POLICY CENTER FOR THE NEW SOUTH
THINK • STIMULATE • BRIDGE

Policy Brief
November 2019, PB-19/41

Le Cyberespace africain : un champ aux contradictions manifestes

Par Mourad El Manir

Abstract

L'évolution du cyberespace s'est traduite par son intégration dans le champ des relations internationales à travers les transformations introduites dans les concepts de la Puissance, de la dissuasion et de la souveraineté. Dans cet environnement aux multiples facettes, l'Afrique, dont la digitalisation est en nette expansion, tente d'y prendre pied sans être préparée ni en termes de ressources humaines judicieusement formées, ni sur le registre des infrastructures physiques et informatiques nécessaires. Le continent est également handicapé par le manque d'outils et d'instruments pour faire face aux menaces et aux risques générés par le développement du cyberespace.

La présente étude vise à faire ressortir le degré de préparation du continent africain pour faire face aux défis posés par le cyberespace à travers l'examen de la situation cybernétique africaine, sous le prisme des avancées enregistrées et des vulnérabilités relevées, avant d'aborder les propositions susceptibles de permettre au continent africain de mieux prendre en charge l'enjeu cybernétique.

Introduction

Le prix du meilleur roman africain de science-fiction au titre de l'année 2017 a été remporté par Tade Thompson pour son livre intitulé "Rosewater" qui aborde la lutte contre les cyber-fraudes au Nigéria en 2066. Cette référence à un roman de science-fiction n'est pas fortuite dans la mesure où le mot "cyberespace", inspiré du mot "cybernétique", fut utilisé, pour la première fois, en 1984, par l'auteur de romans de science-fiction William Gibson, pour désigner "Une hallucination consensuelle vécue quotidiennement en toute légalité, dans tous les pays, par des gosses auxquelles on enseigne les concepts mathématiques."

Le rapprochement entre ces deux romans vise à montrer

que **l'Afrique a intégré dans son présent et surtout dans son avenir l'évolution fulgurante des technologies d'information et de communication**, qui a généré une véritable transformation de la société et de l'économie mondiale.

Au-delà des aspects techniques du cyber-espace, la cyber-attaque contre l'Estonie en 2007, a élevé le cyberespace au rang de théâtre d'opération militaire au même titre que les milieux aéroterrestre et maritime et la conflictualité dans ce milieu n'est plus perçue comme un affrontement de technologies, mais comme "l'utilisation des moyens numériques à des fins de contrôle de la volonté de l'adversaire", rejoignant, en cela, la célèbre formule du théoricien allemand Carl Von Clausewitz "la guerre n'est que le prolongement de la politique par d'autres moyens".

Cette conflictualité du cyberespace est confortée par la multiplication des cyber-attaques intervenues dans le champ des affrontements globaux1, par l'institutionnalisation de capacités de défense cybernétiques et par les dynamiques internationales de régulation de l'espace cybernétique.

L'évolution du cyberespace s'est traduite aussi par son intégration dans le champ des relations internationales à travers les transformations introduites dans les concepts de la Puissance, de la dissuasion et de la souveraineté.

Dans cet environnement aux multiples facettes, l'Afrique, dont la digitalisation est en nette expansion, tente d'y prendre pied sans être préparée ni en termes de ressources humaines judicieusement formées, ni sur le registre des infrastructures physiques et informatiques nécessaires. Le continent est également handicapé par le manque d'outils et d'instruments pour faire face aux menaces et aux risques générés par le développement du cyberespace.

La présente étude vise à faire ressortir le degré de préparation du continent africain pour faire face aux défis posés par le cyberespace à travers l'examen de la situation cybernétique africaine, sous le prisme des avancées enregistrées et des vulnérabilités relevées, avant d'aborder les propositions susceptibles de permettre au continent africain de mieux prendre en charge l'enjeu cybernétique.

