CAHIERS AFRICAINS DES DROITS DE L'HOMME ET DE LA DÉMOCRATIE AINSI QUE DU DÉVELOPPEMENT DURABLE
REVUE AFRICAINE INTERDISCIPLINAIRE

ISSN : 2791-1063 (Imprimé)
ISSN : 2791-1071 (En ligne)

26ème année - Numéro 76 - Volume 1 - Juillet-Septembre 2022

L'OPTIMISATION DES INFRASTRUCTURES DE SURVEILLANCE ET DES OUTILS DE SECURITE NUMERIQUE

Par

Guylain NZE BOLEILANGA
Chef de Travaux
Doctorant en Droit économique et social à l'Université de Kinshasa
Juge Permanent au Tribunal de Commerce de Kinshasa/Matete

RÉSUMÉ

Face aux enjeux notamment d'investissements, de concurrence et des politiques publiques, la République Démocratique du Congo doit faire un choix judicieux entre une concurrence basée sur les services, à l'opposé d'une concurrence basée sur les infrastructures. A notre sens, le développement équilibré du réseau national des télécommunications passe par une concurrence basée sur les services[1], dans ce cas, la régulation du partage serait celle qui facilite l'intervention des investisseurs et qui tient compte du principe de participation des collectivités locales.

Dans cette veine, un environnement informatique qui favorise le développement et le partage efficace des infrastructures donne la possibilité à l'administration, en l'occurrence fiscale, de voir ses procédures de recouvrement et de contrôle des recettes s'opérer convenablement. L'automatisation des processus permettant de standardiser les processus communs à toutes les plateformes ainsi que d'automatiser les tâches répétitives, et le personnel informatique peut de cette manière se concentrer sur les résultats plutôt que sur la gestion des plateformes.[2]

Ainsi, au vu de l'importance des infrastructures sur la croissance économique des Etats, des coûts de déploiement qui en découlent, des importants besoins en couverture, de l'existence des réseaux privés qui traversent de vastes zones rurales et dont le maillage dépasse parfois celui des réseaux ouverts au public, la rationalisation du partage des infrastructures trouve dans ce contexte un point d'encrage. Dans un marché largement ouvert à la concurrence, l'Etat voit son rôle réduit principalement à la régulation de toutes les opérations qui se font dans le secteur des technologies du numérique ; la surveillance ainsi que la sécurité des infrastructures appellent la multiplication d'efforts considérables.

Mots-clés *: Cybersécurité, optimisation des outils de sécurité, contre des malveillances informatiques, pour des fins fiscales.*

---

[1] BOUNOUNG ESSONO Sosthène, *Le partage d'infrastructures et la coordination des politiques publiques,* Table ronde sur : « *Quelle régulation du partage d'infrastructures ?* », 7ème Réunion annuelle du Fratel, ART Cameroun, Bruxelles, 2009, pp. 10-14.

[2] IBM, *Optimisation des infrastructures informatiques : une source pour un avantage concurrentiel durable,* 2008, p. 16.

SUMMARY

Faced with the challenges of investment, competition and public policy, the Democratic Republic of Congo must make a judicious choice between service-based competition and infrastructure-based competition. In our view, the balanced development of the national telecommunications network requires service-based competition, in which case the regulation of sharing would be one that facilitates the intervention of investors and takes into account the principle of participation of local authorities.

In this vein, an IT environment that promotes the development and efficient sharing of infrastructure gives the administration, in this case tax, the opportunity to see its procedures for collection and control of revenue operate properly. By automating processes, common processes across platforms can be standardized and repetitive tasks can be automated, allowing IT staff to focus on results rather than platform management.

Thus, given the importance of infrastructure on the economic growth of states, the costs of deployment that result, the significant coverage needs, the existence of private networks that cross vast rural areas and whose mesh sometimes exceeds that of networks open to the public, the rationalization of infrastructure sharing finds in this context an anchor. In a market that is largely open to competition, the role of the State is mainly reduced to the regulation of all the operations that take place in the digital technology sector; the monitoring and security of the infrastructures call for the multiplication of considerable efforts.

Keywords: *Cybersecurity, optimization of security tools, against computer malware, for tax purposes.*

INTRODUCTION

Le boom numérique contribue universellement à l'essor de bien de secteurs, en modifiant les habitudes d'antan ainsi que la mise en mal notamment du principe de la souveraineté territoriale des Etats.

