Lettre mensuelle – Novembre 2019 - disponible sur omc.ceis.eu

Table des matières

ANALYSES

1. QUEL AVENIR POUR LES NÉGOCIATIONS INTERNATIONALES SUR LA RÉGULATION DU CYBERESPACE ?

En octobre 2018, après 20 ans de discussions pour la promotion de la stabilité dans le cyberespace au sein des Nations Unies marquées notamment par plusieurs cycles de négociations du Groupe d'Experts Gouvernementaux (GGE)[1], les efforts de régulation du cyberespace prennent une nouvelle dimension. La Première Commission de l'Assemblée générale de l'ONU a en effet approuvé l'adoption de deux résolutions parallèles et concurrentes dont l'objectif affiché est pourtant le même : poursuivre les avancées entreprises par les cycles de négociation précédents, y compris dans la définition de comportements responsables pour les États dans le cyberespace. La première résolution, portée par la Fédération de Russie, propose comme cadre des discussions un groupe de travail à composition non limitée, ou *Open-Ended Working Group* (OEWG), qui a donc été lancé en 2019. La seconde résolution, soutenue par les États-Unis, créé un sixième GGE, également lancé en 2019.

Or si tous les États ont reconnu la nécessité de réguler leur comportement dans le cyberespace, ils – et en particulier les États porteurs des deux résolutions concurrentes – sont néanmoins en désaccord sur la manière dont le droit international doit s'appliquer au cyberespace. De nombreuses questions se posent alors : la création de deux groupes reflète-t-elle deux visions, opposées sinon distinctes, de la paix, de la sécurité et de la stabilité dans le cyberespace ? Le vote ayant mené à la création de ces deux groupes de travail ne constitue-t-il pas une remise en cause du format initial des négociations internationales au sein de l'ONU, opposant à l'approche restreinte des premiers GGE un nouveau modèle plus ouvert, mois inclusif ? Ces deux cycles de négociations parallèles peuvent-ils donc devenir une source de conflits majeurs ? Que peut-on vraiment attendre de ces nouveaux cycles de négociations ?

1. Les aléas des négociations internationales, reflets de visions divergentes de la paix et de la stabilité du cyberespace ?

1.1. Une multiplication des cadres de négociations au service de projets concurrents

Les négociations internationales sur la régulation du cyberspace ont, depuis leurs débuts en 2013, toujours cristallisé les tensions diplomatiques entre les principaux acteurs étatiques du cyberespace. Ainsi, les avancées des premiers cycles du GGE sont autant le fruit de consensus entre des visions parfois difficiles à

[1] Le détail de la composition limitée du GGE figure dans le tableau Partie 1, sous-partie 1.1.

concilier de la paix et de la stabilité du cyberespace, que leur échec en 2017 ne témoigne de l'exacerbation de ces divergences[2].

C'est en effet l'échec de ce dernier cycle qui a conduit la Russie à proposer une résolution devant permettre la création d'un groupe de travail plus large. La Russie s'appuyait sur deux arguments : d'une part l'échec du dernier GGE démontre que le modèle était arrivé à bout de souffle, et d'autre part la composition restreinte de ce groupe est symptomatique de ce que la Russie qualifie « d'accords de club » non démocratiques au sein de l'ONU, qui n'ont pas lieu d'être et qui biaisent les discussions. Dans le compte-rendu de la 12e session de la Première Commission (2017), le représentant de la Fédération de Russie confiait ainsi « *avoir l'impression que la défense, « en petit comité », de l'application du droit international existant au cyberspace est un moyen de couvrir des actions de force dans le domaine sensible de l'information d'origine spatiale* »[3].

Sans surprise, les États-Unis et leurs alliés ont vivement critiqué la proposition russe et ont défendu *a contrario* leur propre proposition de relance des négociations dans le cadre d'un nouveau GGE. Pour autant, une majorité suffisante d'États semble avoir vu l'intérêt que pourrait représenter la mise en place de deux groupes de travail, pour que les deux résolutions aient pu être approuvées simultanément.

Ceci n'est pas sans soulever un certain nombre de questions sur la pertinence et l'efficacité de cette double démarche. D'abord, la délimitation des mandats des deux groupes n'est pas totalement lisible. Lors de son discours de juin 2019, l'ambassadeur Andrey Krutskikh, représentant de la Fédération de Russie déclarait "*It is important to ensure that this process is complementary, non-confrontational, constructive and based on cooperation*"[4] tout en rappelant que le mandat de l'OEWG était plus large que celui du GGE. Le nouveau groupe ne devait ainsi pas être perçu comme une simple plateforme de discussions mais bien comme un organe de l'Assemblée générale avec un véritable mandat, chargé de trouver des solutions concrètes et de rendre universelles les règles et normes adoptées jusque-là, par l'ONU et au-delà. Mais qu'en est-il de la réalité ? N'y a-t-il pas un risque de redondance avec les travaux parallèles du GGE ? Et comment établir un consensus à 193 États au sein de l'OEWG ? Au moins 20%[5] des premières discussions ont en effet montré des divergences d'opinion entre les membres, notamment sur la nécessité ou non d'élargir le cadre juridique actuel.

[2] En 2013, le premier rapport du GGE reconnaissait l'applicabilité du droit international au cyberespace et élaborait un ensemble de normes. En 2015, le deuxième rapport présentait des règles propres à la sécurité et la stabilité dans le cyberespace mais séparait cette fois-ci le droit international des normes. En 2017, aucun consensus quant à l'interprétation du droit international n'était trouvé au sein du groupe restreint qu'est le GGE.