I. Des avancées indéniables

La rentrée de l'Afrique dans l'ère numérique est une réalité incontestable. En effet, sur les trois indicateurs adoptés à l'échelle internationale, les chiffres réalisés par le continent sont prometteurs.

Ainsi, en à peine quelques années, le taux d'accès de la population à Internet a enregistré une avancée exponentielle. Au 30 juin 2019, ce taux atteignait 39,8% alors qu'il n'était que de 5% en 2007[2], la moyenne mondiale étant de 57,3%. D'après le cabinet Deloitte, l'Afrique compte aujourd'hui 450 millions d'africains connectés (sur 1,2 milliard) via leur Smartphone. Sur le nombre d'utilisateurs actifs de Facebook, l'Afrique se prévaut de 211 millions (janvier 2019) soit une progression de 15% par rapport à 2018. La région la plus connectée reste l'Afrique du Nord. Enfin, sur le taux de pénétration de la téléphonie mobile, qui constitue la porte d'entrée de l'Afrique dans le monde digital, le continent comptera 660 millions équipés d'un Smartphone en 2020, soit le double qu'en 2016.

En termes d'avancées, il y a lieu de souligner aussi le développement d'une économie numérique, notamment dans les secteurs bancaires (l'Afrique est bien positionnée dans le registre de "mobile banking"), les services en ligne, les télécommunications, les médias, les assurances mais aussi dans les secteurs de l'éducation et de la culture ou de la santé. Dans ce cadre, les revenus issus de la téléphonie mobile représentent 3,7% du PIB sur le continent africain, soit le triple de ceux des économies développées.

Même dans le domaine de l'intelligence artificielle, le continent est en passe de conquérir une part de ce marché d'avenir. En juin 2018, l'entreprise américaine Google a annoncé l'ouverture d'un centre de recherche en intelligence artificielle au Ghana pour inclure cette technologie dans les programmes de formation et de développement.

Le spécialiste américain du Big Data, l'entreprise SAS, a annoncé l'investissement d'un milliard de dollars en Afrique pour financer la formation des ressources humaines et l'accès des opérateurs locaux aux dernières technologies liées à l'intelligence artificielle.

1. Tableau détaillé des cyber-attaques en Annexe

2. www.internetworldstats.com

Dans ce domaine, le Togo accueillera du 16 au 17 décembre 2019, un symposium régional sur le thème pour "pour une intelligence artificielle (IA) éthique et inclusive au service du développement durable, de la paix et de la sécurité en Afrique de l'Ouest", en marge duquel sera posée la première pierre de l'Agence francophone de l'intelligence artificielle (Afria) à Aneho.[3] Ce symposium intervient après le 1er forum africain sur l'intelligence artificielle organisé par l'Unesco en décembre 2018 à l'université polytechnique de Ben-Guerrir au Royaume du Maroc.

Par ailleurs, certains pays africains ont enregistré des évolutions substantielles dans des secteurs très pointus comme celui de la Block-Chain.[4]. L'Afrique du Sud a mis sur pied la « Blockchain Academy" qui offre des formations sur les crypto-monnaies et la technologie de Blockchain. Le Kenya a mis sur pied un groupe de travail sur cette technologie en particulier et sur l'intelligence artificielle comme moyen d'optimiser la gestion publique. Au Nigéria, des organisations se multiplient pour la maitrise de l'environnement des monnaies numériques. En Ouganda, le gouvernement est fortement impliqué dans l'introduction de la Block-Chain dans le secteur bancaire en vue de réduire les couts opérationnels et les risques. La Sierra- Leone se prévaut de l'utilisation de la Block-Chain dans la gestion des processus électoraux. Sur le plan des législations, les gouvernements africains mettent progressivement en place des mesures sous forme de lois, d'organisations spécialisées et d'infrastructures pouvant assurer la protection numérique du grand public (entreprises et citoyens). En plus du volet juridique, plusieurs Etats africains ont mis en place des autorités nationales compétentes en la matière ainsi que des équipes opérationnelles de réponse immédiates.

