les autorités chinoises ne les détaillant que rarement, ce qui rend toute analyse très compliquée. En revanche, il est possible d'affirmer que les attaques viennent à la fois de l'extérieur de la Chine mais également de l'intérieur. La rhétorique chinoise face aux attaques américaines et les accusations d'espionnage sont courantes et font état d'une stratégie politique visant, entre autre, à contrer l'influence américaine dans la

[112] https://www.aspi.org.au/publications/cyber-maturity-in-the-asia-pacific-region-2015/Cyber-Maturity-2015.pdf
[113] Gary KING, Jennifer PAN, Margaret E. ROBERTS, "How censorship in China allows government criticism but silences collective expression", *American Political Science Review*, mai 2013, 18p., disponible sur http://gking.harvard.edu/files/gking/files/censored.pdf?m=1367505213

région et à pousser de nouveaux sujets dans les enceintes internationales. Quelle que soit l'origine des attaques, *« l'Internet est au cœur de la croissance économique, de la sécurité nationale et de la stabilité du régime. L'absence de cybersécurité représente dès lors une menace majeure »*[114].

2.1.2 Les enjeux numériques pour la Chine

Les enjeux numériques technologiques et économiques

Dans plusieurs domaines industriels, la Chine a développé et soutenu des industries afin d'en faire des champions nationaux, sur le marché chinois et à l'exportation. Pour ce faire, elle a largement soutenu les entreprises via des aides financières directes et en leur facilitant l'accès au crédit. Le domaine des technologies de l'information et des communications n'a pas échappé à cette stratégie. Vis-à-vis des autres Etats, les enjeux sont liés au développement des exportations des produits chinois. Face à une concurrence principalement dominée par les Etats-Unis, la Corée et le Japon, la Chine peut se targuer d'avoir des entreprises très présentes à l'export : Huawei, Datang, Alibaba, ZTE et Lenovo pour n'en citer que quelques-unes.

Cependant, cette montée en puissance des entreprises chinoises s'est heurtée à une résistance de la part de certains Etats. Courant 2012, un mouvement hostile aux produits chinois s'est ainsi développé dans plusieurs pays pour dénoncer le manque de sécurité des produits chinois. Pire, ces produits possèderaient selon leurs détracteurs des *backdoors* permettant au Gouvernement chinois d'espionner les utilisateurs et de récupérer de l'information. Pour faire face à ces risques présumés, le sénateur Jean-Marie BOCKEL a proposé dans un rapport parlementaire *« d'interdire sur le territoire national et européen le déploiement et l'utilisation de routeurs ou équipements de cœur de réseaux qui présentent un risque pour la sécurité nationale, en particulier les routeurs et autres équipements informatiques d'origine chinoise »*[115]. Aux Etats-Unis, les entreprises chinoises Huawei et ZTE ont également dû, à l'automne 2012, s'expliquer sur les accusations d'espionnage devant la Commission du renseignement de la Chambre des représentants présidée par Mike Rogers. Le Sénat et la Chambre des représentants ont quelques mois plus tard voté une loi interdisant à certaines agences ou organismes gouvernementaux d'acheter des équipements informatiques chinois avec des fonds publics sans vérification préalable de leur sécurité par le FBI[116]. Le rapport Mandiant[117] publié début 2013 sur une unité de cyberespionnage chinoise viendra appuyer les décideurs politiques dans leurs convictions et renforcer leur argumentaire. La Chine et les entreprises chinoises ont toujours contesté ces accusations.

Il ne faut cependant pas se méprendre sur les raisons de ce mouvement. S'il obéit à des préoccupations de sécurité, il s'explique aussi par des motivations économiques, les gouvernements occidentaux souhaitant défendre leur base industrielle et technologique face à la domination progressive du marché des technologies de l'information et de la communication par les entreprises chinoises.

Les révélations Snowden à partir de juin 2013 sont venues changer la donne, les Etats-Unis et les entreprises américaines étant à leur tour pointées du doigt pour leurs opérations de surveillance de masse et leur coopération avec le gouvernement. Ces révélations ont incontestablement servi les entreprises chinoises dans la conquête de nouveaux marchés. Elles leur ont également offert l'opportunité de redorer leur image après les accusations de 2012 et 2013.

Au plan interne, les autorités chinoises ont depuis plusieurs années adopté une politique de soutien à l'industrie des technologies de l'information et de la communication. Le plan quinquennal annoncé en 2011[118] faisait du secteur l'une de ses sept priorités avec pour objectifs le développement de nouvelles infrastructures, d'un Internet de nouvelle génération ainsi que le renforcement de la sécurité des réseaux et de l'information. En mars 2015, lors du congrès du Parti, le Premier ministre a annoncé deux initiatives en ce sens : « Made in China 2025 » et « Internet Plus »[119]. Cette dernière vise à intégrer Internet dans les industries plus traditionnelles. D'ici à 2025, l'objectif est celui d'un nouveau modèle économique source de revenus importante grâce au *big data*, au *cloud computing* ou encore à l'Internet des objets. C'est donc une industrie très fortement subventionnée qui va être développée. Il s'agit pour la Chine de créer de nouvelles richesses, y compris à l'intérieur de son territoire, et de continuer la transformation de son industrie. Enfin, notons que celle-ci passe également par la mise en place de nouvelles normes imposant aux entreprises étrangères de se soumettre à un certain nombre de contraintes si celles-ci souhaitent s'implanter en Chine. Ainsi, sous couvert de lutte contre le terrorisme, le gouvernement chinois exige des entreprises l'accès aux données chiffrées.

[114] Chaire Castex de cyberstratégie, *Géopolitique du cyber en Asie*, Etude réalisée avec le soutien de la Direction aux Affaires Stratégiques, septembre 2014, p.13
[115] J-M BOCKEL, Rapport d'information sur la cyberdéfense, juillet 2012, p.127, disponible sur http://www.senat.fr/rap/r11-681/r11-6811.pdf
[116] Pour plus d'explications voir Chaire Castex de cyberstratégie, *Géopolitique du cyber en Asie*, *op. cit.*, p.22
[117] http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf
[118] http://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Publicationseries/5-years-plan/Documents/China-12th-Five-Year-Plan-Overview-201104.pdf
[119] http://english.gov.cn/policies/latest_releases/2015/07/04/content_281475140165588.htm

L'intérêt économique transparaît dans cette disposition dans la mesure où l'espionnage économique est ainsi facilité.
La Chine multiplie donc les initiatives pour d'une part progresser et d'autre part connecter son territoire. Si aujourd'hui les grandes entreprises chinoises telles que Baidu (moteur de recherche en mandarin) ou Alibaba (site internet de commerce électronique) côtées au Nasdaq, sont essentiellement tournées vers le seul marché interne, l'hypothèse de l'ouverture future vers l'extérieur n'est pas à exclure.
Compte tenu du taux moyen de connectivité, les perspectives économiques, parmi lesquelles le e-commerce, sont importantes sur le territoire chinois. Face à un taux de croissance en baisse depuis quelques années, il s'agit donc d'un enjeu majeur pour le pays.

Les enjeux numériques politiques[120]