[3] https://www.un.org/press/fr/2017/agdsi3586.doc.htm

[4] https://rusemb.org.uk/article/541

[5] https://ethicsandtechnology.org/oewg-on-cybersecurity-first-week-of-the-open-ended-working-group-at-the-un-in-new-york/

	GGE	OEWG
Création	2014 avec l'historique suivant : - GGE 2004/2005 : A/RES/58/32 - GGE 2009/2010 : A/RES/60/45 - GGE 2012/2013 : A/RES/66/24 - GGE 2014/2015 : A/RES/68/243 - GGE 2016/2017 : A/RES/70/237	2018 (résolution A/RES/73/27)
Format	Huit-clos (présidence : Brésil)	Public et inclusif (présidence : Suisse)
Membres	En général, entre 15 et 25 pays participants. En 2013, la France, les États-Unis, la Chine, le Royaume-Uni et le Brésil étaient parmi les participants ; Traditionnellement, les 5 membres permanents du Conseil de sécurité de l'ONU ont un siège. Les autres sièges sont attribués selon une certaine balance géopolitique et après étude des demandes officielles déposées par les États. Un expert par État est ensuite nommé.	Les 193 pays membres de l'ONU peuvent prendre part au groupe ; Consultations auprès de la sphère privée, des ONG et du monde académique via des réunions intersessions.
Mandat	Nouveau mandat pour 3 ans (résolution A/RES/73/266 pour 2019-2021)	Pas de réelle limitation de mandat mais résolution A/RES/73/27 pour 2019/2020
Missions	Dans la continuité des anciens travaux du GGE : - Adoption de normes, principes, règles et mesures de confiance menant à une vision commune d'un comportement responsable des États dans le cyberespace ; - Applicabilité du droit international.	- Réflexion sur les normes existantes, voire la création de nouvelles normes et mesures de confiance ; - Applicabilité du droit international ; - Établir un cadre international de discussions ouvert au sein de l'ONU ; - Capacité à contrôler les infrastructures TIC.

Les deux groupes de travail parallèles : GGE et OEWG

1.2. La multiplication des acteurs de la régulation, remise en cause des efforts étatiques ?

Pour ajouter à cette confusion, d'autres acteurs, non étatiques, ont dans le même temps multiplié leurs initiatives en faveur de la régulation du cyberespace, dans la droite ligne du « *multistakeholder environment* » prôné par la *Global Commission on the Stability of Cyberspace* (GCSC). En effet, si les acteurs privés ne peuvent encadrer la responsabilité des États directement – n'étant pas des acteurs du droit international en tant que tel – ils peuvent en revanche faire pression sur ces derniers au travers de leurs propres initiatives. Les travaux de la GCSC (groupe international d'experts[6]), du CyberPeace Institute (ONG), de l'ICT4Peace (fondation), du Charter of Trust de Siemens ou encore de Digital Peace Now de Microsoft[7] (pétition appelant les dirigeants à créer des règles afin d'instaurer la paix numérique) témoignent de cet engagement de la société civile en faveur d'une régulation du cyberespace, et par la même, d'une certaine façon, d'une remise en cause de l'efficacité des négociations internationales conduites dans les enceintes multinationales au niveau étatique.

1.3. L'élaboration de nouvelles normes, point d'achoppement des négociations internationales ?

Plusieurs pays ont réaffirmé lors des premières réunions de l'OEWG que le rapport 2014/2015 du GGE, qui permis l'élaboration d'un certain nombre de normes, devait être le point de départ des discussions dans ce

[6] Ils sont issus de la société civile, des gouvernements, des secteurs privés ou du monde académique visant à proposer une série de normes de comportement responsable pour le cyberespace.

[7] https://digitalpeace.microsoft.com

nouveau cadre de travail élargi. Ces pays considéraient ainsi que les discussions menées dans le cadre de l'OEWG, plutôt que de porter sur l'élaboration de nouvelles normes potentiellement contradictoires avec celles créées par les premiers GGE ou de créer de nouvelles normes s'y ajoutant, devaient donc surtout avoir vocation à rendre plus claires les normes actuelles et à faciliter leur application aux systèmes nationaux. Autrement dit, l'élaboration de nouvelles normes ne semble plus aujourd'hui être une priorité pour la plupart des pays acteurs des négociations internationales « *sauf à ce qu'elles servent à préciser dans leur champ matériel les dispositions existantes. Et encore, tout dépend de la façon dont elles sont rédigées* »[8].

« *We're not starting from scratch* » [“*Nous ne partons pas de zero”*], tel était donc le leitmotiv de l'OEWG à l'occasion de sa première réunion. Des 25 normes initialement proposées dans le projet de résolution sur la création de l'OEWG, il n'en subsiste que 13 dans la résolution 73/27 de 2018 portant création de l'OEWG. Ces 13 normes sont basées sur celles présentes dans le rapport du GGE de 2015 et sur une disposition de la partie « droit international » du même rapport. Parallèlement, certaines propositions actuellement débattues au sein de l'OEWG reprennent les recommandations de la GCSC (8 normes proposées) telles que la protection du noyau public d'Internet[9].

On comprend que, malgré des divergences marquées sur les objectifs de régulation du cyberespace, il semble exister une volonté partagée d'œuvrer pour un environnement stable et un cyberespace « *safe and secure* ». A ce titre, la discussion sur les mesures de confiance, moins contraignantes que les normes et plus flexibles, témoignent d'une volonté de trouver des moyens de faciliter la mise en œuvre des normes existantes. Celles-ci peuvent cependant également s'avérer source de tensions ou du moins de désaccords puisqu'elles ne sont appréhendées de la même manière par les deux groupes de négociations. Alors que la Russie entend développer ces mesures au sein de l'OEWG, les États-Unis et leurs alliés estiment en revancge que ce rôle revient aux organisations régionales.