Les plateformes sur lesquelles s'exercent les activités du numérique, du reste dominées par les multinationales et certaines puissances étatiques, ignorent les frontières des Etats. Ce cyberespace donne de frisson aux Etats relativement en ce qui concerne la sécurisation de leurs populations, économies et territoires face notamment aux cyber-attaques qui se sont développées en parallèle du numérique. Certes, il n'y a jamais eu autant de matériels et d'intelligence artificielle au service de la cybersécurité, et pourtant le monde n'a jamais été aussi malmené, notamment par des cyber-attaques constitutives de la force de frappe des terroristes et mises au rang d'armement militaire par certains Etats.

Toutefois, une cyberattaque réussie est rarement le résultat d'une sophistication technologique, elle est souvent la conséquence des transactions d'un utilisateur insouciant ou berné. Ce qui amène à s'interroger sur le fait qu'une cybersécurité efficace est finalement une affaire de culture, dépendant de ce fait d'un Etat à un autre.

L'Etat devrait avoir une attitude de prudence au regard des merveilles de la digitalisation (I), en s'investissant résolument dans le développement des infrastructures de surveillance et des outils de sécurité (II).

I. LA PRUDENCE FACE AUX MERVEILLES DU NUMÉRIQUE

Le mouvement de la digitalisation est de plus en plus marqué dans toutes les organisations et entités du secteur privé ou public. L'utilisation des nouvelles technologies de l'information et de la communication (NTIC), devient un levier incontournable pour le développement économique et social de chaque entité, relevant une nouvelle ère des performances et considérant le développement technologique comme étant l'un des piliers fondamentaux de cette performance.[3]

Sans cesse, les nouvelles technologies de l'information et de la communication poursuivent leur développement, au point qu'il serait hasardeux de prédire ce qu'elles en seront davantage à l'avenir, ainsi que le soutiennent Daniel HARDY, Guy MALLEUS et Jean-Noël MEREUR.[4]

La position desdits auteurs est d'autant plus vraie car, il suffit de se remémorer comment à titre d'exemple, le développement de l'imprimerie a ouvert le domaine du texte écrit à un champ de sujets bien plus vaste que le champ initial du texte écrit, largement concentré sur la matière religieuse, accélérant ainsi la diffusion mais également la création des sciences et de la littérature en tous genres.

Même si la difficulté de prédire avec exactitude le futur du numérique demeure, son ancrage (A) dans la société à l'échelle mondiale ne fait l'ombre d'aucun doute, malgré l'alerte, avertissant sur les divers dangers qui la guette (B).

---

[3] MISOID MAHJOUBA et ELBAHLOULI LAMIAA *(Doctorantes en sciences de gestion - FSJES de Casablanca, Université Hassan II),* « La contribution de la télédéclaration dans l'amélioration de la performance de la Direction Générale des Impôts au Maroc », *Revue du contrôle, de la comptabilité et de l'audit,* n° 8, vol. 3 : n° 4, mars 2019, p. 2.

[4] HARDY Daniel, MALLEUS Guy et MEREUR Jean-Noël (Eds), *Réseaux, Internet, téléphonie, multimédia, convergences et complémentarités,* Lavoisier, 2002, pp. 760-761.

A. L'ancrage de la dématérialisation à l'échelle mondiale

Depuis son invention, son émergence, jusqu'à maintenant, de bout en bout de l'univers, traversant vents et marées, à la vitesse exponentielle, le numérique ne cesse de laisser sur son sillon des merveilles, du reste incontestables.

Les expériences réalisées dans le domaine notamment de la télémédecine satellitaire a donné l'espoir au continent africain lors des assises du sommet de Johannesburg dans le cadre du Nouveau Partenariat pour le Développement de l'Afrique (NEPAD) quant à son entrée dans le monde du numérique.

Ainsi, de l'influence aujourd'hui incontournable de la messagerie e-mail, et bien plus des services à valeur ajoutée et diverses fonctionnalités qu'il ne cesse d'engendrer, l'Internet rythme la civilisation et les comportements, ce grâce à son progrès exceptionnel.

Il faut également ajouter une forte propension du format Html pour la fouille des documentations diverses. De même, par l'accès aux portails pour le grand public, se faisant principalement par des usagers connectés à relativement bas débit, cela a conduit à une modification des pages d'accueil de ces portails vers une simplification et une utilisation minimale de la bande passante.

L'on pourrait valablement s'attendre à une évolution dans le sens inverse d'un contenu de plus en plus riche en éléments multimédia, à mesure que les accès à haut débit deviennent la norme, non seulement pour les entreprises mais également pour les particuliers.