La montée en puissance de la Chine dans le cyberespace s'est toujours accompagnée d'une farouche volonté d'affirmer sa souveraineté dans cet espace. Ainsi, son livre blanc *The Internet in China* publié le 8 juin 2010 proclame qu'à *« l'intérieur du territoire chinois, Internet est soumis à la souveraineté chinoise. La souveraineté de la Chine sur Internet devrait être respectée et protégée. Les citoyens de la République populaire de Chine et les citoyens étrangers, personnes privées et organisations, ont le droit et la liberté d'utiliser Internet sur le territoire chinois ; dans le même temps, ils doivent obéir aux lois et régulations chinoises et protéger la sécurité d'Internet de façon consciencieuse »*[121]. La souveraineté est un attribut spécifique et unique des Etats et constitue donc la source de son pouvoir illimité et suprême. La Chine a plusieurs fois revendiqué sa souveraineté sur « son » cyberespace, comme lors d'une conférence de presse du porte-parole du ministre des affaires étrangères en février 2015 (*« … the Chinese side believes that all countries have the right to administer the cyberspace in accordance with the law and the cyber sovereignty of all countries should be respected and maintained »*[122]) ou lors du sommet de Wuzhen[123] le 16 décembre 2015. A ce titre, les dirigeants chinois rappellent régulièrement les corollaires de l'égalité souveraine des Etats et notamment la non-ingérence dans les affaires intérieures : la Chine est donc libre de réguler, comme elle le souhaite, Internet sur son territoire, tandis que les autres Etats ne devraient pas utiliser ce moyen pour tenter d'influencer la population.
Si elle affirme son engagement pour un cyberespace sûr, pacifique et ouvert, la Chine entend bien continuer à faire appliquer son droit sur son territoire et sur les personnes y résident, y compris sur la question de la liberté d'expression et de la censure. Pour faire face aux critiques, les autorités chinoises ont habilement invoqué l'article 19 du Pacte international relatif aux droits civils et politiques qui dispose que la liberté d'expression peut être limitée dans un certain nombre de cas. Bien qu'ayant une interprétation extensive de ces limites, la Chine inscrit son action dans le droit international pour faire taire les affirmations selon lesquelles la censure sur Internet serait illicite. La mise en place de mesures technico-juridiques à l'encontre des entreprises souhaitant s'installer en Chine participe de ces revendications de souveraineté.
Début 2015, une série de mesure visant à renforcer la censure fut en effet adoptée. En réponse à ces mesures, plusieurs sites anti-censure commencèrent à héberger les contenus contestés. La réponse du gouvernement fut immédiate. Les autorités dévoilèrent un de leurs outils : le « grand canon », bloquant l'accès à certains sites via des attaques DDoS. Si le résultat fut mitigé et les contenus non supprimés, ce fut un message clair de la part des autorités chinoises : « *nous mettrons en œuvre notre souveraineté même si cela nécessite des opérations en dehors de l'Internet chinois* »[124].
Enfin, cette politique se traduit également en matière commerciale dans la mesure où les entreprises chinoises, notamment dans le domaine bancaire, font preuve d'ingénierie juridique pour rester exclusivement soumises au droit chinois et échapper à la juridiction des Etats sur le territoire desquels elles sont présentes.
La lutte contre le terrorisme constitue également une opportunité pour la Chine d'affirmer sa souveraineté dans le cyberespace. La loi anti-terroriste[125] votée en décembre 2015 fait peser un certain nombre d'obligations sur les entreprises étrangères, parmi lesquelles l'obligation pour ces entreprises de mettre à disposition des autorités chinoises les clés de déchiffrement des données cryptées. De plus, une autre loi[126] adoptée également en décembre 2015 oblige les entreprises faisant des cartes à localiser leurs données sur le

[120] Voir également fiche pays « Chine »
[121] State Council Information Office of People's Public of China, "The Internet in China", *China Daily*, 8 juin 2010, disponible sur http://www.chinadaily.com.cn/china/2010-06/08/content_9950198_2.htm
[122] http://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1234787.shtml
[123] http://english.cntv.cn/2015/12/16/VIDE1450236360367156.shtml
[124] Pour plus de détails voir Crowd Strike, *2015 Global Threat Report*, 2016, p.13
[125] Emily RAUHALA, « China passes sweeping anti-terrorist law with tighter grip on data flow", *The Washington Post*, 28 décembre 2015, disponible sur https://www.washingtonpost.com/world/china-passes-sweeping-anti-terrorism-law-with-tighter-grip-on-data-flow/2015/12/28/4ac6fe06-d79b-4c4c-bda9-27f15fabf892_story.html
[126] Bo XIANG, « China focus: China unveils new rules on maps, regulating online map services", *Xinhua*, 14 décembre 2015, disponible sur http://news.xinhuanet.com/english/2015-12/14/c_134916387.htm

territoire chinois. Ces deux textes participent donc à la défense de la souveraineté de la Chine en permettant un plus grand contrôle des autorités sur les données stockées et transitant sur et par son territoire.
Le second grand enjeu politique de la Chine est sa montée en puissance internationale, c'est-à-dire sa place et son poids dans les discussions au sein des enceintes internationales sur les sujets liés à Internet et au cyberespace. En février 2014, le président Xi Jinping a ainsi déclaré que la Chine ferait tout son possible pour devenir une cyberpuissance[127].
En matière de gouvernance d'Internet, la position chinoise est très claire : la gouvernance est l'apanage des Etats, les entreprises privées devant développer l'industrie et la société civile les soutenir. Elle défend donc une approche strictement multilatérale de la gouvernance d'Internet.
Sa montée en puissance internationale passe également par sa présence dans le débat sur les normes dans le cyberespace. Au niveau onusien, elle a soutenu dès 1998 une proposition de résolution[128] déposée par la Russie devant la 1ère commission de l'Assemblée générale des Nations unies. En 2015, elle a, avec la Russie, le Kazakhstan, le Tadjikistan et l'Ouzbékistan déposé un projet de code de conduite[129] auprès du Secrétaire général des Nations unies. Elle a également participé aux débats du groupe d'experts gouvernementaux au sein des Nations unies. Lors des réunions du Groupe d'experts, elle a réussi à faire adopter par les autres participants plusieurs de ses idées. Elle souhaitait ainsi que les discussions portent sur les normes en temps de paix et sur la prévention des conflits, et non sur le droit de la guerre. Or plusieurs des propositions contenues dans le projet de Code de conduite et le rapport du groupe d'experts gouvernementaux se ressemblent. Même si des différences notables existent, l'esprit de certaines dispositions est bien semblable. La signature d'accords bilatéraux avec la Russie et les Etats-Unis démontre également la volonté de la Chine de se placer sur la scène internationale comme un acteur majeur des discussions, ce qui lui permet de pousser ses idées au plan international.
En matière de coopération économique régionale, la Chine s'est investie dès 2001 sur la question des normes dans la mesure où les débats portaient principalement sur des aspects économiques et sur la protection des infrastructures vitales. Au niveau régional, elle est également très impliquée dans les débats sur ces questions. Les mécanismes de coopération sont nombreux et elle s'impose comme un acteur majeur de la région, y compris sur les sujets d'intérêt cyber[130]. Elle participe ainsi activement à l'APCERT.

Les enjeux numériques militaires[131]

La stratégie de montée en puissance chinoise passe enfin par le développement de ses capacités, en particulier militaires. La réorganisation de son administration (création d'une administration dédiée au cyberespace) et de ses armées sont deux éléments centraux de la mise en œuvre de sa stratégie.
L'enjeu pour la Chine est à la fois technologique et organisationnel. Afin d'y parvenir, le président Xi Jinping a affirmé courant 2015 qu'un commandement spécialisé et interarmées était nécessaire pour que la Chine soit pleinement capable de défendre son territoire, y compris dans le cyberespace. Cette réorganisation devrait être finalisée pour 2020. Le développement de capacités défensives et offensives est au cœur de la stratégie chinoise depuis plusieurs années.
La publication en mai 2015 de la *Stratégie militaire chinoise*[132] constitue un élément clé pour les observateurs étrangers dans la mesure où il permet d'avoir plus de visibilité sur les ambitions de la Chine. Le document adopte un ton relativement agressif, indiquant « qu'une armée forte » fait partie du rêve chinois et qu'il s'agit d'une condition pour que la Chine soit un pays fort et puisse se développer comme elle le souhaite. Il n'est pas fait mention de stratégie spécifique pour l'armée dans le cyberespace mais celui-ci fait partie intégrante de la stratégie générale en ce qu'il est considéré comme un nouveau domaine d'action. Parmi les missions assignées à l'Armée populaire de libération, figure en effet la préservation de sa sécurité et de ses intérêts dans les nouveaux domaines dont le cyberespace. La stratégie militaire chinoise est fondée sur le concept de défense active qui, d'après le document officiel, pourrait être résumé de la façon suivante : adhésion aux principes de la défense, à savoir légitime défense et adhésion au principe selon lequel « on n'attaquera pas à moins d'être attaqué mais [que] l'on contre-attaquera définitivement si l'on est attaqué ». Pour faire face aux nouvelles situations (opérations dans le cyberespace), une mise à jour des doctrines d'emploi sera effectuée. Enfin, le cyberespace est considéré comme un domaine critique, de la même façon que la mer, l'espace et le nucléaire.

[127] Zhu Ningzhu, ed., 'Xi Jinping Leads Internet Security Group,' English.news.cn, February 27, 2014, http://news.xinhuanet.com/english/china/2014-02/27/c_133148273.htm.
[128] United Nations, General Assembly resolution 53/70, Developments in the Field of Information and Telecommunications in the Context of International Security, A/RES/53/70 (4 January 1999), RES/53/70.
[129] https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf
[130] Voir analyse régionale Asie-Pacifique
[131] Voir également fiche pays « Chine »
[132] The State Council Information Office of the People's Republic of China, China's Military Strategy (May 2015), Beijing, http://www.chinadaily.com.cn/china/2015-05/26/content_20820628.htm.