Dans un rapport sur les évolutions en cyber-sécurité, rendu public en 2017, l'Union internationale des télécommunications (UIT), a précisé que plusieurs pays africains ont mis en place de bonnes pratiques de renforcement des capacités de lutte contre la cybercriminalité.

La question cybernétique est également prise en charge par certaines organisations régionales. La CEDEAO (Communauté économique des Etats de l'Afrique de l'Ouest) a mis en place une initiative régionale qui organise régulièrement des forums sur des sujets relatifs à la cyber sécurité et la SADC (Communauté de développement de l'Afrique Australe) coordonne les efforts de ses Etats membres pour renforcer la cyber-sécurité en Afrique Australe.

Sur le plan continental, l'Union africaine a adopté "la convention sur la cyber- sécurité et la protection des données à caractère personnel ", à l'issue de la 23ème Assemblée des chefs d'Etat et des gouvernements de l'Union africaine, tenue à Malabo les 26 et 27 juin 2014. Cette convention appelée "Convention de Malabo" a pour but de mettre en place un cadre juridique pour la cyber sécurité et la protection des données personnelles.

Compte tenu de l'importance de cette question, l'UA a inscrit la cyber-sécurité en tant que programme phare de l'Agenda 2063, traduisant le souci d'incorporer dans les plans africains de développement, les changements provoqués par les technologies émergentes, en veillant à ce qu'elles soient utilisées par les particuliers, les institutions et les Etats dans de bonnes conditions de sécurité.

Sur le plan opérationnel, l'Africa-CERT, lancé le 30 mai 2010 à Kigali au Rwanda, vise à aider les pays africains à créer et à mettre en place des équipes de sécurité informatique et d'intervention en cas d'incident. Il y a lieu de préciser que les pays africains membres de l'OCI (Organisation de la Conférence Islamique) bénéficient de l'expertise de "l'OIC- CERT"

Dans le domaine de la cyber-défense, les acquis, bien que modestes, ont le mérite d'exister. Ils sont encadrés par des initiatives privées. Les pays de l'Afrique Australe organisent, de manière bisannuelle, un forum portant le nom "Africa Cyber Defence Summit".[5] Par ailleurs, des études sont menées, actuellement, pour procéder à l'ouverture de trois centres d'opérations de cyber-défense, au Nigéria, à l'Ile Maurice et au Sénégal, en plus de celui déjà ouvert en Afrique du Sud.

Il reste que si les avancées cybernétiques africaines sont

3. Marie –France Réveillard "la première agence pour l'intelligence artificielle en Afrique francophone siégera au Togo". La tribune.fr, le 12 septembre 2019.

4. Block-Chain peut être défini comme la technologie de stockage et de transmission d'information, transparente, sécurisée et fonctionnant sans organe central. C'est une sorte de base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création en 2008.

5. Francois-Xavier Djimgou "Souveraineté numérique et cyber-défense : un enjeu de taille pour l'Afrique". Editions Edilivre. 2019.

une réalité tangible, les vulnérabilités ne le sont pas moins.

II. Des vulnérabilités persistantes

Sur le plan technologique, le continent enregistre une inégalité dans l'accès à l'espace numérique. En effet, certaines régions et une grande partie de la population sont totalement absentes du cyberespace, de ses enjeux et de ses retombées économiques. Cette situation est due à la faiblesse des infrastructures nationales, rendant une connexion à internet onéreuse : en République centrafricaine ou en Guinée, une connexion haut débit peut couter jusqu'à 500 dollars par mois.
Dans le même registre, l'Afrique connaît une fissure cybernétique entre les Etats[6] ayant massivement investi dans le cyber (infrastructures, concepts d'emploi, moyens) quand d'autres manquent de ressources nécessaires pour assurer une protection minimum. Cette déficience a été mise en évidence par une enquête de la Commission de l'Union Africaine sur les tendances de la cyber sécurité et de la cybercriminalité en Afrique qui a souligné que seulement 15 pays africains ont mis en place une législation en matière de cybercriminalité.