Les débats parallèles au sein du GGE et de l'OEWG pourraient ainsi amener des résultats divergents, voire difficilement compatibles, sur l'applicabilité du droit international dans le cyberespace, rendant la situation plus complexe qu'elle ne l'était auparavant.

2. Les initiatives internationales de régulation du cyberspace, un projet voué à l'échec ?

A cette multiplication de dispositions juridiques s'ajoute désormais d'autres obstacles d'ordre géopolitique. Différentes visions de l'Internet et le jeu de puissances viennent complexifier le tout. Néanmoins, force est de constater que la reprise des négociations dans le cadre des Nations Unies et la publication de doctrines juridiques sur l'application du droit international aux cyberopérations par certains États constituent des avancées positives pour la paix et la sécurité dans le cyberspace.

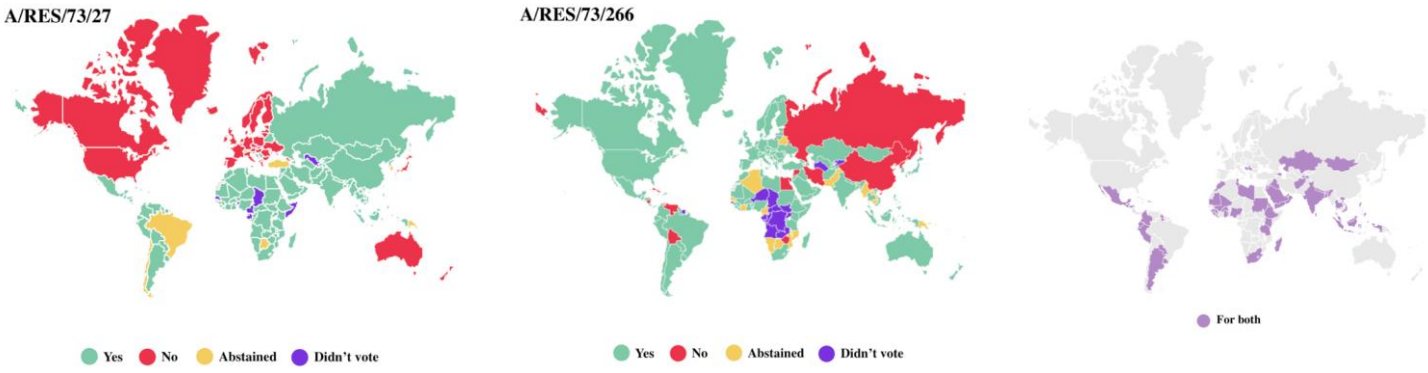
[8] Échange avec Aude GÉRY, Chercheuse à GEODE (centre de recherche et de formation sur la datasphère)

[9] Norm 1: “State and non-state actors should neither conduct nor knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace”. Rapport final de la GCSC, Novembre 2019.

2.1. La multiplication des initiatives internationales, facteur potentiel de blocages critiques

L'émergence de deux groupes de travail concurrents pourrait aboutir à deux situations dommageables pour la régulation des comportements des États dans le cyberspace.
D'abord, un risque de blocage des négociations, sans doute l'option la plus probable. Au sein de l'OEWG, les pays partisans du GGE pourraient ainsi volontairement bloquer les discussions pour ralentir voire provoquer l'échec de ce groupe plus large dont ils contestent l'existence même. Parallèlement, les entreprises privées signataires ou soutiens du Tech Accord, de la Convention de Genève numérique ou de l'Appel de Paris, *a priori* plus favorables au GGE qu'à l'OEWG – et que le mandat de ce dernier autorise à consulter –, pourraient s'en abstenir ou soutenir le blocage des pays porteurs du GGE. Ensuite, un blocage de fond pourrait survenir entre le GGE et l'OEWG si ces derniers adoptent des propositions divergentes voire opposées à l'issue de leur mandat.

On peut craindre aussi, et il s'agirait sans doute de la situation la plus critique pour l'avenir des négociations internationales, une remise en cause par l'OEWG des principes adoptés lors des précédents GGE. A cela s'ajouterait l'adoption de nouveaux principes plus conformes aux visions russes ou chinoises de la gouvernance du cyberespace[10] mais contradictoires avec celles portées par les pays partisans du GGE. Cependant, ce dernier scénario semble à ce jour peu probable au regard des positions ambiguës des alliés de la Chine et de la Russie lors du vote sur l'adoption des résolutions concurrentes sur l'établissement de deux groupes parallèles. L'Inde et l'Afrique du Sud – pays membres des BRICS – se sont par exemple prononcées en faveur des deux groupes de travail. Le Brésil s'est quant à lui abstenu sur la résolution proposée par la Russie, tout en votant en faveur de celle soutenue par les États-Unis.