Un paragraphe traite spécifiquement du cyberespace. *« Le cyberespace est devenu un nouveau pilier du développement économique et social et un nouveau domaine de la sécurité nationale ».* Pour les prochaines années, l'enjeu pour la Chine sera donc d'atteindre ces objectifs et d'intégrer au mieux ses capacités cyber au sein de ses forces armées.
Cependant, une des difficultés à laquelle la Chine devra faire face sera la gestion des groupes de hackers agissant pour son compte sous un contrôle plus ou moins fort de l'administration afin de maintenir une cohérence dans les actions entreprises.

Les défis pour la Chine sont nombreux et intrinsèquement liés à une légitimation des mesures adoptées sur son territoire via la promotion de ses idées sur la scène internationale. Un des enjeux sera la réhabilitation, au niveau international, du concept de souveraineté, largement dévoyé depuis de nombreuses années.

2.2 RUSSIE

La Russie comptait 146,2 millions d'habitants fin novembre 2015, dont 103,1 millions utilisaient Internet. Le taux de pénétration de la région s'élevait donc à 70.5%. Parmi ces internautes, seuls 11 millions possédaient un compte Facebook, équivalent à un taux de pénétration de 7,5%[133], ce qui s'explique par la présence d'autres services concurrents, comme Vekontakte. La Moscovite Alena Popova[134], experte en réseaux sociaux, explique que les russes sont de plus en plus connectés sur de nouveaux réseaux sociaux comme Vkontakte.ru, Odnoklassiniki.ru, Livejournal.com ou encore Yandex, qui sont nettement préférés à Facebook[135]. L'espace numérique russe se développe ainsi de façon relativement autonome et indépendante par rapport aux grandes plateformes occidentales, principalement américaines. Le taux de pénétration mobile s'élève à 72%, avec 103.2 millions de russes détenteurs d'un mobile.

2.2.1 Perception des menaces globales et cyber

Les conflits internationaux, ukrainiens et syriens notamment, l'équilibre des pouvoirs, les questions d'énergies et d'économie liées à la division par trois des cours des hydrocarbures depuis 2014 et aux sanctions européennes, ont été les principaux thèmes de catharsis dans le cyberespace en 2015.[136] Les questions d'ordre géopolitique sont portées jusque dans le cyberespace via des activités hacktivistes, cybercriminelles, ou encore d'espionnage. A l'image de la Chine, la Russie se positionne de façon relativement ambivalente face à la cybercriminalité et parait ne pas hésiter à s'en servir à des fins étatiques. Les manifestations patriotiques sur Internet peuvent en effet servir en partie les intérêts du pouvoir : constitution d'un vivier de compétences informatiques dans lequel le gouvernement pourrait « piocher » pour des opérations de guerre informatique, contrôle de l'information sur Internet, démonstration de force vis-à-vis des grandes puissances, etc. Déjà dans le cas des affrontements informatiques qui ont accompagnés le conflit avec la Géorgie en 2008, une organisation de jeunesse réputée proche du Kremlin comme Nashi a joué un vrai rôle de fédérateur et de mobilisateur de la jeunesse russe autour des quelques objectifs patriotiques, contribuant ainsi, au moins de façon indirecte, au conflit informatique. La Russie semble avoir réitéré ces pratiques dans son conflit face à l'Ukraine qui dure depuis 2014. Pour Kevin Limonier, Maître de conférences en études slaves & géopolitique (université Paris VIII), enseignant en géopolitique et langue russe, la « menace » russe dans le cyberespace ne se cantonne plus aux cyberattaques stricto sensu (intrusions, vol d'information, dénis de services, etc.), mais intègre aujourd'hui des notions d'influence et de « guerre informationnelle ».[137]

[133] http://www.internetworldstats.com/europa2.htm#ru
[134] http://alenapopova.com/bio.html
[135] http://www.rfi.fr/asie-pacifique/20111110-russie-poutine-medvedev-vkontakte-livejournal-yandex-odnoklassiniki-facebook/
[136] http://www.crowdstrike.com/global-threat-report-2015/
[137] http://villesfermees.hypotheses.org/378

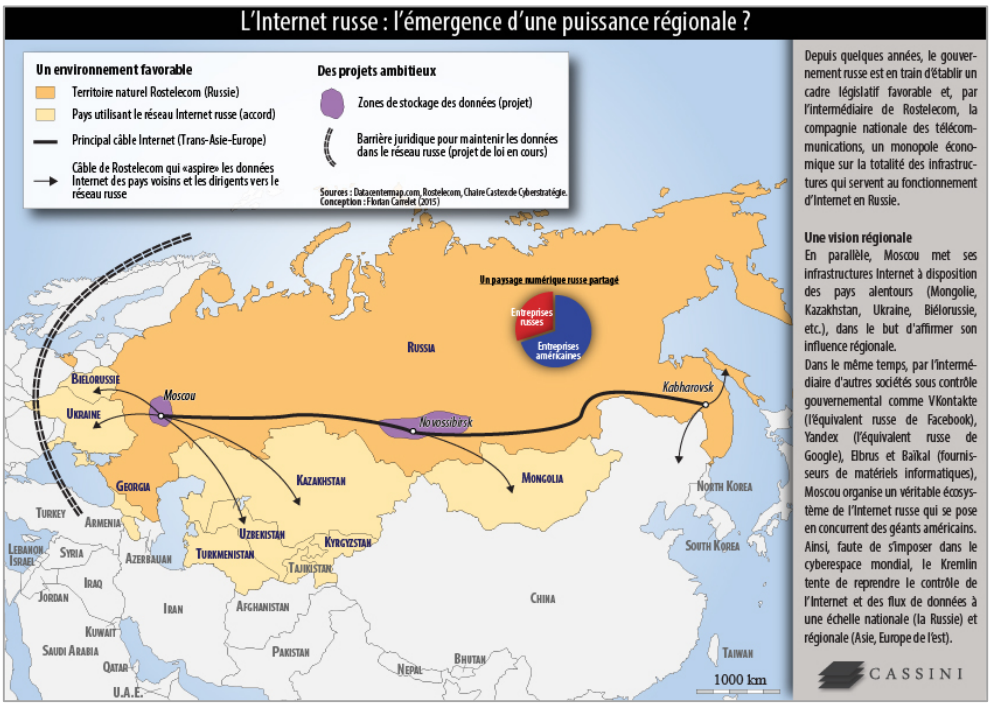
Trois menaces cybernétiques émanent de la Russie : l'hacktivisme, la cybercriminalité et les attaques ciblées sponsorisées par l'Etats, dont le mode opératoire est principalement basé sur les « Advanced Persistent Threat » (APT).
Beaucoup d'attaques APT émanent en effet de Russie avec pour cibles des organisations variées : entreprises, banques, ONG, etc. Ces attaques sont conduites à des fins de cyberespionnage par des mercenaires informatiques onéreux.
La forte cybercriminalité qui émane de Russie utilise n'importe quel type de malware, ce qui est chose aisée puisque le pays abrite une communauté de développeurs qui est réputée la meilleure en matière de développement de malwares. La constante évolution de cette cybercriminalité s'explique principalement par la grande tolérance dont fait preuve le gouvernement russe à l'égard des « black hats » qui s'en prennent aux pays rivaux. On trouve ainsi de nombreux espaces marchands sur internet (*black market*) qui offrent des outils de piratage, des malwares, à des prix variées. Ces plateformes, de plus en plus tournées à l'international avec des hackers qui communiquent non seulement en russe mais aussi en anglais afin d'attirer une clientèle internationale, sont connues et font pourtant rarement l'objet de procédures. Les black markets russes constituent notamment le lieu d'échange des malwares financiers les plus avant-gardistes.
Enfin, l'hacktivisme russe est relativement marginal. Les Anonymous International ont cependant développé une plateforme qui vend aux enchères les contenus volés concernant les membres du gouvernement russe, y compris Vladimir Poutine et Dmitri Medvedev. Si cette démarche répond à des considérations financières évidentes, elle participe aussi à la dénonciation de « l'armée des trolls » qui défend le gouvernement russe dans les médias sociaux.
Mais la Russie connait depuis un an une révolution en matière de menaces cybernétiques : la combinaison des attaques dites APT et de la cybercriminalité. C'est un phénomène unique au monde qui s'est développé avec le groupe Carbanak. Si à l'origine le groupe avait donné naissance à un malware bancaire traditionnel (Carberp), voué à être diffusé à un certain nombre de criminels en vue de cibler un très grand nombre de personnes. Suite à la fuite du code source de ce malware, le groupe a finalement décidé de passer à l'opérationnel en ciblant directement d'importantes organisations financières, dans un premier temps strictement russes, adoptant ainsi le style de l'attaque APT. Le groupe procède à une petite révolution, d'autant qu'il est aussi le premier groupe russophone à s'en prendre aux institutions russes. Le groupe casse ainsi les codes de la cybercriminalité russe qui ne s'en prenait jusqu'ici pas à des russophones puisque les descriptifs des malwares vendus par des hackers russes comportent généralement une mention précisant que le malware ne fonctionne pas en Russie, certains malwares s'arrêtant même de fonctionner si le système d'exploitation de la cible est associé à la langue russe et possède un clavier cyrillique. Le principal forum russe de vente de malware impose aux vendeurs de ne pas vendre de malware pouvant fonctionne en Russie et dans les autres pays de la CEI (ex-URSS).
Les inquiétudes face à l'évolution de la cybercriminalité russe s'expliquent par le rôle de modèle que celle-ci joue sur la scène internationale de la cybercriminalité. Le marché du cybercrime russophone est connu dans le monde entier depuis en raison de la couverture médiatique importante dont il bénéficie, mais aussi parce qu'il est très facile d'accéder aux plateformes en ligne utilisées par les réseaux criminels pour distribuer des produits toujours plus sophistiqués. Une étude[138] sur l'écosystème cybercriminel brésilien de Kaspersky Lab souligne ainsi que le cybercrime brésilien coopère avec les gangs européens impliqués dans la création des malwares ZeuS, SpyEye et d'autres Trojans en provenance du marché russophone.