Ces conclusions ont été largement réitérées lors de l'"AfricaSEC 2019", tenue à Marrakech, les 8 et 9 février 2019, qui a relevé que les Etats africains sont divisés entre trois tendances : La majorité n'a entrepris aucune démarche alors qu'une minorité a mis en place des mesures concrètes, tandis qu'au milieu, un groupe d'Etats a adopté des instruments juridiques sans actions concrètes.

En termes de cyber-nuisance, l'Afrique remporte la palme de la cybercriminalité. Cette situation ne cesse d'être dénoncée[7].

Elle est induite par l'accessibilité d'internet, le développement de la 3G/4G, l'anonymat sur le web, le manque de sécurisation de certaines infrastructures critiques et sensibles ainsi que par le manque de sensibilisation à la cyber-sécurité des acteurs évoluant dans les Entreprises et des populations.

Dans ce registre, le panorama cybercriminel-istique africain est particulier. Il inclut le piratage des serveurs téléphoniques, communément appelé "phreaking", le piratage des systèmes d'informatiques avec demande de rançon "ransomware", la manipulation du trafic d'un site internet avec le but de dérober des informations confidentielles, le "pahrming" ainsi que la cyber escroquerie dans ses différentes formes, allant de l'arnaque aux sentiments au chantage à la vidéo, en passant par les faux visas ainsi que les fausses offres d'emploi et de bourses d'études.

La cybercriminalité ciblant les entreprises englobe les atteintes aux systèmes de traitement automatisé de données, les violations de données personnelles, les atteintes à l'e-réputation ainsi que la contrefaçon de marques et de logiciels.

Cette cybercriminalité africaine à un coût. Il est énorme. La société de cyber-sécurité kenyane Serianu qui a diligenté un audit en partenariat avec plus de 700 institutions publiques et privées africaines, fait état de chiffres alarmants. Rien que pour l'année 2017, la cybercriminalité continentale a engendré des préjudices financiers considérables : le Nigéria (649 millions de dollars), le Kenya (210 millions de dollars) ou encre la Tanzanie (99 millions de dollars). Au total, le continent a enregistré une perte de 3,5 milliards de dollars pour l'année 2017.

D'un autre côté, le continent enregistre une déficience criante en matière de cyber-défense. L'incident le plus significatif porte sur les révélations de l'espionnage du siège de l'union africaine par la Chine de janvier 2012 à janvier 2017. L'affaire, rapportée par la presse mondiale, fait état que des dispositifs chinois mis en place lors de la construction du Quartier Général de l'Union Africaine, par des entreprises chinoises avec des systèmes informatiques livrés clés en main, permettaient de transférer chaque nuit, l'intégralité du contenu des serveurs du bâtiment de l'organisation africaine vers des ordinateurs situés à Shanghai. L'Etat chinois aurait eu accès non seulement à l'ensemble des documents produits par l'organisation, mais également aux lignes téléphoniques et aux micros des visioconférences installés sur le site.

Le leadership africain est également ciblé par d'autres pays comme l'a mis en évidence le journal français "le

6. Au sein même des Etats africains, la fissure cybernétique existe entre les zones urbaines et les zones rurales.

7. Lors du "4ème Africa Cybersecurity Conference d'Abidjan", tenue les 3 et 4 octobre 2019, les intervenants ont déploré que "l'Afrique reste le continent le plus exposé à la cybercriminalité"

Monde" qui avait publié une enquête sur les plateformes occidentales de recherche des informations sur les hauts cadres africains.[8]

Sur la question du cyber-terrorisme, dans le sens de l'utilisation réseaux sociaux pour véhiculer des messages de haine, le recrutement de djihadistes ou la collecte de financements occultes, les experts restent sceptiques, en avançant que dans beaucoup de pays africains, touchés de plein fouet par le terrorisme (Nigéria, Niger, Tchad, Soudan, Ethiopie, Somalie), le taux d'abonnement au téléphone mobile est inférieur aux moyennes africaines.
Dans son livre "l'Afrique, Nouvelle frontière du Djihad", Marc-Antoine Pérouse de Montclos précise que "des sondages réalisés auprès d'anciens combattants de Boko Haram dans des camps déplacés au Nigéria ont montré qu'aucun d'entre eux n'a été recruté en ligne"[9].