(A/RES/73/27 pour résolution de la Russie et A/RES/73/266 pour résolution des États-Unis. Source : https://www.diplomacy.edu/blog/discussing-state-behaviour-cyberspace-what-should-we-expect)

2.2. De nouvelles initiatives pour un nouveau souffle ?

Malgré les divergences, la reprise des négociations au sein des Nations Unies et la création de l'OEWG peuvent présenter des perspectives positives :

[10] https://www.cyberscoop.com/un-cyber-norms-general-assembly-2019/

D'une part, l'implication d'une plus large communauté d'États et la possibilité pour le secteur privé de formuler auprès de ces derniers des propositions dans le processus de régulation pourraient s'avérer bénéfiques pour maintenir la paix et la sécurité dans le cyberespace. A ce titre, de nombreux États d'Amérique du Sud, d'Afrique, du Moyen-Orient ou d'Asie du Sud-Est ont exprimé leur volonté de faire progresser l'application de normes de comportement dans le cyberespace indépendamment des divergences idéologiques sur la gouvernance du cyberespace. Par ailleurs, ces mêmes États, rejoints par d'autres (telle l'Estonie) ont indiqué souhaiter que le GGE et l'OEWG travaillent de manière complémentaire dans les prochaines années[11]. Les organisations régionales qui seront consultées tant au sein de l'OEWG qu'au GGE devraient avoir un rôle important à jouer dans cette complémentarité ;

D'autre part, la résolution A/RES/73/266 portée par les États-Unis prévoit que les États participant au GGE devront communiquer au groupe un document (qui sera annexé aux propositions du GGE) présentant leur vision juridique[12], ce qui devrait inciter les États participants mais aussi les autres États membres de l'OEWG souhaitant collaborer avec le GGE à publier leur vision de l'application du droit international au cyberespace. Ces publications présenteront l'avantage de clarifier les visions communes ou divergentes et pourraient servir de base concrète pour trouver un consensus en cas de litige ou pour éviter une escalade des conflits. Pour l'heure, les États suivants ont publié leur vision :

- Les Pays-Bas[13] ;
- Le Royaume-Uni[14] ;
- L'Australie[15] ;
- L'Estonie[16] ;
- Les États-Unis[17][18].

Parmi ces positions, la vision française[19] a été saluée par certains commentateurs pour sa clarté et sa cohérence dans l'application des normes internationales au cyberespace[20]. Sa contribution devrait permettre de faire avancer les débats et pourrait être une source d'inspiration pour des États qui n'auraient pas encore

---

[11] https://www.un.org/press/fr/2019/agdsi3636.doc.htm

[12] https://undocs.org/en/A/RES/73/266

[13] https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis/ ; https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace

[14] https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century

[15] https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/chapters/annexes.html#Annex-A

[16] https://www.justsecurity.org/64490/estonia-speaks-out-on-key-rules-for-cyberspace/

[17]https://www.law.berkeley.edu/wp-content/uploads/2016/12/BJIL-article-International-Law-and-Stability-in-Cyberspace.pdf

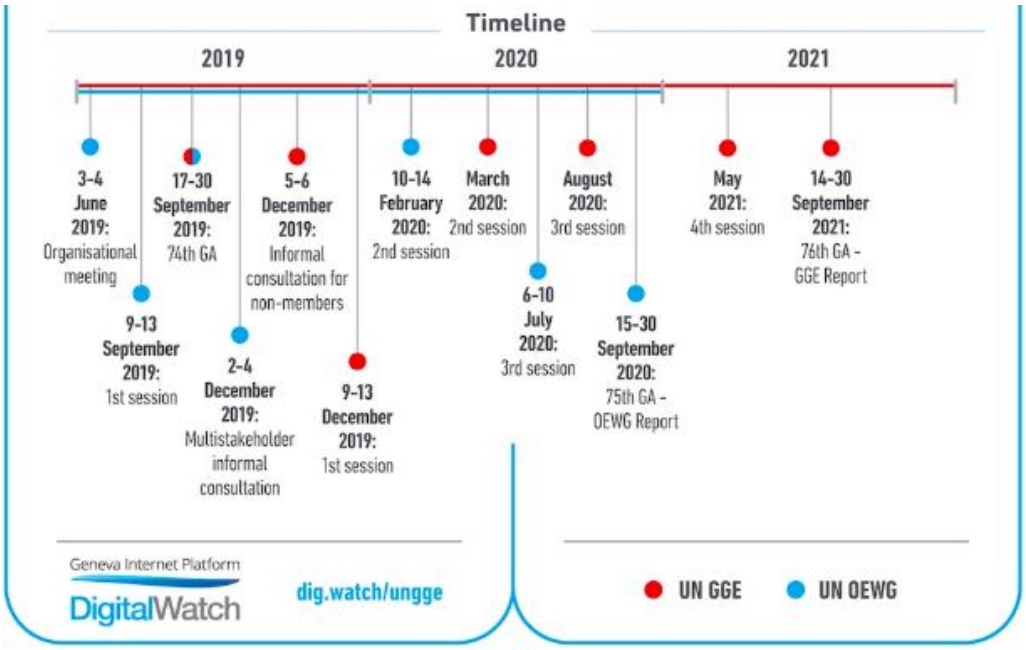
18 https://2009-2017.state.gov/s/l/releases/remarks/197924.htm

[19] https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqu%C3%A9+aux+op%C3%A9rations+Cyberespace.pdf

[20] https://www.justsecurity.org/66194/frances-major-statement-on-international-law-and-cyber-an-assessment/

matérialisé leur vision[21]. La parole de la France devrait ainsi recevoir une attention particulière des autres États, que ce soit dans le cadre du GGE ou dans l'OEWG, lors des négociations à venir.

NB : Échéances à venir



(Source : https://dig.watch/processes/un-gge)

[21] https://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-ii/

2. LA CHINE, « LE NOUVEAU GRAND-FRÈRE » EN AFRIQUE ?

On observe depuis une dizaine d'années une accélération du développement des relations diplomatiques, économiques et technologiques de la Chine avec de nombreux pays d'Afrique.

Sur le plan diplomatique, les tentatives de rapprochement des autorités chinoises avec leurs homologues africains passent par des événements sino-africains tels que le Forum sur la Coopération sino-africaine (FOCAC) et le *China-Africa Peace and Security Forum,* auquel des représentants de 50 pays d'Afrique (sur 54) ont participé à Pékin en juillet 2019.