2.2.2 Les enjeux numériques pour la Russie

Economie et technologies au service d'une politique de souveraineté

Le gouvernement russe s'oppose à la gouvernance multi-acteurs prônée principalement par les pays occidentaux, qui, selon lui, renforce la domination américaine dans le cyberespace. Pour la Russie, le gouvernement américain disposerait *« des normes, des infrastructures (concentration des data centers), du matériel informatique, et des services (via les géants du net comme Google ou Facebook) »*[139]. Cette crainte d'un internet trop occidentalisé a conduit le gouvernement russe à développer une vision régionale d'Internet en s'accaparant, via Rostelecom, la compagnie nationale des télécommunications, le monopole économique de la totalité des infrastructures qui servent au fonctionnement d'Internet en Russie, tout en mettant ses infrastructures à disposition des pays voisins : Mongolie, Kazakhstan, Ukraine, Biélorussie.

[138] https://securelist.com/analysis/publications/72652/beaches-carnivals-and-cybercrime-a-look-inside-the-brazilian-underground/
[139] http://www.diploweb.com/Vers-un-Internet-russe.html



Carte « l'Internet russe : l'émergence d'une puissance régionale ? » par Florian Carrelet, pour Cassini[140]

La Russie recherche véritablement l'indépendance technologique et elle entend pour cela se débarrasser des technologies occidentales, principalement américaines. C'est ainsi que le gouvernement russe cherche à évincer Windows au profit de Linux. Si la Russie a émis le souhait de développer son propre système d'exploitation, il y a un fossé entre la volonté politique et la mise en pratique. Cinq ans après la décision de Vladimir Poutine de basculer les infrastructures étatiques de Windows à Linux, la transition n'est visiblement pas encore tout à fait opérée. Néanmoins, le nouveau responsable de la politique numérique et technique du Kremlin, German Klimenko, a affirmé, début février 2016, à Bloomberg, que le gouvernement russe poursuivait toujours ce but. Selon ce dernier, 22 000 collectivités territoriales seraient d'ores et déjà prêtes à passer immédiatement à Linux. Il indiquait d'ailleurs qu'il s'agissait d'une bascule « inévitable », mais qui ne concernait que les ordinateurs gouvernementaux, le grand public n'étant pas tenu de suivre les mêmes directives que les administrations de l'État. Bloomberg a abordé le possible départ des firmes américaines face à la politique du gouvernement russe, ce à quoi German Klimenko a répondu – prenant l'exemple de Google – que *« ça ne sera pas fatal si elles quittent la Russie — Yandex et Mail.ru ont des technologies similaires »*.[141] D'ailleurs le moteur de recherche russe Yandex surpasse largement Google en Russie, ce dont le pouvoir russe a déjà bien conscience.

Windows n'est en effet pas la seule cible du gouvernement russe puisque d'autres initiatives ont déjà vu le jour. Les autorités russes souhaitent par exemple également s'affranchir davantage de Google en développant un nouveau moteur de recherche étatique – baptisé Spoutnik – qui devrait notamment être imposé dans les administrations du pays. Le pays a enfin annoncé son intention de remplacer ses ordinateurs et serveurs équipés de processeurs américains AMD ou Intel par ses propres processeurs Baikal, basés sur une architecture ARM. Et un autre de ses autres projets consiste à développer un système d'exploitation mobile pour échapper à la domination des plateformes américaines. Le pays espère ainsi ramener la part conjointe d'Android, d'iOS et de Windows Phone à moins de 50% d'ici 2025.

Ces initiatives s'inscrivent toutes dans la volonté russe de développer ses propres capacités afin de ne plus dépendre de solutions étrangères, notamment américaines, pour des questions de souveraineté nationale. C'est par cette voie là que le Kremlin tente, faute de s'imposer dans le cyberespace mondial, *« de reprendre le*

[140] Ibidem.
[141] http://www.numerama.com/tech/145055-la-russie-veut-toujours-se-debarrasser-de-windows.html

contrôle de l'Internet et des flux de données à une échelle nationale (La Russie) et régionale (Asie, Europe de l'Est) »[142].

La Russie entend ainsi sortir de l'idée prégnante d'unipolarité, et du face-à-face avec l'Organisation du traité de l'atlantique nord (OTAN). C'est la raison pour laquelle elle tourne son regard vers ses deux principaux partenaires : l'Inde et la Chine, mais aussi le Moyen-Orient. Une grande partie de son attention s'est d'ailleurs focalisée sur les activités cybernétiques émanant du Moyen-Orient et des groupes de hackers arabophones, parfois eux-mêmes formés par des hackers tchétchènes.

Du point de vue militaire

Comme le soulignait Kévin Limonier, la Russie a intégré des notions d'influence et de « guerre informationnelle »[143] dans les menaces à combattre. C'est pourquoi, selon le directeur adjoint du FSB, le Général d'armée Sergey Smirnov, le FSB avait reçu comme mission, pendant le Printemps arabe, d'élaborer des mesures pour contrer les activités des agences de renseignement occidentales dans la blogosphère. La dimension psychologique des affrontements informatiques est au cœur de la posture russe. La sécurité informatique n'est pas définie uniquement comme la sécurité du contenant mais également comme la sécurité des contenus, avec tout ce que cela peut entraîner en termes de censure sur Internet.

D'autre part, la conception offensive de la cybernétique, bien que longtemps non reconnue par les autorités russes, ne fait plus aucun doute, notamment au regard du soutien aux hackers patriotiques. A titre d'exemple, une coupure d'électricité a plongé une grande partie de la région ukrainienne d'Ivano-Frankivsk dans le noir pendant plusieurs heures le 23 décembre 2015, panne qui pourrait avoir été causée par un piratage informatique. La société ESET aurait en effet trouvé des traces du malware "BlackEnergy" sur les serveurs infectés. Apparu en 2007, BlackEnergy est un logiciel malveillant dont la conception est attribuée au groupe "Sandworm" qui serait basé en Russie, et qui a notamment été utilisé lors des cyberattaques en Géorgie de 2008[144]. Le groupe aurait d'ailleurs déjà mené des attaques contre des cibles du gouvernement ukrainien mais aussi polonais, des médias ukrainiens et des services de l'OTAN. Si ces éléments se révélaient exacts, il s'agirait là de la première cyberattaque générant le blocage d'une infrastructure critique.[145]

2.3 IRAN

L'Iran comptait 81.8 millions d'habitants fin novembre 2015, dont 46.8 millions utilisaient Internet. Le taux de pénétration de la région s'élevait donc à 57,2%. Fin 2015, le taux de pénétration mobile en Iran s'élève à 136,1%[146], ce qui fait du marché de la téléphonie iranien l'un des plus attrayants du Moyen-Orient avec celui de la Turquie.

Les chiites sont majoritaires en Iran, tout comme en Irak et au Liban. Cette division religieuse est aujourd'hui instrumentalisée par le politique et les deux camps sont en guerre dans le Golfe arabo-persique.

L'année 2015 marque la conclusion du *Joint Comprehensive Plan of Action* (JCPOA), accord qui met fin aux intenses discussions relatives au programme nucléaire iranien avec les membres permanents du Conseil de sécurité des Nations Unies et l'Union européenne. Cet accord scelle la levée des dix années de gel économique, avec la fin des sanctions économiques et financières multilatérales et nationales liées au programme nucléaire iranien, effective depuis le 16 janvier 2016.