Concernant les enjeux internationaux liés au numérique, l'Afrique enregistre un retard considérable sur la question stratégique des Datacenter, dans le sens d'infrastructures de stockage et de traitement de données. L'enjeu est de maintenir les données stratégiques et les données personnelles sur le sol africain. Actuellement, le continent ne compte que 80 Centres de Données dont la moitié est implantée en Afrique du Sud. La situation est telle qu'une importante part des données africaines est stockée et exploitée en dehors du continent. Sur ce sujet, une importante bataille est engagée sur la future mise en place des Datacenter africains, dans laquelle les pays anglophones, particulièrement ceux ayant un accès à la mer (proximité des câbles marins) ont la prééminence. Il y a lieu de signaler que le Royaume du Maroc est en passe de se positionner comme un hub pour les Datacenter au Nord de l'Afrique.

Par ailleurs, le besoin africain en investissements et en transfert de technologies dans le domaine cybernétique place l'Afrique dans une posture de vulnérabilité extrême, à tel point que des experts n'hésitent pas à parler de "cyber-colonialisme". Ce concept est défini comme "la politique ou la pratique permettant de prendre le contrôle total ou partiel du cyberespace d'un pays par des technologies et de l'exploiter économiquement". Le doigt accusateur est dirigé vers les Gafam qui en offrant des services gratuits (Facebook) organisent le secteur du numérique en Afrique pour pouvoir le contrôler à leur profit. L'ONG Global Justice Now a publié en mai 2018, un rapport, au titre évocateur, "Comment l'agenda global du e-commerce annonce le pouvoir des grandes firmes numériques et menace le Sud."

En dernier lieu, le continent africain est confronté au développement considérable des pratiques de manipulation des informations (Fake news), induit par la facilité d'accès à l'Internet et aux Smartphones ainsi qu'au faible taux de sensibilisation des populations. La situation est telle que les "fake news" sont considérées comme une menace à la paix sociale sur le continent, particulièrement[10] en Afrique subsaharienne.

En effet, récemment, la diffusion de fake news a potentiellement :

- déclenché des violences ethniques à cause de photos manipulées de corps de somaliens de souche poussés dans une tombe peu profonde dans la région d'Oromia en Ethiopie ;
- semé la confusion parmi les électeurs du scrutin présidentiel du Nigéria, suite à de fausses informations sur les candidats ;
- provoqué des fluctuations monétaires après la rumeur de la démission du président sud-africain Jacob Zuma.

En tout état de cause, les vulnérabilités cybernétiques africaines, réelles, nécessitent la mise en place d'actions concertées visant à consolider les acquis et à réduire les déficiences.

III. Consolidation des acquis et réduction des déficiences

Compte tenu des enjeux cybernétiques en présence, la mise en place d'une cyber-stratégie africaine, une impérieuse nécessité, passe, d'abord, par l'instauration d'un climat de confiance.

En effet, l'espace cyber est un domaine où la méfiance est de rigueur, compte tenu des révélations sur les écoutes

8. Journal "le Monde", intitulé "Chefs d'Etats, diplomates, hommes d'affaires, le Who'Who des écoutes britanniques en Afrique." Publié, le 08 décembre 2016.
9. Marc-Antoine Pérouse de Montclos, "l'Afrique nouvelle frontière du djihad", éditions la découverte. 2018
10. Ecofin hebdo, "l'explosion des fake news en Afrique, une menace pour la paix sociale et la pérennité des réseaux sociaux." Article publié le 14 février 2019.

et les activités de surveillance auxquelles se livrent les Etats entre eux, en utilisant justement les moyens offerts par le cyber.