Par ailleurs, la prolifération des accès à haut débit et l'augmentation des débits des réseaux fédérateurs laissent poindre l'arrivée de la visioconférence à grande échelle et de qualité conviviale. En effet, la demande latente dans ce domaine s'est trouvée accélérée par les événements tragiques qui ont frappé les Etats-Unis d'Amérique en septembre 2001, rendant le voyage aérien certainement moins commode et perçu comme insuffisamment sécurisé.

A long terme, la visioconférence peut paver la voie à une réalité virtuelle plus totale encore, impliquant d'autres sens que la vue et l'ouïe. En effet, il est intéressant de constater que le multimédia a jusque-là couvert l'audio et la vidéo, en codant en numérique les éléments analogiques perceptibles par les organes sensitifs tels que l'œil et/ou l'oreille, et en restituant à l'autre bout de la chaine de communication les signaux analogiques et ce, à partir des messages numériques transmis par le réseau.

On entre dans un cycle où il devient possible d'encoder puis de restituer des sensations olfactives ou tactiles ou encore gustatives ; n'étant en rien

limitées par les techniques des réseaux qui en sont tout à fait capables à présent, mais plutôt par manque d'équipements « terminaux » pratiques en périphérie du réseau, agissant comme transcodeurs des informations olfactives ou tactiles ou gustatives. Tous les acteurs, à savoir, les Etats, les entreprises et les particuliers recourent au bienfait de ce nouvel outil de travail qu'est le numérique en raison des avantages qu'il procure en termes d'efficacité, de fiabilité, du temps et moyens à gagner. Mais des alertes sont lancées pour fustiger le côté pervers du numérique.

B. Les alertes contre les dangers

Phénomène nouveau, le numérique n'a pas jusque-là livré tout son secret, un autre phénomène aux répercussions importantes sera celui de la connectivité mobile croissante, par voie d'équipement des personnes ou de leurs véhicules, de moyens d'accès et de communication portables ou embarqués.[5] On parle de l'intelligence artificielle des objets.

Ces développements pourraient infléchir de manière significative des notions aussi importantes que la sécurité personnelle ou l'adaptation du contenu à la localisation géographique de l'utilisateur au moment de l'accès, ou le concept de maintenance de l'automobile, etc. Les techniques de sécurité des réseaux et les fonctions d'authentification, d'autorisation et de chiffrement des communications sont également les conditions nécessaires au développement supplémentaire de l'utilisation du réseau à des fins commerciales, financières, médicales, fiscales ou d'état civil, pour n'en citer que quelques applications.

Et encore avec beaucoup d'acuité, les réseaux de télécommunications constituent aujourd'hui, de manière encore plus prononcée que par le passé, un élément majeur d'infrastructures stratégiques pour les sociétés, les économies ou les Nations. La qualité et le taux de pénétration de ces infrastructures, ainsi que leur robustesse, constitueront une base de différenciation importante entre les sociétés ou les économies mondiales.

Cependant, ce phénomène peut être une source d'opportunités ou de risques, car il appartient à la catégorie d'événements phares qui imposent des virages brutaux par rapport au statut *quo ante*. La prise de ces virages avec succès, ou son échec, peut laisser les participants au jeu mondial du bon ou du mauvais côté du fossé numérique, impactant ainsi leur position de manière durable au sein de leurs sphères respectives.

Evidemment, les TIC ont modifié de façon fondamentale la majorité des entreprises. Les processus d'information et des systèmes d'information constituent un atout essentiel ainsi qu'un différenciateur concurrentiel

[5] HARDY Daniel, MALLEUS Guy et MEREUR Jean-Noël (Eds), *Op. Cit.*, p. 761.

fondamental. La perte ou la compromission de ces informations (ou de la capacité à les utiliser) représente un risque important pour la valeur actionnariale. Elle est bien souvent d'une nature hautement sensible et confidentielle et doit être sauvegardée afin de protéger les relations avec les clients.

Hors de question de faire semblant, les administrations publiques en ce compris, l'administration fiscale, ainsi que les entreprises connaîtront à un moment donné une attaque réussie, qu'elles s'en rendent compte ou pas. Et ces attaques peuvent venir de partout. L'essentiel du battage médiatique autour des solutions de sécurité actuelles se focalise toujours sur le périmètre du réseau. La plupart des attaques passent néanmoins par la grande porte et ne rencontrent jamais le périmètre du réseau.

Pour rester en effet compétitives, les entreprises doivent accélérer leur transformation digitale, tout en garantissant la protection de leur patrimoine d'informations.