Malgré un rapport ambivalent à Internet, perçu à la fois comme vecteur de modernisation et de propagande, tout en étant un moyen de contestation et d'information alternatif pour la population, l'Iran reste le pays le plus connecté à Internet dans le monde arabo-musulman.

2.3.1 Perception des menaces globales et cyber

[142] http://www.diploweb.com/Vers-un-Internet-russe.html
[143] http://villesfermees.hypotheses.org/378
[144] https://securelist.com/blog/research/73440/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/
[145] http://www.lemonde.fr/pixels/article/2016/01/05/un-piratage-soupconne-d-etre-a-l-origine-d-une-coupure-electrique-en-ukraine_4841756_4408996.html#tsYUwHlyQuuZGbJT.99
[146] http://www.marketresearch.com/Business-Monitor-International-v304/Iran-Telecommunications-Q4-9257973/

Les tensions internationales

Aux yeux du gouvernement iranien, le bouleversement induit par la levée des sanctions économiques et l'ouverture du pays est autant une opportunité qu'une menace. Le régime craint que la reprise des échanges économiques et financiers avec l'Occident entraine la dégradation des valeurs et de la culture islamique iranienne. C'est la raison pour laquelle l'Iran devrait accroitre ses capacités de cyber espionnage et de censure.

La menace nucléaire que représentait le pays aux yeux des Etats-Unis a poussé l'Iran à développer une stratégie défensive en cas d'échec des négociations. Une stratégie justifiée si l'on en juge la série d'attaques que l'administration Obama avait prévu de lancer (plan *Nitro Zeus*) contre les infrastructures vitales et les systèmes de communication iraniens avant la finalisation du *Joint Comprehensive Plan of Action* (JCPOA) en juillet 2015 qui a fort heureusement soulagé les tensions.[147] Selon le producteur du documentaire "*Zero Days*", ce plan souligne l'importance croissante des cyberattaques dans les actions militaires des Etats-Unis. *Nitro Zeus* était *"probablement le plus grand et le plus complexe plan de cyberguerre jamais créé par les Etats-Unis"* a déclaré Alex Gibney à Buzzfeed.

A la suite de l'affaire Stuxnet, et face à la crainte d'une nouvelle attaque informatique américaine, le pays a donc développé des capacités cybernétiques qui sont elles-mêmes devenues une importante menace. La Russie et la Corée du Nord auraient d'ailleurs travaillé avec l'Iran pour améliorer et développer des outils d'attaques. Le pays considère en effet ces cyberattaques comme un outil stratégique pour des guerres asymétriques contre des adversaires plus puissants. Il s'agit aussi de réprimer toute dissidence face aux vulnérabilités que crée Internet en matière de contrôle de l'information, notamment suite à la « Green Revolution » de 2009. Les dirigeants iraniens craignent en effet profondément le pouvoir des réseaux, notamment depuis les printemps arabes égyptiens et tunisiens de 2011. Le ministre de l'intérieur, Mostafa Najjar, indiquait ainsi en 2012 : *« les satellites et Facebook sont les moyens électroniques d'une guerre d'influence par l'Ouest pour que s'effondre l'Iran »*[148]. La donne n'a pas changé.

Dans les derniers mois de l'année 2015, les Etats-Unis ont vu derrière la multiplication des cyberattaques visant des sites internet officiels américains la main de l'Iran. Les attaques de la fin du mois de novembre, qui visaient les comptes de messageries et de réseaux sociaux de hauts fonctionnaires de l'administration d'Obama, auraient été menées par l'unité de cyberguerre du Corps des gardiens de la révolution iranienne (force militaire iranienne distincte du corps principal et proche du chef suprême du régime, l'ayatollah Ali Khamenei).[149]

Certains responsables de l'administration Obama considèrent que cette vague d'attaques était liée à l'arrestation sur le territoire iranien, en octobre, de l'irano-américain Siamak Namazi, partisan de la normalisation. Cette arrestation pourrait s'inscrire dans le cadre de la lutte d'influence qui se déroulerait au sein du régime iranien entre les réformateurs et les conservateurs. Proches de Khamenei, ces derniers craignent en effet que l'accord nucléaire conclu avec les puissances mondiales en juillet n'annonce une libéralisation et un réchauffement des liens avec l'Occident.[150]

Le fait que ces attaques ne semblaient être motivées par l'espionnage, comme c'est le cas pour les attaques russes ou chinoises, mais semblent plutôt avoir eu pour objectif de bloquer des institutions américaines, rend cette menace plus inquiétante. Afin de résister aux éventuelles attaques de ses rivaux, l'Iran tente sans cesse d'accroître ses capacités de résilience et de contre-attaque sur le plan de la cyberguerre. A titre d'exemple, il peut être cité les attaques comme celles dirigées entre 2012 et 2013 à l'encontre des banques et la presse américaine[151], qui constituent des outils de propagande pour l'Iran en raison de la couverture médiatique importante dont elles bénéficient. Le véritable danger est qu'Israël pourrait devenir la cible d'un Iran qui cherche à devenir la puissance dominante du Moyen-Orient[152], ce qui conduirait à une dangereuse escalade.

Signe de l'importance accordé par le régime au cyberspace, l'Ayatollah Khamenei a choisi le 5 septembre 2015 les nouveaux membres du *Supreme Council of Virtual Space* mis en place en mars 2012. Ce conseil, qui devait jusque-là faire face à la concurrence d'autres entités gouvernementales en matière de régulation et de politique relative à Internet, a également vu ses prérogatives renforcées, au point d'être aujourd'hui le seul responsable d'Internet dans le pays. Pour l'Ayatollah Khamenei, le pays doit en effet sortir d'une posture passive en matière de cyberespace pour pouvoir tirer bénéfice du JCPOA sans subir la pénétration d'une idéologie occidentale susceptible de menacer le régime.

[147] http://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html?_r=1
[148] http://www.payvand.com/news/12/mar/1129.html
[149] http://fr.timesofisrael.com/liran-aurait-mene-des-cyberattaques-contre-des-responsables-americains/
[150] http://www.wsj.com/articles/u-s-detects-flurry-of-iranian-hacking-1446684754
151 http://www.theguardian.com/world/2016/mar/24/us-charges-iranian-hackers-cyber-attacks-banks
[152] http://uk.businessinsider.com/iran-is-emerging-as-one-of-the-most-dangerous-cyber-threats-to-the-us-2015-12

Les tensions du Golfe

Le conflit qui oppose l'Iran et les nations Arabes du Golfe, Arabie Saoudite en tête, se joue aussi et devrait se jouer sur le terrain cybernétique. Les capacités d'attaques cybernétiques de l'Iran sont en effet une source majeure de crainte pour les Etats du Golfe, tout comme celles d'Israël. La montée en puissance de l'Iran et d'Israël en matière de capacités cybernétiques bouscule les six pétromonarchies arabes et musulmanes du golfe arabique, membres du Gulf Cooperation Council (GCC) : l'Arabie saoudite, Bahreïn, les Émirats arabes unis, le Koweït, Oman et le Qatar, qui ne possèdent pas de capacités similaires, même si l'attaque iranienne sur l'Arabie Saoudite en 2012 fut un *wake-up call* pour la région.[153] Depuis, les Etats-Unis ont soutenu les pays du Golfe dans l'amélioration de leurs capacités de cyberdéfense.

2.3.2 Les enjeux numériques pour l'Iran

Du point de vue technologique

En mai 2011, la presse locale iranienne a annoncé que l'Iran souhaitait développer son système d'exploitation pour remplacer Windows[154]. Toutefois, ce projet n'a toujours pas été concrétisé. En septembre 2012, l'Iran a également lancé son propre réseau national pour ses administrations et a coupé l'accès à Google et Yahoo ![155]. Parallèlement, il semble que le réseau contrôlé soit sur pied et fonctionnel. Huawei aurait fourni les équipements permettant sa mise en place.[156]

En dépit d'une main d'œuvre compétente et d'une capacité scientifique et technique réelle, l'industrie informatique iranienne a souffert de gros handicaps. La majeure partie des logiciels était importée ou piratée et seules quelques entreprises iraniennes ont pu développer des liens internationaux. L'essor de l'industrie informatique iranienne est jusque-là resté le fait de quelques programmes structurants dans le cadre des objectifs définis par les plans de développement quinquennaux et les initiatives gouvernementales.

Les multinationales du net, Facebook, Twitter, LINE, WhatsApp, Tango, font l'objet d'une surveillance accrue, et ont pour la plupart déjà été suspendues, ou menacées de l'être.