Par ailleurs, le continent africain, doit, partir en rangs unis pour, consolider sa digitalisation, en vue de disposer de l'outil qui lui permettra, le cas échéant, de se positionner en acteur efficace et efficient dans l'espace numérique.

Dans ce cadre, il doit relever, dans l'immédiat, trois défis :

- **La connectivité :** bien que le niveau de la connectivité du continent africain est en nette progression, il demeure en deçà des chiffres mondiaux. Dans ce cadre, il y a lieu de renforcer les infrastructures des pays africains de manière à rendre la connexion à internet moins onéreuse.
- **L'infrastructure électrique :** une attention particulière doit être accordée à la résolution des problèmes d'approvisionnement et de délestage électrique, avant d'investir dans les infrastructures nationales des technologies de l'information et de communication.
- **Les équipements :** la numérisation du continent est tributaire de la réalisation des équipements adéquats. Outre leur réalisation, les Etats africains doivent s'approprier la capacité de leur utilisation. Par ailleurs, ils doivent encourager la mutualisation des moyens, pour réaliser des économies d'échelle.

En termes de cyber-menaces, la lutte contre la cybercriminalité, doit être placée en première priorité, en axant l'effort sur la formation et la sensibilisation :

- La formation des spécialistes qui doit englober la formation initiale pour constituer un vivier de professionnels de la sécurité. Elle doit aussi englober la formation continue en vue de renforcer l'expertise des acteurs sur le terrain.
- La sensibilisation à la sécurité de l'ensemble des filières des autres corps de métier de l'informatique, ingénieurs systèmes et réseaux, développeurs, ainsi que tous les citoyens de façon globale, plus particulièrement aux techniques d'ingénierie sociale. Dans le cyber-domaine, chaque utilisateur est un membre actif de la chaine de cyber-sécurité et une chaine n'est jamais solide que par son maillon le plus faible.

La lutte contre la cybercriminalité doit englober aussi des actions opérationnelles portant :

- Généralisation des capacités de réaction. A cet effet, les structures de type CERT (Computer emergency response team), doivent être généralisées à l'ensemble des pays africains. Bien plus, la mise en place d'un centre africain de cyber-opérations comme lieu d'intégration des capacités nationales, est de nature à renforcer la résilience cybernétique.
- Mise à niveau juridique, en apportant un soutien aux pays africains trouvant une difficulté à mettre en place une législation adaptée aux défis cybernétiques. Dans ce domaine, les mécanismes juridiques mis en place doivent accompagner le développement de la technologie et des cyber-nuisances.

Sur le plan de la cyber-défense, talon d'Achille de la cybernétique africaine, l'action doit privilégier la coopération intra-africaine, susceptible d'harmoniser les efforts.

Ce panafricanisme cybernétique passerait par :

- la mise en place d'une structure africaine de cyber-défense, rattachée à l'Union Africaine qui pourra être constituée de représentants des Etats membres mais aussi d'experts de la société civile et du secteur privé africain. Cette structure aura pour mission d'élaborer une vision africaine de la souveraineté numérique ;
- l'amélioration de la protection des réseaux de communication existants ;
- la facilitation des échanges entre les Etats membres des doctrines en matière de cyber- défense;
- l'organisation d'une réflexion pour le développement d'une filière industrielle africaine axée sur le domaine cybernétique, de manière à diminuer la dépendance vis à vis des produits physiques, logiciels et cognitifs développés par les Puissances cybernétiques.
- la mise sur pied d'une plateforme de formation, d'éducation et d'exercices de cyber-défense, dont les budgets de fonctionnement, de recherche et d'investissement doivent être exclusivement africains. Cette mesure est de nature à concrétiser les impératifs de formation et de mutualisation des moyens;
- la promotion de l'adoption du nom de domaine e.Africa, lancé, officiellement, le 3 juillet 2017, qui se veut l'identité numérique du continent. Cette proposition permettrait de préciser les contours de la souveraineté numérique africaine;
- l'intensification du développement des infrastructures d'interconnexion et d'hébergement de données sur le continent. Dans ce cadre, il est