Dans le même temps, les investissements chinois sur le continent vont croissant, notamment dans les infrastructures et les parcs industriels. Selon le ministère du Commerce chinois, 3 milliards de dollars ont été investis annuellement en Afrique par Pékin depuis 2015[22]. Une somme qu'il faut mettre en regard avec les 132 milliards de dollars de dettes contractées par le continent auprès de Pékin selon l'institut américain *The China Africa Research Initiative* [23]. Si la Chine devient plus regardante sur la soutenabilité financière des projets qu'elle soutient en Afrique, elle ne réduit pour autant pas son implication locale. Le président chinois XI Jinping a d'ailleurs annoncé lors du FOCAC de septembre 2018 que son pays consacrerait 60 milliards de dollars supplémentaires au développement économique des pays africains[24].

La manne financière chinoise se double pour les pays africains de ventes de matériels, notamment dans le domaine des télécommunications et du numérique, qui passent désormais aussi à travers les Nouvelles Routes de la Soie lancées en 2013 par XI Jinping et qui constituent un multiplicateur de l'influence chinoise en Afrique. Cette influence dans le numérique et les télécommunications s'étend en réalité au-delà des simples partenariats technologiques et financiers : elle instaure une véritable dépendance technique et humaine.

1. Une mainmise grandissante sur les infrastructures de télécommunications

La mainmise chinoise en Afrique dans le secteur du numérique est aujourd'hui une réalité, les infrastructures télécom étant désormais quasiment exclusivement d'origine chinoise[25].

Si la Chine a pris le dessus en tant que fournisseur d'infrastructures télécom sur le continent africain, c'est notamment parce qu'en tant qu'ancien pays émergent elle sait offrir des produits adaptés aux contextes locaux et à des prix souvent inférieurs à ceux de la concurrence occidentale. Le marché africain, en pleine croissance et souvent délaissé par les anciennes puissances tutélaires, représente un débouché non négligeable pour

---

[22] https://www.capital.fr/economie-politique/la-chine-promet-60-mds-de-dollars-au-developpement-de-lafrique-1305327

[23] https://www.jeuneafrique.com/mag/619267/economie/dette-le-casse-tete-chinois/

[24] https://www.jeuneafrique.com/623983/economie/forum-sino-africain-pekin-promet-60-milliards-de-dollars-pour-le-developpement-de-lafrique/ ;

Les 60 milliards ont ensuite été répartis en 5 milliards de dollars d'aide gratuite et sans intérêts, 35 milliards de dollars de prêts préférentiels et de crédits à l'exportation, 5 milliards de dollars de fonds supplémentaires pour le Fonds de développement Chine-Afrique, et 10 milliards de dollars de financement pour une coopération de capacité de production sino-africaine, https://www.lesechos.fr/19/07/2018/lesechos.fr/0302004048984_la-chine-est-de-plus-en-plus-omnipresente-en-afrique.html

[25] Voir aussi les nombreux débats mis en ligne sur Youtube, parmi lesquels :
Afrique - Chine : le piège de la dépendance ? https://www.youtube.com/watch?v=4Fk7FfVRabg,
La Chine est-elle en train de faire main basse sur l'Afrique ?: https://www.youtube.com/watch?v=mZ2O3gUTmuE.

les produits chinois qui font face à un ralentissement de la consommation intérieure chinoise. Les géants chinois du numérique comme Huawei ou ZTE ont d'autant plus entrepris d'exporter vers l'Afrique que les dirigeants du continent sont plus ouverts aux conditions des échanges chinois (transferts de personnels chinois, prise en charge de la construction et de la maintenance des infrastructures par des opérateurs chinois etc.) que l'Union européenne et *a fortiori* les Etats-Unis.

Depuis 2013, les échanges sino-africains peuvent s'inscrire dans le programme des *Nouvelles routes de la Soie*. Ainsi, parallèlement au développement des infrastructures portuaires, routières et ferroviaires, la Chine investit considérablement dans les infrastructures et systèmes de télécommunication (câbles sous-marins et dorsales terrestres, cœurs de réseau, satellites… jusqu'aux terminaux) [26], essentiels pour soutenir ses activités dans d'autres secteurs clés du continent, comme les mines, l'agro-business, le commerce en ligne, et de plus en plus d'applications numériques (e-santé, e-éducation, etc.).

Les entreprises chinoises (équipementiers, opérateurs, spécialistes de la fibre optique ou des antennes mobiles) sont désormais particulièrement nombreuses dans les salons dédiés aux télécommunication, comme Africacom, le plus grand événement africain avec 15 000 participants au Cape (Afrique du Sud) en 2019[27].

Le géant des télécoms Huawei opère déjà dans le secteur des réseaux télécoms d'une vingtaine de pays africains. Il réalise ainsi 15 % de ses revenus sur le continent, et forme chaque année 12 000 étudiants africains en télécommunications dans des centres en Angola, au Congo, en Égypte, au Kenya, au Maroc, au Nigeria et en Afrique du Sud[28]. Il domine largement le secteur avec ses réseaux 3G/4G, les fibres télécoms et les téléphones portables dont il possède 15 % du marché. De nouveaux acteurs sont aussi en train de percer dans toutes les technologies numériques, comme par exemple le domaine de l'intelligence artificielle.

La Chine devrait encore accroître son avance avec le lancement du projet « Pakistan East Africa Cable Express » (PEACE), un câble sous-marin de télécommunication reliant l'Asie et l'Afrique. La société chinoise Hengtong construit en effet un nouveau câble qui reliera d'ici 2021, le Pakistan, Djibouti, le Kenya, l'Égypte et la France. Long de 12.000 km, le câble sera plus tard doté d'une extension vers l'Afrique du Sud (*cf. Fig. 1*).