Du point de vue politique et économique

Le 6ème plan quinquennal du gouvernement iranien (2016-2021), dévoilé le 30 juin 2015, met en lumière la priorité accordée par le pays au développement des capacités cybernétiques et des moyens de contrôle. Ainsi le programme Black spider devrait être étendu à d'autres médias sociaux comme Instagram, Viber ou encore Whatsapp.[157] Le gouvernement iranien mène une véritable lutte contre la menace que peut représenter un Internet ouvert sur le monde pour la stabilité du régime. Cette volonté politique, qui n'est pas nouvelle, s'appuyait depuis 2006 sur le développement d'un Internet alternatif national qui devait, à long terme, remplacer l'Internet mondial dans le pays. Cet Internet national devait se conformer aux lois islamiques et respecter l'éthique et la morale musulmane. Cependant, au-delà des contraintes techniques qu'implique un tel projet, le fait de limiter l'accès à l'Internet mondial pourrait avoir de larges répercussions économiques pour l'Iran, notamment avec des partenaires comme la Chine ou encore la Russie. Ce projet d'« Internet Halal[158] », baptisé Iraniannet[159], dans lequel un milliard de dollars aurait été investi par le gouvernement en 2008[160], s'avère finalement être composé de plusieurs outils de recherche en ligne et de média sociaux propre à l'Iran, sur le modèle de ceux présents en Occident.[161]

Néanmoins, la levée des sanctions contre l'Iran devrait pousser le gouvernement à améliorer son projet, afin de mieux protéger son Internet national des idées occidentales. Il coopère d'ailleurs avec la Chine en vue de l'amélioration de cet Internet national.[162]

C'est dans ce but que le 6ème plan quinquennal entend favoriser l'éclosion de nouveaux réseaux sociaux locaux qui permettront un meilleur contrôle de l'information.

[153] http://csis.org/publication/cybersecurity-and-stability-gulf
[154] http://www.africaburkina.com/spip.php?article456
[155] http://www.telerama.fr/medias/l-iran-se-coupe-de-l-internet-mondial,87043.php
[156] http://articles.washingtonpost.com/2012-09-19/world/35496978_1_huawei-iranian-activists-iranian-government
[157] http://www.crowdstrike.com/global-threat-report-2015/
[158] http://iran.blog.lemonde.fr/2011/04/27/un-internet-halal-bientot-en-iran/
[159] http://www.africaburkina.com/spip.php?article456
[160] http://online.wsj.com/article/SB10001424052748704889404576277391449002016.html
[161] http://www.crowdstrike.com/global-threat-report-2015/
[162] http://www.crowdstrike.com/global-threat-report-2015/

Du point de vue militaire
Le 6ème plan quinquennal fait aussi référence aux questions de défense et de sécurité. Dans ce dernier, le guide suprême indique vouloir allouer au moins 5% du budget de la défense dans le développement des capacités de cyberdéfense et de cybersécurité des infrastructures.
L'Institut américain Defensetech classait d'ailleurs l'Iran au 5ème rang des puissances mondiales en termes de capacités de cyberguerre. Une analyse qu'il convient de relativiser : le terme « cyberguerre » utilisé par Defensetech englobe à la fois la guerre informatique stricto sensu et la guerre de l'information, deux formes d'affrontement intimement liées mais qui ne peuvent cependant pas être mises sur le même plan tant les moyens impliqués sont différents. Pourtant, les capacités de cyberguerre de l'Iran ne sont plus à mettre en doute après une année 2015 marquée par les actions de l'unité de cyberguerre du Corps des gardiens de la révolution iranienne.

L'accord du 14 juillet 2015, portant sur la levée des sanctions économiques à l'encontre du pays, soulève des craintes dans la région du fait de son ambiguïté. En effet, si le JCPOA est robuste à court terme (8-15 ans), l'Iran pourrait de nouveau prétendre à l'arme nucléaire à moyen terme. Pour Nicolas Roche, conseiller diplomatique du ministre de la défense de juillet 2012 à janvier 2014 et directeur de la stratégie à la Direction des applications militaires du CEA depuis janvier 2014, l'accord repose finalement sur un pari politique, stratégique et technologique selon lequel d'ici 15 ans, le régime iranien sera suffisamment intégré dans les relations internationales pour ne plus souhaiter obtenir l'arme nucléaire. Un pari qui attise les craintes des pays du Golfe et qui pourrait bouleverser les équilibres et entrainer une potentielle cascade de prolifération si ces pays décidaient de se retirer du traité de non-prolifération (TNP) ou développer les technologies duales nécessaire à la construction d'une arme nucléaire, pour se préparer au cas où l'Iran ne respectait pas l'accord.
Sur le plan numérique, l'Iran, bien conscient de l'opportunité que représente le cyberespace, doit maintenant compter avec une ouverture sur le monde extérieur qui pourrait lui porter préjudice. Le pays se prépare d'ores-et-déjà à faire face à ce qui lui apparait comme la plus grande menace : l'occidentalisation de la société iranienne.

2.4 ISRAËL

Israël comptait 7,9 millions d'habitants fin novembre 2015, dont 5,9 millions utilisaient Internet, soit un taux de pénétration de 74,78%. Fin 2015, le taux de pénétration mobile en Israël s'élevait quant à lui à plus de 100%[163].
Israël reste le pays le plus avancé du Moyen-Orient au plan numérique. Internet est devenu pour le pays une arme médiatique et un véritable espace de guerre informationnelle. Le réseau est en effet perçu comme un vecteur d'influence permettant de justifier au travers de campagnes de communication efficientes, des actions ou des choix politiques opérés par Israël.
Conscientes de l'intérêt stratégique que représente Internet, les autorités israéliennes apparaissent comme les acteurs principaux en matière de gouvernance du réseau et ont mis l'accent sur une approche à la fois défensive mais aussi offensive du cyberespace. Parallèlement, le privé joue également un rôle en mettant sur le marché des technologies très performantes, ce qui pousse de plus en plus de grandes entreprises à établir des centres de R&D dans le pays, qui se prévaut également d'un nombre très important de start-ups dans le domaine de la cybersécurité.

2.4.1 Perception des menaces globales et cyber

La principale menace qui pèse sur Israël reste la menace palestinienne dans cette « dialectique récurrente de vie et de survie [qui] nourrit des tensions permanentes, entre guerres ouvertes et paix armées »[164] alors que l'assise territoriale d'un futur Etat palestinien se réduit à mesure que les colonies de peuplement israélien se développent[165].

[163] http://www.nationmaster.com/country/is-israel/med-media
[164] Jean-Marie Deblonde, Philippe Veyron, *Géopolitique du conflit israélo-palestinien.Les hommes, la terre et l'eau*, Ellipses, Paris, 2009.
[165] http://www.diploweb.com/Conflit-israelo-palestinien-un.html

Kavé Salamatian, professeur d'informatique à l'Université de Savoie qui aborde la question de la géographie du cyberespace, rappelle comment, dès l'origine des réseaux sociaux, le conflit israélo-palestinien s'est exporté dans le cyberespace pour former une caisse de résonnance pour la propagande des deux camps. Depuis l'Opération Pilier de défense en novembre 2012, *« tous les leviers de la cyberstratégie ont été [et sont] utilisés : l'attaque de déni de service par les Anonymous, l'intrusion informatique, l'utilisation d'outil de key logging sur des ordinateurs d'activistes pro-palestiniens, et une surveillance permanent des réseaux sociaux et des médias pour une réaction en temps réel. L'ensemble de ces leviers ont été utilisés afin d'asseoir une suprématie dans le cyberespace* ».[166] Autant d'actions qui démontrent que les cyberattaques sont aujourd'hui un outil stratégique pour des guerres asymétriques menées contre des adversaires plus puissants.
Si la transposition du conflit israélo-palestinien dans le cyberespace constitue la première source de menaces, Israël est en réalité confronté à des menaces variées, qu'il s'agisse d'attaques étatiques, de cybercriminalité ou d'hacktivisme. Le pays a ainsi été à plusieurs reprises victime d'attaques fomentées par le Hamas ou le Hezbollah, mais aussi la cible d'un groupe affilié à la *China's People's Liberation Army* qui cherchait à dérober les plans de systèmes anti-missiles israéliens, de la Syrian Electronic Army ou de l'Iran à des fins d'espionnage. En 2015, les Anonymous menaçaient également de reproduire un « electronical Holocaust ». Sans oublier les attaques en provenance de la Turquie, d'Afrique du Nord et des populations palestiniennes.[167]