La cybersécurité apporte le socle de confiance indispensable à cette mutation ; la plupart des dirigeants d'entreprises du monde l'ont bien compris. De plus en plus sensibles aux risques d'entreprises induits par une menace croissante, ils augmentent en grande majorité leurs investissements en cybersécurité ; chose que font également certains Etats pour leurs administrations.

Notons que même si les machines peuvent avoir leur défaillance, la négligence humaine reste toujours la principale source de risques, avec de lourds impacts potentiels pour les utilisateurs du numérique, à l'Etat de s'activer pour offrir une protection efficace aux infrastructures numériques.

II. LA PROTECTION ÉTATIQUE DES INFRASTRUCTURES NUMÉRIQUES

Lorsqu'on aborde la question de la cybersécurité auprès de toutes sortes d'organisations, quels que soient leurs secteurs d'activités et leur taille, celles-ci ont en général toujours le sentiment de disposer d'une sécurité adéquate ou au moins suffisante de leurs systèmes d'information (SI), tout en étant parfaitement conscientes de leur extrême dépendance à leur système d'information.[6]

[6] POGGIOLI Jean-Paul (Directeur de projet et consultant Médiaterra consultants), « La cybersécurité efficace, une affaire de culture », FIC 2017, 9e Forum international de la cybersécurité, *Une sécurité intelligente pour les technologies du futur,* Revue trimestrielle, janvier 2017, p. 146.

A un moment donné, si rien n'est fait, ce sera la catastrophe, l'État a un rôle à jouer pour enfin définir les niveaux de résilience (A) ainsi que les moyens de leur mise en place (B).

A. La définition d'un seuil de résilience

Tout porte à croire que malgré des efforts de plus en plus importants en matière de sécurité, notamment du fait de la croissance des investissements technologiques dans ce domaine, le danger est loin d'être écarté, bien au contraire, il s'empire chaque seconde.

A ce sujet, le rapport 2016 du ''*Clusif* '' sur les menaces informatiques et pratiques de la sécurité indique que les incidents logiques par malveillance sont toujours en croissance.

Arrivent donc en tête, les infections par virus avec 44% des entreprises concernées, soit 14 points de plus que l'année précédente. Pourtant, 49% de ces mêmes entreprises ne disposent toujours pas d'une cellule de collecte et de traitement des incidents de sécurité de l'information… Près du tiers ne prennent pas en compte la continuité d'activités, alors qu'elles sont conscientes de leur dépendance des systèmes d'information.[7]

Il en découle que la protection des infrastructures du fait de leur fragilité avérée, demeure une préoccupation. Ces infrastructures dites critiques jouissent d'une sécurité informatique pas toujours efficace, mais obsolète.

Raison pour laquelle, il demeure impérieux de renforcer la cybersécurité des infrastructures critiques.

Toutefois, la protection en amont desdites infrastructures ne saurait occulter la mise en place des stratégies de résilience performantes.

Une infrastructure critique est donc celle qui permet à un État de pouvoir fonctionner.

Cette notion recouvre, pour compréhension, plusieurs domaines tels que la santé publique, l'énergie, les services financiers, les transports, l'administration, etc.

Par ailleurs, la résilience est la capacité de se préparer et de s'adapter à un environnement changeant et de faire face à l'insécurité et aux divers risques qui menacent une organisation (pays, administrations ou entreprises). Dans ce cas, la résilience doit être proactive (ou préventive) et réactive.

[7] Lire à ce sujet, CLUSIF : Club de la Sécurité de l'information français, in http://www.clusif.fr/ - Club professionnel, constitué en association indépendante, ouvert à toute entreprise ou collectivité. Sa finalité est d'agir pour la sécurité de l'information, facteur de pérennité des entreprises et des collectivités publiques.

Ainsi, la mesure du degré de « criticité » d'une infrastructure relève de la responsabilité du Gouvernement. Elle nécessite de procéder à une évaluation des risques.

Le monde évolue constamment, et il convient en effet de se protéger tant des menaces actuelles que de celles qui peuvent venir à plus ou moins brève échéance.[8]

C'est vrai qu'il est difficile d'assurer à la résilience des infrastructures critiques, une gouvernance identique pour celles relevant du secteur public et celles relevant du secteur privé.

Les motivations de l'un et de l'autre diffèrent en effet, et cette différence justifie une approche spécifique de chaque secteur et les moyens à mettre en œuvre obéissent à la même approche.

B. Les moyens d'atteinte de la résilience

La détermination des seuils de résilience a un lien avec les moyens à mobiliser pour que l'Etat joue bien son rôle de sécurisation des infrastructures. S'agissant d'un domaine hautement technologique, les moyens de sécurisation les sont aussi.