primordial de favoriser la mise en place des serveurs et des Data-Center sur les territoires des Etats africains, au moins pour les données sensibles des gouvernements, dans le cas idéal pour les données personnelles;
- le renforcement de la coopération avec les partenaires internationaux concernés, particulièrement à travers l'échange des bonnes pratiques en matière de gestion de crise.

Conclusion

Le champ des études sur la Sécurité s'est élargi avec la consécration du Cyberespace comme un théâtre de confrontation à part entière, au même titre que la Terre, l'Air, la Mer et l'Espace.

Ce faisant, la cyber-conflictualité qui en découle n'est plus perçue comme un affrontement de technologies mais comme un moyen, un autre, en plus, et/ou en complément, des formes de combat cinétiques et létaux, pour réaliser des objectifs stratégiques.

Par ailleurs, l'espace numérique, qui devenu un espace de tensions culturelles, politiques, sécuritaires et économiques, offre un nouveau cadre pour le jeu des rivalités et de coopération entre acteurs stratégiques, avec pour conséquence une reconfiguration des rapports de forces sur la scène internationale.

Dans ce contexte, les pays africains qui ont réussi, relativement, à amorcer leur digitalisation, ont appréhendé, à quelques exceptions, le cyberespace administrativement, sans prendre conscience des conséquences négatives d'un déficit opérationnel sur leur sécurité nationale.

Certes, des mesures préventives et de protection ont été entreprises pour combattre la cybercriminalité qui gangrène le continent, particulièrement dans son espace subsaharien, cependant l'ampleur du mal est telle que seule une approche continentale et holistique peut en réduire la propagation.

La même approche doit guider la mise en place d'une cyber-défense africaine, talon d'Achille du cyberespace africain, pour permettre aux pays africains de sauvegarder leur souveraineté numérique et de développer une résilience numérique.

Annexe

Aperçu sur les Cyber-attaques annoncées, depuis 2007

Années	Evénements survenus
2007	• Une cyber-attaque cible l'Estonie causant un déni de service prolongé de ses infrastructures stratégiques, des banques et des journaux, sur fond de tension avec la Russie
2008	• La Géorgie en conflit avec la Russie subit de vastes cyber-attaques handicapant toutes les infrastructures de ce pays.
2009	• Plusieurs sites gouvernementaux sud-coréens sont ciblés par des attaques à grande échelle, sur fonds de tensions avec la Corée du Nord
2010	• Une cyber-attaque a mis hors d'état de fonctionnement la centrale nucléaire de Bouchehr. Les Etats-Unis et Israël sont soupçonnés d'être derrière cette attaque
2011-2012	• Le constructeur américain "Lockheed Martin" a été victime d'une cyber-attaque massive qui paralysé ses systèmes informatiques pendant plusieurs heures • Plusieurs comptes Gmail de hauts fonctionnaires américains, des dissidents chinois, des responsables de plusieurs pays asiatiques, des journalistes ont été piratés. Google a déclaré que l'origine de l'attaque est Jinan en Chine. • Une vague d'attaques informatiques cibles plusieurs sites gouvernementaux japonais • Une cyber-attaque d'envergure a ciblé des banques américaines, européennes et latino-américaines causant la perte de plus de 80 millions de dollars • Une cyber-attaque cible les systèmes informatiques de plusieurs firmes énergétiques saoudiennes, attribuée au gouvernement iranien. (Virus Shamoon)