La menace palestinienne est considérée comme la plus prégnante, si bien qu'en octobre 2015 les forces de police israéliennes ont annoncé la mise en place d'une unité spécifiquement dédiée à la lutte contre la terreur arabe dans le cyberespace. Cette unité traque les tentatives de coordination d'attaques terroristes, notamment sur les médias sociaux, afin d'identifier les individus impliqués et de stopper toute tentative d'action.[168] Israël a aussi développé des systèmes de protection permettant d'identifier les fournisseurs d'accès Internet et les pays les plus susceptibles d'être utilisés pour une attaque, désignant la Russie, la Chine, la Turquie, l'Arabie Saoudite et l'Iran comme les pays à risques.[169]

Even, Shmuel et David Siman-Tov indiquaient déjà en 2012 dans « Cyber Warfare : Concepts and Strategic Trends » que le cyberespace était autant une source de profits que de menaces pour Israël. La puissance numérique du pays en fait en effet une cible de choix alors que ses ennemis gagnent en maturité sur ce terrain. Ainsi, en 2014, ce n'est pas moins d'un million de cyberattaques par jour qui touchaient le pays durant les opérations menées par Israël contre le Hamas à Gaza.[170] Israël prend donc la menace cybernétique très au sérieux, la définissant comme l'une des plus graves et des plus rapides à s'étendre. Il se positionne aujourd'hui comme l'un des plus avancés au regard de son économie et de ses capacités technologiques[171], un résultat qui ne doit rien au hasard. Dès 1997, Israël créait en effet la Tehila (Governement Infrastructure for the Internet Age), qui avait pour mission de sécuriser les connexions et réseaux gouvernementaux.[172] En 2014, le Premier ministre Benjamin Netanyahu déclarait même que les cyberattaques étaient l'une des quatre menaces principales pour Israël.[173] Comme le soulignait Carr Jeffrey, dans « Inside Cyber Warfare » publié en 2012, pour Israël, le cyberespace constitue une véritable alternative à la guerre conventionnelle. D'autant que Meir Elran et Gabi Siboni, dans « Establishing an IDF Cyber Command. » publié en 2015, soulignaient la mutation engagée par l'Israel Defense Forces (IDF) en juin 2015. Objectif : établir d'ici juin 2017 un nouveau Cyber Command, réunissant les capacités cybernétiques défensives et offensives sous le même toit.

Déjà évoquée plus haut, la levée des sanctions économiques à l'égard de l'Iran constitue un facteur d'inquiétude supplémentaire. Israël est en effet en première ligne face à l'ambition de l'Iran de devenir la puissance dominante dans la région. Le pari politique, stratégique et technologique sur lequel repose l'accord du 14 juillet 2015 pourrait par ailleurs bouleverser les équilibres et entrainer une prolifération en cascade si certains décidaient de se retirer du traité de non-prolifération (TNP) ou de développer les technologies duales nécessaires à la construction d'une arme nucléaire, pour se préparer au cas où l'Iran ne respectait pas l'accord.

[166] http://israelenergy.hypotheses.org/301
[167] Cohen, Matthew S., Charles (Chuck) D. Freilich and Gabi Siboni. (2015) Israel and Cyberspace: Unique Threat and Response. International Studies Perspectives, doi: 10.1093/isp/ekv023
[168] http://www.dcoi-conference.org/#!Executive-Cyber-Intelligence-BiWeekly-Report-Oct-15-2015/c1nz1/561e7b2d0cf297bd6863e21b
[169] Cohen, Matthew S., Charles (Chuck) D. Freilich and Gabi Siboni. (2015) Israel and Cyberspace: Unique Threat and Response. International Studies Perspectives, doi: 10.1093/isp/ekv023
[170] Ibidem.
[171] Ibidem.
[172] Ibidem.
[173] http://www.haaretz.com/misc/iphone-article/1.615637

2.4.2 Les enjeux numériques pour Israël

Du point de vue technologique

Israël est depuis une vingtaine d'année le deuxième écosystème d'innovation dans le monde derrière la Silicon Valley de San Francisco.[174] Le pays possède sa propre Silicon Valley surnommée la Silicon Wadi, pour désigner la zone forte concentration de sociétés du secteur de la haute technologie située sur la côte israélienne, autour de villes telles que Tel Aviv, Haifa et Caesarea. Il se créerait près de 500 start-up chaque année[175] et le secteur de la cybersécurité a vu ses exportations augmenter de 10% en 2015, avec un chiffre d'affaires d'environ 3 milliards de dollars[176]. Il y aurait entre 200 et 250 start-up en Israël travaillant sur des questions relatives à la cyberdéfense, ainsi qu'environ 7 à 8 000 ingénieurs.[177]

Le gouvernement et le secteur privé israélien se sont tous deux tournés vers leurs homologues américains en vue d'améliorer les capacités du pays. Les deux pays ont travaillé à la création de fondations binationales afin de supporter la recherche et le développement de leurs capacités. De plus, les partenariats entre entreprises israéliennes et américaines sont nombreux, tandis que nombre de géants américains sont déjà implantés dans le pays, tels Microsoft, Apple, Cisco, IBM, ou encore Google[178] qui est en pleine expansion en Israël. En tout, 2,3 milliards de dollars ont été investis entre 2010 et 2015 par la société rien que pour le rachat de sociétés israéliennes de cybersécurité.

Imbrication politique et économique et militaire

Entretenant d'ores et déjà des relations durables, la Défense et le secteur privé israélien trouvent dans les questions cybernétiques matière à renouveler et approfondir leurs liens.

Le succès de l'innovation israélienne s'explique en effet en partie par une intégration particulièrement importante du secteur de la Défense dans les activités industrielles nationales[179]. Ce secteur est en outre le principal client et financeur, tout en participant activement au transfert de technologies vers le milieu civil. Israël bénéficie par ailleurs de véritables politiques favorisant l'innovation technologique, notamment par le biais de politiques fiscales incitatives. Le pays est aujourd'hui au premier rang mondial en terme d'intensité de la recherche puisque l'Etat alloue chaque année entre 5 et 6% de son PIB à la R&D quand ce pourcentage atteint en moyenne 1,9% au sein de l'Union européenne et 3 % aux Etats-Unis.[180]

Les capacités de cyberdéfense et de cyberguerre d'Israël ne sont donc plus à mettre en doute, et ce même au regard de l'acceptation la plus large du terme « cyberguerre » qui englobe à la fois la guerre informatique stricto sensu et la guerre de l'information. Sans oublier le fait que le pays est considéré comme le meilleur au monde en matière de cyber-renseignement du fait des capacités des 7 500 opérateurs de l'unité 8 200 – l'équivalent de la NSA pour Israël.[181]

Le pays a pris la mesure de l'opportunité et des enjeux que représente le cyberespace. Le pays entend donc bien rester à l'avant-garde, et il devra pour cela se concentrer sur sa propre résilience aux attaques. Il s'agira par exemple de définir quels sont les réseaux vitaux à protéger et quelles sont les mesures à prendre lorsqu'une attaque survient.

2.5 ROYAUME-UNI

Le Royaume-Uni est l'un des pays européens les plus connectés : il comptait 64,7 millions d'habitants fin novembre 2015, dont 59,3 millions utilisaient Internet, soit un taux de pénétration de 91,6%.

Grande puissance européenne, aux côtés de l'Allemagne et de la France, le Royaume-Uni a massivement investi dans le domaine de la cybersécurité et de la cyberdéfense, que ce soit en matière législative au sujet de

[174] Cohen, Matthew S., Charles (Chuck) D. Freilich and Gabi Siboni. (2015) Israel and Cyberspace: Unique Threat and Response. International Studies Perspectives, doi: 10.1093/isp/ekv023

[175] http://www.lefigaro.fr/conjoncture/2011/07/14/04016-20110714ARTFIG00405-israel-nouvel-eldorado-des-start-up.php

[176] http://www.dcoi-conference.org/#!Executive-Cyber-Intelligence-BiWeekly-Report-Jan-15th-2016/c1nz1/5698fae60cf20ee37c77086c

[177] Cohen, Matthew S., Charles (Chuck) D. Freilich and Gabi Siboni. (2015) Israel and Cyberspace: Unique Threat and Response. International Studies Perspectives, doi: 10.1093/isp/ekv023

[178] Cohen, Matthew S., Charles (Chuck) D. Freilich and Gabi Siboni. (2015) Israel and Cyberspace: Unique Threat and Response. International Studies Perspectives, doi: 10.1093/isp/ekv023

[179] La Méditerranée intelligente, Notes et documents ANIMA, Novembre 2005.