[26] https://www.latribune.fr/technos-medias/telecoms/telecoms-la-chine-a-l-assaut-de-l-afrique-797975.html
[27] https://tmt.knect365.com/africacom/
[28] https://www.jeuneafrique.com/mag/453084/economie/cherche-chine-investissant-autant-afrique/

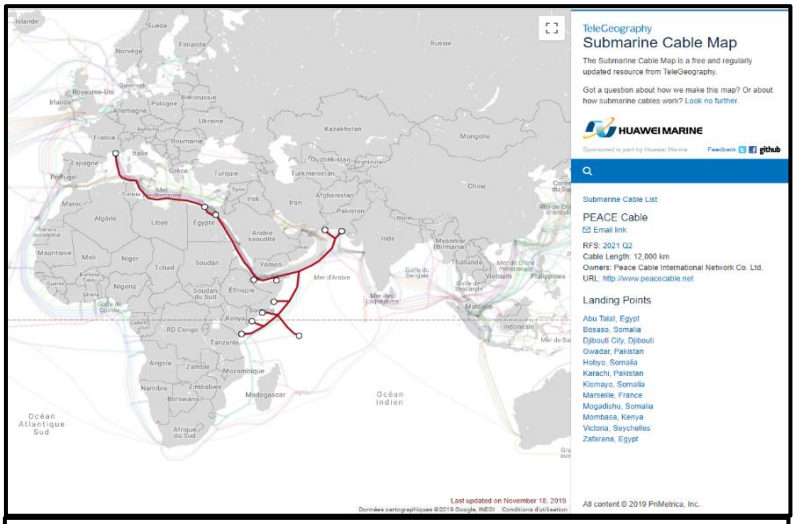


Figure 1 :https://www.submarinecablemap.com/#/submarine-cable/peace-cable

2. La présence accrue de personnels et de ressources humaines

Le continent africain représente un débouché considérable pour la Chine, non seulement pour les produits et services chinois, mais aussi pour la main d'œuvre masculine chinoise. En effet, les infrastructures et services exportés sont gérés sur place par des équipes chinoises, employés permanents ou prestataires de service : en 2019, 160 000 ressortissants chinois résideraient sur le continent, tous secteurs d'activité confondus[29]. Par exemple, la société China Cybersecurity, qui dépend de la China *Electronics Technology Cybersecurity* (CETC) dispose de personnels notamment au Sénégal, en Algérie, en Namibie et en Ethiopie[30].

La CETC organise également depuis 2010 des formations techniques à destination des personnels locaux. Son blog précise notamment que la société s'intéresse particulièrement aux pays francophones (*cf. Fig.2)*.

[29] http://mini.eastday.com/mobile/190408033531986.html#

[30] La CETC est une entreprise publique qui dépend du ministère de l'Industrie et des Technologies de l'Information (MIIT). Elle développe des logiciels et des matériels de communication tels que des équipements réseaux et des systèmes d'opération ; dans le domaine militaire elle développe notamment des radars de défense aérienne et des systèmes de transmission satellitaires. Elle participe aussi à la construction d'infrastructures : des hôtels aux camps militares, en passant par des usines de ciment.
http://en.cetc.com.cn/enzgdzkj/products/ternational_trade38/index.html

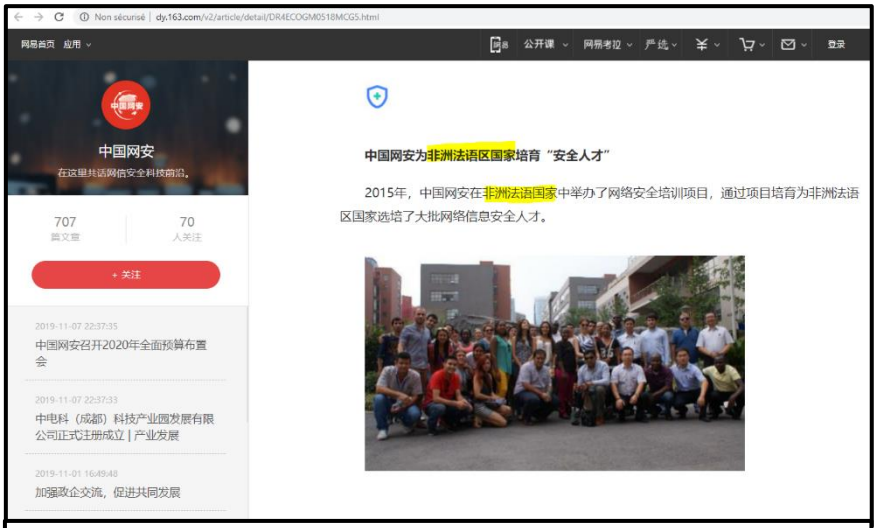


Figure 2 : http://dy.163.com/v2/article/detail/DR4ECOGM0518MCG5.html

L'initiative « Jeunes scientifiques et techniciens africains innovants en Chine » (非洲青年科技人员创新中国行) par exemple, fait partie de ces programmes de fidélisation des futures élites africaines. Dix-huit pays prennent part à l'initiative, dont l'Egypte, le Kenya, l'Afrique du Sud, l'Ethiopie et la Tanzanie entre autres[31]. La formation d'un nombre grandissant d'étudiants africains en Chine ou localement par des entreprises chinoises, constitue donc un risque, parce que ces étudiants pourraient, d'une part, devenir des défenseurs des intérêts chinois, d'autre part accepter, à terme, de partager des informations avec les autorités chinoises.