2014	• Un groupe de hackers iraniens a piraté et volé des données confidentielles d'un groupe de loisirs américain dont le propriétaire avait suggéré de raser Téhéran sous le feu nucléaire • Le groupe Sony renonce à la sortie d'un film sur un complot fictif de la CIA pour assassiner le président nord coréen Kim Jong-Un suite à un vol massif de ses données informatiques
2015	• La télévision "TV5 Monde" est victime d'une cyber-attaque entrainant l'arrêt de la diffusion de ses programmes • Le compte Twitter du Commandement américain au Moyen Orient (Centcom) a été piraté par des membres de l'Etat Islamique. • Envoi de menaces de mort, via Facebook, à cinq épouses de militaires américains.
2016	• La Banque centrale du Bangladesh victime d'un piratage informatique a perdu 81 millions de dollars. • Une banque équatorienne est attaquée et a perdu 10,7 millions d'euros • La Russie est accusée d'ingérence dans les élections présidentielles américaines
2017	• Une cyber-attaque de grande envergure (Wanacry) paralyse les ordinateurs de multinationales et de services publics d'une centaine de pays (système de santé britannique, ministère russe de l'intérieur, des entreprises) et fait plus de 200 000 victimes. • Une cyber-attaque (Adylkuzz) s'attaque aux ressources des ordinateurs pour y faire du cryptomoning. L'attaque fait des centaines de milliers de victimes • Une cyber-attaque d'envergure (NotPetya) a ciblé, initialement, des entreprises majeures en Ukraine a paralysé une centaine d'entreprises mondiales. • L' essai d'armes cybernétiques russe perturbe le réseau téléphonique de la Lettonie
2018	• L'infrastructure informatique russe et iranienne est la cible d'attaques informatiques avec des répercussions sur les fournisseurs des services internet et les centres de données • La banque HSBC révèle que des comptes bancaires en ligne de ses clients ont été l'objet d'attaques informatiques • Le ministère français des affaires étrangères annonce qu'il a été l'objet d'une opération de piratage de sa messagerie email.
2019	• Des documents appartenant à des responsables politiques allemands sont publiés en ligne • Airbus annonce avoir été victime d'une intrusion dans le système d'information de sa branche avions commerciaux • les forces de défense israéliennes ont twitté sur leur Compte officiel "nous avons contrecarré une tentative d'attaque cyber de Hamas contre des cibles israéliennes, en frappant l'immeuble utilisé par les hackers de Hamas" • Les Etats-Unis lancent des cyber-attaques contre l'Iran

À propos de Policy Center for the New South

Le Policy Center for the New South: Un bien public pour le renforcement des politiques publiques. Le Policy Center for the New South (PCNS) est un think tank marocain dont la mission est de contribuer à l'amélioration des politiques publiques, aussi bien économiques que sociales et internationales, qui concernent le Maroc et l'Afrique, parties intégrantes du Sud global.

Le PCNS défend le concept d'un « nouveau Sud » ouvert, responsable et entreprenant ; un Sud qui définit ses propres narratifs, ainsi que les cartes mentales autour des bassins de la Méditerranée et de l'Atlantique Sud, dans le cadre d'un rapport décomplexé avec le reste du monde. Le think tank se propose d'accompagner, par ses travaux, l'élaboration des politiques publiques en Afrique, et de donner la parole aux experts du Sud sur les évolutions géopolitiques qui les concernent. Ce positionnement, axé sur le dialogue et les partenariats, consiste à cultiver une expertise et une excellence africaines, à même de contribuer au diagnostic et aux solutions des défis africains.

Lire plus

Les opinions exprimées dans cette publication sont celles de l'auteur.

POLICY CENTER FOR THE NEW SOUTH
THINK • STIMULATE • BRIDGE

Policy Center for the New South

Suncity Complex, Building C, Av. Addolb, Albortokal Street,
Hay Riad, Rabat, Maroc.
Email : contact@policycenter.ma
Phone : +212 (0) 537 54 04 04 / Fax : +212 (0) 537 71 31 54
Website : www.policycenter.ma