A ce sujet, il existe toute une panoplie de produits et systèmes informatiques de sécurisation des infrastructures, équipements et systèmes d'information auxquels l'Etat peut recourir.

On peut proposer par exemple :[9]

La « *Defensive Security* » qui répond aux enjeux de sécurisation du système d'information des entreprises et organisations. La sécurité est au cœur des projets de transformation et de digitalisation des entreprises. Son approche consiste en effet à agir avec expertise et méthodologie aussi bien au niveau des infrastructures, des applications que des processus pour la préservation des entreprises.

Par ailleurs, le « *SealCrypt* » permet l'apposition d'une signature électronique sur un document physique ou virtuel. Sous forme d'un code 2D, il rend le document hybride : c'est-à-dire, apporte les garanties d'intégrité et de sécurité de la signature électronique. Le code devient ainsi lisible et authentifiable sur Smartphone/PC afin d'afficher le document d'origine et vérifier la signature.

---

[8] SAIZ Jérôme et al., *Résilience des infrastructures critiques,* FIC 2014, 6e Forum international de la cybersécurité, in *Identité numérique et confiance,* les Actes du Forum, janvier 2014, p. 134.

[9] Consulter à ce sujet, FRANCE CYBERSECURITY, Label France Cybersecurity, Catalogue 2017 des offres labellisées, les offres labellisées / Segmentation, Paris, 2017, pp. 11, 12, 13, 14, 19, 22, 23, 30, 31 et 47.

« *Oodrive* », par contre, à travers sa filiale « *CertEurope* », propose une offre assurant la sécurité et l'intégrité des échanges électroniques, au-travers l'identification du certificat électronique et la signature en ligne à valeur légale. Et permet même de dater un fichier grâce à l'horodatage.

De son côté, « *GenMsecure* » a conçu des solutions bâties autour de son moteur d'authentification forte utilisant le smartphone comme terminal d'authentification et de validation afin de garantir la sécurité des transactions financières ou commerciales, ainsi que la protection des accès (Web, réseaux et physiques) des entreprises.

Aussi, « *Wallix* » propose des solutions logicielles de gestion des accès à privilèges pour les grandes et moyennes entreprises, organisations publiques et opérateurs de services *cloud.* Ces solutions aident leurs utilisateurs à protéger les actifs informatiques critiques parmi lesquels leurs données, serveurs, terminaux et objets connectés.

« *Cryptobox* » apporte par contre aux entreprises et Institutions une solution de partage et de travail collaboratif sécurisant leurs échanges internes et externes au-travers d'un chiffrement de bout-en-bout. Les bénéficiaires peuvent donc accéder à leurs documents depuis n'importe quel terminal de manière totalement sécurisée.

En revanche, « *BlueFiles* » est une solution qui permet de sécuriser les fichiers confidentiels qui sont envoyés hors d'un réseau sécurisé. Avec une technologie inédite ''*end-to-end User*'', *BlueFiles* renforce la protection des données en neutralisant de nombreuses failles de sécurité non résolues par un système de chiffrement standard.

Et en véritable backup automatique, la très spécifique plateforme « *YooBackup de Wooxo* » sauvegarde automatiquement 100% du patrimoine numérique professionnel : toutes les données et applications des serveurs physiques, virtuels, stations de travail et équipements nomades ainsi que leurs systèmes d'exploitation pour une restauration rapide en cas de survenance d'un sinistre informatique.

Cela exige ainsi la sécurisation et l'optimisation des réseaux, des systèmes, des postes de travail que des serveurs, au-travers notamment les solutions proposées de la firme « *Alter Sir GSS* » pour une bonne sécurité de l'environnement virtuel, du patrimoine informationnel, des réseaux sans-fil et des communications (fixes et mobiles), ainsi que la gestion des identités et des accès, etc.[10]

[10] Ce, avec pour dénominateurs supplémentaires, la solution « *Idecsi Access Analyzer* » qui permet de protéger totalement les boîtes mails des dirigeants et du management - transparence pour les utilisateurs et le système d'information, couvrant de ce fait tous les

En outre, force est de constater que l'Etat n'est pas l'unique acteur engagé dans ce combat contre la cybercriminalité, les multinationales ne ménagent aucun effort dans cette lutte, au nombre desquelles[11] l'on peut singulièrement épingler « *Bitdefender* »,[12] un spécialiste des solutions antimalwares et expert en cybersécurité. Ses technologies proactives classées n° 1 en détection et en performance par les organismes de tests indépendants protègent plus de 500 millions d'utilisateurs.