3. Un risque stratégique pour les intérêts africains et français

Le risque humain est aggravé par la mainmise chinoise sur les réseaux télécom africains qui présente de réels risques stratégiques pour les intérêts tant africains que français[32].

D'abord, le quasi-monopole technologique de la Chine sur les infrastructures de télécommunication rend possible la surveillance des réseaux et facilite les actions ciblées d'espionnage ou de perturbation du service (déni de service, action sur l'intégrité des données, etc.), voire d'appui à des opposants armés par les services chinois. D'ailleurs, en janvier 2017, à Addis-Abeba, les informaticiens de l'Union africaine (UA) ont découvert ce qui semblait être une opération chinoise d'espionnage de grande ampleur[33]. En effet, l'intégralité du contenu des serveurs du siège de l'UA, offerts en 2012 par le gouvernement chinois, était en fait transférée en Chine via des backdoors.

Considérant qu'un nombre croissant de pays tels que la Zambie, l'Éthiopie et le Zimbabwe, se dote d'équipements de surveillance des réseaux de communication en faisant appel à des entreprises chinoises pour mettre en place des systèmes de contrôle d'Internet et des réseaux de télécommunication, le risque d'intrusion est bien réel. Ces pays augmentent par là-même leur exposition aux manœuvres techniques

[31] http://www.cac.gov.cn/2019-05/08/c_1124464905.htm

[32] https://www.lemonde.fr/afrique/article/2018/09/04/la-chine-s-appuie-sur-l-afrique-pour-construire-une-muraille-face-aux-pays-occidentaux_5350032_3212.html

[33] https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html

chinoises. De surcroît, les personnels, institutions et organisations français présents dans les pays africains, notamment francophones, pourraient devenir la cible des interférences de la Chine. Et ce, d'autant plus que la France et d'ores et déjà une cible des services de renseignement chinois. De ce point de vue, l'attention portée par la CETC aux pays d'Afrique francophones est peut-être significative.

Le risque d'exposition est régulièrement dénoncé par les services de renseignement occidentaux, notamment anglo-saxons, en raison des liens entre les grands conglomérats chinois et l'Armée populaire de libération[34], et a conduit plusieurs pays à interdire certains produits ou technologies chinois dans leurs réseaux les plus sensibles.

L'influence et l'implication de la Chine dans les domaines du numérique et des télécommunications sur le continent africain constituent un risque stratégique non négligeable pour les pays d'Afrique. Pourtant, sur le continent africain comme souvent en Europe, les considérations financières se substituent aux enjeux stratégiques.

FOCUS INNOVATION

HIAsecure : l'authentification par l'intelligence humaine

La société

HIAsecure, créée en 2017 par Marc Olivier notamment, rassemble aujourd'hui une équipe de 7 personnes dont 4 experts en cybersécurité.

La création de la société HIAsecure part du constat que la majorité des méthodes d'authentification par mots de passe sont sujettes à des fraudes massives, entraînant non seulement de nombreux problèmes de sécurité, mais aussi un manque à gagner conséquent pour les sociétés victimes. Selon les fondateurs, la plupart des méthodes d'authentification sont faillibles car elles reposent sur l'authentification d'un objet, et non d'un individu : les systèmes d'authentifications se contentent en effet de vérifier que l'authentifié possède bien les logins et mots de passe, non que la validation est bien effectuée par un être humain.

L'objectif était donc double : replacer l'Humain au centre du processus d'identification, et protéger les données de l'utilisateur en prévenant les tentatives d'attaques basées sur l'IA.

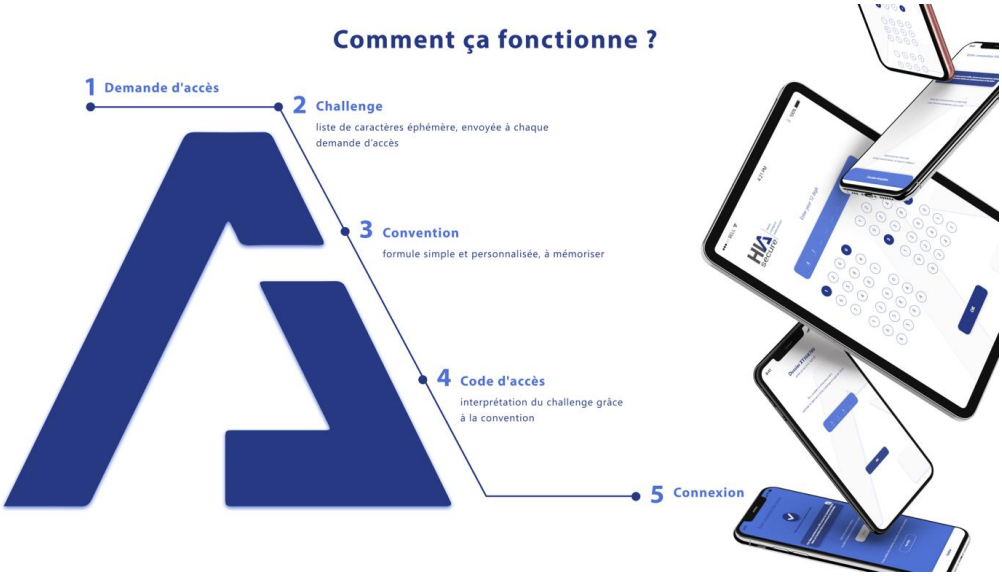
L'innovation

La solution HIAsecure repose ainsi sur une technologie d'authentification qui utilise les processus cognitifs spécifiques à l'être humain. Plus précisément, elle s'appuie sur la génération, par l'utilisateur même, de codes à usage unique pour l'accès à des services ou la validation de transactions. Ces codes ne sont générés que si l'utilisateur résout, pour chaque demande d'accès ou de validation d'une transaction, un challenge

[34] https://www.lopinion.fr/edition/international/l-armee-populaire-est-acteur-majeur-relation-sino-africaine-160865

(consistant en une suite de symboles et de caractères), sur la base d'une convention, c'est-à-dire d'instructions de lecture du challenge, qui lui sont remises une seule et unique fois lors de sa première utilisation et qui lui sont propres et confidentielles.