[180] http://seekingalpha.com/article/189500-israel-s-r-d-spending-is-tops-in-the-world

[181] http://www.atlantico.fr/decryptage/comment-israel-reussi-lutter-contre-terrorisme-grace-aux-reseaux-sociaux-eric-denece-facebook-twitter-dark-net-web-internet-2672382.html#oLv2LoTS7uDbMzTR.99

la protection des infrastructures critiques ou de la certification des produits. Le pays joue donc un rôle moteur, tant au niveau de l'Union européenne que de l'OTAN. Mais au-delà d'un certain seuil, la participation du Royaume-Uni à l'approfondissement de l'Union se heurte à son désir de souveraineté. Si le capacity building ne soulève que peu de difficultés de ce point de vue, il n'en va pas de même pour la mutualisation ou le partage capacitaire.

2.5.1 Perception des menaces globales et cyber

La première menace perçue reste, comme dans nombre de pays européens, celle du terrorisme, à la suite des attentats de 2015 à Paris. La propagation de cette menace via le cyberespace est ainsi venue nourrir les tensions entre les pays européens et les plateformes d'intermédiation. Tout au long de l'année 2015 les déclarations combinées des directeurs du MI5 et de la police britannique autour des problématiques liées au terrorisme n'ont eu de cesse que de montrer du doigt les plateformes internet en les présentant comme des zones de non-droit au sens où les forces de l'ordre ne pouvaient pas intervenir. Un discours qui a permis au pays d'adopter, le 4 novembre 2015, le projet de loi Investigatory Powers Bill.[182] Dans l'objectif de lutter contre les criminalités les plus graves telles que le terrorisme ou la pédophilie, ce projet de loi prévoit notamment un renforcement des pouvoirs de surveillance de la police et des services de renseignement permettant, l'obligation pour les fournisseurs d'accès à internet à conserver l'intégralité des données de connexion de leurs clients, le renforcement des pouvoirs de censure du régulateur des télécommunications anglais Ofcom ou encore le renforcement des pouvoirs du ministère de l'intérieur pour l'interdiction.[183] Ce texte a été et est toujours source de vifs débats au sein des parlementaires considérant qu'il est trop intrusif et imprécis. C'est pourquoi, une nouvelle version du projet avec des aménagements a été proposée le 1er mars 2016 par le ministère de l'intérieur britannique. Loin de faire l'unanimité, certains considèrent que les aménagements proposés sont « cosmétiques ».[184]

Ce discours a également permis au Royaume-Uni, dans un contexte de dilution de la souveraineté, notamment face au poids des géants du net, de réaffirmer un peu plus ses ambitions. Pour le Royaume-Uni et les Etats européens, l'un des enjeux majeurs est en effet la préservation de leur souveraineté face aux plateformes d'intermédiations qui ont pris une place cruciale dans nos économies. Principalement américaines et représentées par les GAFAM (Google, Apple, Facebook, Amazon, Microsoft), elles agissent au niveau transnational, alors que les pouvoirs publics s'étendent eux sur des territoires bien précis, plus limités que les plateformes et leur siège.

L'année 2015 marque à cet égard un tournant avec la décision de la Cour de justice de l'Union européenne (CJUE) d'invalider l'accord Safe harbor, dit « Sphère de sécurité », qui encadrait – depuis le 26 juillet 2000 et la décision n°2000/520CE de la Commission européenne – les transferts de données personnelles de citoyens européens vers les Etats-Unis. Cette décision qui résulte de l'arrêt « *CJUE C-362/14 Maximillian Schrems/ Data Protection Commissionner* », témoigne de l'enjeu que représentent les compétences extraterritoriales de la législation américaine pour l'Union européenne, mais aussi du rôle accru de la société civile partout où le débat démocratique est possible. Hannes Ebert et Tim Maurer dans leur article « Revendications sur le cyberespace et puissances émergentes » démontraient qu'au *« niveau international, le type de régime joue un rôle considérable sur les cyberpolitiques. C'est un cas d'école de la façon dont les acteurs nationaux exigent que le gouvernement leur rende des comptes, comme il est de mise dans un système démocratique »*[185].

Ce mouvement en faveur d'une protection accrue des données à caractère personnel et de protection de la vie privée se traduit aussi en un bras de fer avec le géant Google. Le gouvernement britannique et l'autorité administrative de protection des données personnelles ont en effet suivi la jurisprudence de la CJUE et ont ordonné à Google d'appliquer le droit au déréférencement de façon extraterritoriale dans le sens de l'arrêt de la CJUE.

[182] http://www.parliament.uk/business/bills-and-legislation/draft-bills/
[183] http://www.lemonde.fr/pixels/article/2015/05/28/au-royaume-uni-une-nouvelle-loi-pour-renforcer-les-pouvoirs-de-surveillance_4642317_4408996.html
[184] http://www.lemonde.fr/pixels/article/2016/03/01/malgre-les-critiques-le-gouvernement-britannique-durcit-son-projet-de-loi-sur-le-renseignement_4874652_4408996.html
[185] Hannes EBERT, Tim MAURER, « Revendications sur le cyberespace et puissances émergentes » *Hérodote*, 2014/1 n°152-153, p.276-295.

2.5.2 Les enjeux numériques pour le Royaume-Uni

Du point de vue technologique

La technologie est au cœur des débats, notamment sur la question du chiffrement. La position des autorités gouvernementales à cet égard est assez "dure". Dès janvier 2015, suite aux attaques de Charlie Hebdo, le Premier ministre britannique annonçait vouloir limiter le chiffrement via une interdiction, ou tout au moins une obligation pour les entreprises de donner les clés de sécurité aux autorités lorsque celles-ci le demandent. En septembre, le directeur du MI5 déclarait dans une interview que les plateformes avaient une responsabilité dans la surveillance des activités terroristes sur Internet. Tandis qu'un mois plus tard, le chef de la police britannique déclarait que les plateformes freinaient à la fois les enquêtes en matière de terrorisme en refusant de coopérer mais aussi l'élaboration d'un projet de loi visant à obliger les entreprises à aider les forces de l'ordre à intercepter et à déchiffrer les données des utilisateurs.

Du point de vue politique et économique

De façon générale, la politique du gouvernement britannique est très volontariste vis-à-vis des entreprises du net et cherche à leur imposer un nombre important de contraintes. On constate en outre un mouvement contradictoire en matière de protection de la vie privée : d'une part, le renforcement des pouvoirs des forces de l'ordre au nom de la sécurité nationale et de la lutte contre le terrorisme, et, d'autre part la recherche d'une application stricte du droit à l'oubli. Il en résulte une position délicate pour les entreprises qui doivent à la fois fournir, sur convocation, toutes les informations sur leurs utilisateurs, et assurer la protection de la vie privée des utilisateurs.

En matière de protection des données à caractère personnel et de protection de la vie privée, le pays n'hésite pas non plus à s'opposer à Google. En témoigne la demande d'application du droit au déréférencement total sur l'ensemble des réseaux et pas seulement les réseaux européens.

Du point de vue militaire

La collaboration entre le Royaume-Uni et les Etats-Unis, révélée au grand jour par PRISM en 2013, s'est intensifiée dès le début de l'année 2015 dans le cadre de la lutte contre les menaces numériques. Le Royaume-Uni possède une relation privilégiée avec la première cyberdéfense du monde et ses capacités s'en trouvent renforcées.[186]

Le Royaume-Uni possède ainsi non seulement des capacités de cyberdéfense, dont l'objectif est de prémunir les installations stratégiques d'attaques potentiellement terroristes, mais également des capacités offensives susceptibles de lui permettre d'intervenir sur un réseau adverse. A cet égard, un plan d'amélioration du système de sécurité britannique, baptisé « Plan National de Cybersécurité », devrait voir prochainement le jour, selon une annonce du ministre anglais des finances, George Osborne fin novembre 2015.

Suites aux attentats du 13 novembre à Paris, la priorité est désormais la prévention de l'évolution des attaques terroristes et le gouvernement britannique entend y consacrer un budget de 2,9 milliards de dollars à l'horizon 2020. Dans ce cadre, le ministre indiquait que les agents d'espionnage britanniques travaillaient déjà à développer leurs capacités offensives à l'encontre de l'Etat Islamique (EI).[187]

Le Royaume-Uni bénéficie d'une situation particulière, entre son grand allié américain et l'Union européenne, dont il fait encore bel et bien partie malgré les menaces de « Brexit ». Ses capacités cybernétiques profitent de l'expertise de ces deux entités et en font l'une des nations les plus expérimentées sur le cyberespace.

[186] http://www.reseaux-telecoms.net/actualites/lire-cyberdefense-les-etats-unis-et-le-royaume-uni-tournent-le-dos-a-l-europe-continentale-27134.html
[187] http://www.haaretz.com/world-news/1.686614?utm_source=Sailthru&utm_medium=email&utm_campaign=New%20Campaign&utm_term=*Situation%20Report