Depuis 2001, « *Bitdefender* » introduit et développe des technologies de protection pour les principaux environnements : les postes physiques et virtualisés et les appareils mobiles. Sa capacité à s'adapter aux menaces en constante évolution, à innover et à concevoir des solutions antimalwares proactives performantes en a fait un leader technologique de la sécurité numérique.

Il en est de même de « *BlackBerry, Cisco, Continental,*[13] *Deloitte,*[14] *Digital Security,*[15] *F-Secure, Fireeye, GFI Informatique,*[16] *Huawei, IBM Sécurité, Kaspersky Lab France, Orange Cyberdéfense, Secure IC », etc.*

---

risques en temps réel (internes, externes…, accès, droits…). Ainsi que celle proposée par le leader mondial de la sécurité e-mail « *Vade Secure Gateway* » contre les malware, phishing, spear phishing, spam, etc. Sa technologie unique basée sur des méthodes d'analyse heuristiques et comportementales protège aujourd'hui près de 300 millions d'utilisateurs dans le monde avec une efficacité reconnue sur toutes les attaques ciblées.

[11] FIC 2017, 9e Forum International de la Cybersécurité, *Smarter security for future technologies,* Manuel de formation, Lille, 24 et 25 janvier 2017, pp. 31, 36, 38, 42, 43, 50, 51, 53, 56, 61, 66 et 73.

[12] FIC 2017, *Smarter security for future technologies,* Manuel de formation, *Idem,* p. 31.

[13] « CONTINENTAL » développe des technologies intelligentes dédiées au transport des biens et des personnes. Véritable partenaire, l'équipementier automobile, fabricant de pneus et fournisseur industriel d'envergure internationale, propose des solutions durables, sûres, confortables, individuelles et abordables. C'est à juste titre qu'il avait réalisé en 2015 un chiffre d'affaires de 39,2 milliards d'euros et emploie actuellement plus de 218.000 personnes dans 55 pays du monde. (FIC 2017, Manuel de formation, *Ibidem,* p. 38).

[14] « DELOITTE », leader mondial du conseil en sécurité (Etude Gartner, Forester, … juillet 2015). Depuis trois années consécutives, il mobilise un ensemble de compétences diversifiées pour répondre aux enjeux de ses clients, de toutes tailles et de tous secteurs. Intégré à un réseau mondial, il compte plus de 8.000 spécialistes des systèmes d'information et de 3.000 experts de la sécurité.

[15] Fondée en 2015 par un groupe d'experts en sécurité des systèmes d'information avec le soutien du Groupe ECONOCOM, « DIGITAL SECURITY » a pour vocation d'offrir aux entreprises et aux administrations des prestations d'audit et de conseil avancées en matière de sécurité des SI.

[16] GFI INFORMATIQUE, (éditeur de logiciels français), propose ses 3 solutions de cybersécurité : *Keenaï*, est la solution SIEM qui permet d'analyser en temps réel l'activité du système d'information, de détecter des scénarios d'attaques et de réagir aux cyber attaques. Elle a reçu le label France Cybersecurity en 2016. *Keenaï Report* s'adresse aux RSSI et la DSI qui souhaitent bénéficier rapidement d'une vision synthétique de la sécurité de leur système d'information, en affichant très facilement des tableaux de bord paramétrables. *Keenaï Scada*

Pour commentaire, il est de réputation connue que « *BlackBerry* » garantit un monde connecté sécurisé, fournissant par ailleurs des solutions innovantes à travers l'ensemble de l'écosystème mobile et au-delà. Il sécurise les données les plus sensibles à travers l'ensemble des points connectés – des voitures aux smartphones – faisant de la vision de l'entreprise mobile une réalité.

« *Cisco* » propose à son tour une offre de sécurité et de services efficaces à la fois intégrée, automatisée, ouverte et facile d'utilisation. En s'appuyant sur une présence inégalée sur le réseau ainsi que sur les meilleures technologies et talents du marché, il délivre une visibilité et une réactivité remarquable pour détecter davantage de menaces et les arrêter plus rapidement.

« *F-Secure* », (expert européen en sécurité informatique), défend, depuis plusieurs décennies, entreprises et particuliers contre toutes les attaques du Web, qu'il s'agisse de *ransomware* ou de cyber attaques évoluées. Ses services et solutions utilisent les innovations brevetées F-Secure et un système sophistiqué des renseignements sur les menaces. Ce qui a amené ses experts à participer à plusieurs enquêtes européennes liées à la cybercriminalité, et ce, plus qu'aucune autre entreprise présente sur le marché.