Le système d'authentification d'HIAsecure fonctionne de la façon suivante :



Source : HIAsecure

Ces challenges, très faciles à résoudre pour tout utilisateur sur la base de sa convention personnelle, sont au contraire extrêmement difficiles à résoudre par une machine ou une intelligence artificielle puisqu'ils constituent des « moving target ». Cette technique de défense a pour objectif de changer constamment la surface de la cible, de sorte que l'attaquant ne puisse pas reproduire un schéma connu. Innovante dans le sens où elle met l'attaquant dans une situation incertaine et imprévisible, cette solution rend une attaque couteuse et quasiment impossible.

Applications

La solution d'authentification HIAsecure permet de

- Sécuriser une authentification, en s'assurant que c'est bien la personne qui possède la convention qui est authentifiée ;
- De réduire les risques d'une authentification frauduleuse sur un service grâce à une solution d'authentification mouvante et donc extrêmement difficile à résoudre par un attaquant et/ou une intelligence artificielle ;
- De compléter une solution d'authentification déjà existante (biométrie, mot de passe/login, etc.).

Après avoir obtenu la note de 72/100 sur la plateforme RateAndGo, HIAsecure a réalisé en décembre 2018 une levée de fonds de 2 millions d'euros.

Finaliste du concours BPI des innovateurs en juillet 2019, la société HIAsecure participera au FIC 2020 et entend s'attaquer prochainement au marché bancaire.

CALENDRIER

17-18/01 : La Fabrique Défense

Visant à l'affermissement du lien armée-Nation et à la constitution d'une culture stratégique européenne, la première édition de **La Fabrique Défense**, évènement tourné vers la jeunesse, se tiendra **les 17 et 18 janvier 2020** au Paris Event Center (Porte de la Villette).

Pilotée par la Direction générale des relations internationales et de la stratégie (DGRIS) du ministère des Armées, **La Fabrique Défense** a pour ambition de **réunir l'écosystème de la défense** (institutions, associations, entreprises, think tanks et académiques) afin d'**échanger avec les jeunes de tout horizon (18-30 ans)** dans le cadre notamment de tables rondes, d'un forum des métiers et d'espaces de présentation des innovations de la Défense.

Outre **la multiplication d'évènements labellisés « La Fabrique Défense » en régions**, cette initiative du ministère des Armées est également mue d'**une ambition européenne**, avec l'organisation prochaine de rendez-vous thématiques (Politique de sécurité et de défense commune, maîtrise des armements, etc.) dans d'autres pays de l'Union européenne.

ACTUALITÉ

Signature d'une convention Cyber entre le ministère des Armées et les industriels de défense

La ministre des Armées a signé le 14 novembre une convention Cyber avec huit industries de défense (Airbus, Ariane Group, Dassault Aviation, MBDA, Naval Group, Nexter, Safran et Thales).

Concrétisant le souhait de la ministre des Armées de **construire une cyberdéfense *« de bout en bout »***, exprimé lors du **Forum international de la cybersécurité de 2019**, la convention a notamment été rédigée par le Commandement de la cyberdéfense et la Direction générale de l'Armement. Elle formalise les engagements mutuels du ministère et des principaux acteurs de la BITD française sur la densification de leur dialogue et la sécurisation des systèmes de productions industriels ; dans une perspective d'**appréhender**

collectivement les cyberattaques qui viseraient directement ou « par ricochet » le ministère, les industriels fournisseurs et les chaînes de sous-traitance.

Première étape d'une transformation du modèle de cyberdéfense, la convention Cyber repose sur :

1. le **partage d'informations** au sein d'un « cercle de confiance » afin de faciliter la réactivité des échanges de données sensibles ;
2. l'établissement d'une **gouvernance partagée** pour traiter le cyber de façon plus transversale ;
3. une meilleure **acculturation** et **sensibilisation** aux problématiques liées au cyber ;
4. la volonté commune de **maîtriser les risques cyber** sur toute la chaîne de soutien de défense.

Alors que des **groupes de travail thématiques** vont prochainement se former pour mettre en œuvre la convention (et devront présenter annuellement leurs avancées), la ministre des Armées a d'ores-et-déjà déclaré qu'un suivi tout particulier sera consacré à **« l'ingénierie des systèmes d'armes, l'anticipation et la détection des attaques, les composants et sous-traitants critiques »**.

Pour plus d'informations : Discours de Florence Parly sur la signature de la convention Cyber entre le ministère des Armées et les représentants de 8 grands maitres d'œuvre industriels de la défense.

La **Direction Générale des Relations Internationales et de la Stratégie (DGRIS)** propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation. Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique**, sous le numéro de marché 1502492543. Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère des Armées
Direction Générale des Relations Internationales et de la Stratégie
60 Boulevard du Général Martial Valin – CS21623 – 75 509 Paris Cedex 15

CEIS
Tour Montparnasse – 33, avenue du Maine – BP 36 – 75 755 - Paris Cedex 15
Téléphone : 01 45 55 00 20
E-mail : omc@ceis-strat.com