Par ailleurs, « *FireEye* » a inventé une plate-forme de sécurité dédiée, basée sur une machine virtuelle, qui fournit aux entreprises et aux Gouvernements une protection efficace contre les cyberattaques de nouvelle génération. Ces attaques hautement sophistiquées passent facilement au travers des défenses traditionnelles basées sur des signatures, dont les *firewalls* de nouvelle génération, les systèmes IPS, les antivirus et autres passerelles.

Le chinois « *Huawei* » par contre, solidement implanté en RDC, est un fournisseur global des solutions dans le domaine des technologies de l'information et de la communication, travaillant avec 45 des 50 plus importants opérateurs sur le marché mondial. Grâce à son investissement auprès de ses clients en matière d'innovation et à des partenariats forts, Huawei propose des solutions efficaces de bout en bout dans les réseaux Télécoms, les terminaux et le *Cloud Computing*. En fournissant des solutions et des services compétitifs, Huawei affirme son engagement dans la création maximale de valeur pour les opérateurs Télécoms, les entreprises et les consommateurs. Ses produits et solutions sont déployés dans plus de 170 pays au monde, au service de plus d'un tiers de la population mondiale.[17]

En revanche, « *Kaspersky Lab* » est une société de cybersécurité mondiale fondée en 1997. Son expertise en matière de « *Threat Intelligence* » et sécurité informatique vient perpétuellement enrichir la création des solutions et des

est la solution innovante de SIEM pour superviser les installations industrielles à l'aide de sonde métier 3D.

[17] FIC 2017, Manuel de formation, *Op. Cit.,* p. 56.

services de sécurité pour protéger les entreprises, les infrastructures critiques, les Gouvernements et les consommateurs. Son large portefeuille de solutions de sécurité comprend la protection avancée et complète des terminaux et un certain nombre de solutions et de services de sécurité dédiés afin de lutter contre les menaces digitales sophistiquées et en constante évolution. Ses technologies aident plus de 400 millions d'utilisateurs et 270.000 clients à protéger ce qui compte le plus pour eux.[18]

La firme « *Orange Cyberdefense* » protège les essentiels : Elle conçoit, opère et surveille les systèmes de défense qui protègent les actifs critiques. Elle imprime une posture de sécurité, mieux un alliage subtil de technologies, de services, et de renseignements sur la menace, permettant ainsi de construire des offres cohérentes et globales. Ses technologies permettent d'aider les clients à pouvoir évaluer leur exposition au risque et à concevoir puis construire, les défenses les plus pertinentes dans leur contexte.[19]

Enfin, ces quinze dernières années, « *IBM* »[20] a orienté ses activités vers le Business Intelligence, l'analyse et le traitement des données, la sécurité et le Cloud. IBM s'est engagé à contribuer à une planète plus sûre en fournissant aux organisations du secteur gouvernemental, du maintien de l'ordre, de la défense, de la sécurité nationale et aux entreprises commerciales, les solutions ''*IBM i2*'' qui aident à mettre en évidence des informations afin de détecter, interrompre ou prévenir des menaces physiques ou cybermenaces dans les domaines de sécurité publique, des renseignements, de la lutte anti-fraude et de la cybercriminalité.

Les cybercriminels devenant plus agiles et menaçants, les organisations doivent renforcer leurs stratégies traditionnelles de cybersécurité en ajustant et en augmentant leurs mesures de sécurité. Les solutions ''*IBM i2*'' aident à découvrir rapidement des informations sur les cybercriminels, leurs motivations, ainsi que leurs méthodes.

Il incombe donc à l'Etat de faire un choix judicieux entre les diverses offres de technologie afin de retenir celles qui s'adaptent les mieux au défit sécuritaire des infrastructures numériques en son sein.

Toutefois, ainsi qu'il vient d'être démontré, la responsabilité reste partagée au niveau national, en matière de gestion et d'opérations.

---

[18] FIC 2017, *Smarter security for future technologies,* Manuel de formation, *op. cit.,* p. 61.
[19] Internet : in www.orange-business.com/fr/securite
[20] FIC 2017, *Ibidem,* p. 56.

La résilience et les infrastructures critiques sont plus une question de gouvernance qu'une question de technologie. La question essentielle ici est celle du rôle du Gouvernement. Pour certains, le Gouvernement apparaît en mesure de tout gérer. Sa position aux rênes du pays et son rôle de coordonnateur favorisent une coopération efficace entre secteurs privé et public. Il veille en définitive au partage des responsabilités entre chaque secteur qui se trouve responsable de sa propre résilience.

CONCLUSION

La République démocratique du Congo doit continuer de s'efforcer pour ne pas rester en marge de cette révolution du millénaire, en prenant notamment un engagement résolu du développement de l'Internet haut débit ; le tout en se basant par exemple, sur des objectifs chiffrés, le seuil de couverture le plus large, au taux le plus bas possible, dans quel délai et pour quel pourcentage de la population.

Au demeurant, nous recommandons au régulateur congolais de ne ménager aucun effort dans la surveillance des règles et exigences d'utilisation saine et recommandée de l'Internet dans notre espace cybernétique, à l'espoir d'une utilisation efficiente et sécurisée de l'Internet de confiance. Cet Internet, respectueux de l'ordre public et des règles de bonne conduite répondant aux valeurs socio-culturelles et éthiques congolaises.

Bien plus, il lui incombe la lourde charge de protéger et de sécuriser au mieux les infrastructures essentielles de notre communauté nationale, de sorte que l'Internet ne puisse pas devenir la cause de notre disparition collective. Aux pouvoirs publics de prendre toutes les dispositions qui s'imposent afin de lutter efficacement contre le sabotage informatique.

BIBLIOGRAPHIE

1. BAUTZMANN A., *Le droit du cyberespace face aux nouvelles réalités géostratégiques, Lecture critique, Revue internationale et stratégique,* février 2001, n° 42, in http://www.cairn.info/revue-internationale-et-strategique-2001-2-page-171.htm.
2. BOUNOUNG ESSONO Sosthène, *Le partage d'infrastructures et la coordination des politiques publiques,* Table ronde sur : « *Quelle régulation du partage d'infrastructures ?* », 7ème Réunion annuelle du Fratel, ART Cameroun, Bruxelles, 2009.
3. CAPELLARI Eric (Responsable cellule e-fraude, Société générale), *Cybermenaces : des modes opératoires de plus en plus sophistiqués,* FIC 2014
4. CLUSIF (Club de la Sécurité de l'Information Français), in http://www.clusif.fr/
5. DAHAN Léonard, (Country Manager France & Benelux, Stonesoft), *Cybermenaces : des modes opératoires de plus en plus sophistiqués,* FIC 2014
6. DELILLE Gil, (RSSI Crédit agricole), *Cybermenaces : des modes opératoires de plus en plus sophistiqués*, FIC 2014.
7. FIC 2017, 9e Forum International de la Cybersécurité, *Smarter security for future technologies,* Manuel de formation, Lille, 24 et 25 janvier 2017.
8. France Cybersecurity, Label France Cybersecurity, Catalogue 2017 des offres labellisées, les offres labellisées / Segmentation, Paris, 2017.
9. HARDY Daniel, MALLEUS Guy et MEREUR Jean-Noël (Eds), *Réseaux, Internet, téléphonie, multimédia, convergences et complémentarités,* Lavoisier, 2002.
10. IBM, *Optimisation des infrastructures informatiques : une source pour un avantage concurrentiel durable,* 2008.
11. MISOID MAHJOUBA et ELBAHLOULI LAMIAA *(Doctorantes en sciences de gestion - FSJES de Casablanca, Université Hassan II), La contribution de la télédéclaration dans l'amélioration de la performance de la Direction Générale des Impôts au Maroc,* in Revue du contrôle, de la comptabilité et de l'audit, n° 8, vol. 3 : n° 4, mars 2019.
12. NZE BOLEILANGA Guylain, *Les Technologies de l'Information et de la Communication, Adaptation du cadre juridique congolais face aux enjeux et à l'évolution des Télécoms,* Livret publié aux éditions du Centre de recherche interdisciplinaire de l'Université Pédagogique Nationale, Collection : Etudes et recherches, n° 40/2016, CRIDUPN, Kinshasa, février 2016
13. POGGIOLI Jean-Paul (Directeur de projet et consultant Médiaterra consultants), *La cybersécurité efficace, une affaire de culture*, FIC 2017, 9e Forum international de la cybersécurité, in « *Une sécurité intelligente pour les technologies du futur* », Revue trimestrielle, janvier 2017.

14. SAIZ Jérôme et al., *Résilience des infrastructures critiques,* FIC 2014, 6e Forum international de la cybersécurité, in « *Identité numérique et confiance* », les Actes du Forum, janvier 2014.
15. Stratégie nationale pour la sécurité du numérique, in htpp://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_fr.pdf (page consultée le 17/07/2022).