FORTERESSE DIGITALE DE DAN BROWN : UNE RÉPONSE LITTÉRAIRE AUX ENJEUX CYBERSÉCURITAIRES AFRICAINS ET GLOBAUX

Selay Marius KOUASSI
Université Peleforo Gon Coulibaly
lebonselay@yahoo.fr

Résumé

À partir de la théorie de la science-fiction, telle que formulée par Friedrich Richter, et de la théorie de la réception, cet article s'inscrit dans une approche solutionniste de la cybercriminalité qui sape les fondements de la paix sociale et du développement durable en Afrique. Il est incontestable que la numérisation des services apporte de nombreux avantages aux populations, en Afrique notamment, où internet connait une progression fulgurante. Cependant, les services numériques n'offrent pas que des avantages ; ils étendent l'éventail des risques et des défis sécuritaires qui menacent gravement la stabilité des États africains, et contre lesquels les gouvernants cherchent inlassablement des solutions durables. Les solutions présentées ici pour résoudre durablement les problèmes de cybersécurité en Afrique se nourrissent de l'intrigue du roman de science-fiction Forteresse digitale (2007), de l'auteur américain Dan Brown.
***Mots clés** : Afrique, Cyber, Numérique, Sécurité, Solutions*

Abstract

From a 'reader-response theory' perspective, and based on Friedrich Richter's science-fiction theory, this paper advocates a problem-solving approach to cybercrime that addresses the challenges undermining the foundations of social peace and sustainable development in Africa. It is undeniable that the digitalization of services offers many opportunities to populations worldwide, particularly in Africa, where internet usage is growing rapidly. However, this digitalization brings not only benefits but also expands the range of risks and security challenges that seriously threaten individuals and the stability of African states. The solutions presented here for sustainably addressing cybersecurity issues, especially in Africa, draw on insights from American author Dan Brown's science-fiction novel Digital Fortress (2007).
***Key words**: Africa, Digital, Cyber, Security, Solutions*

ISBN : 978-2-493659-12-5 COLLECTION RECHERCHES & REGARDS D'AFRIQUE VOL 4 N ° 15 Novembre 2025

Introduction

La révolution numérique a eu et continue d'avoir un impact significatif sur la dynamique des rapports sociaux en Afrique. Elle continue de changer la manière dont les individus interagissent et participent à la vie sociale (N. Friederici et al., 2020). L'essor d'internet en Afrique a également entraîné une reconfiguration des pratiques professionnelles dans de nombreux secteurs comme l'éducation, la santé et le milieu entrepreneurial (J-M. Huet, 2021). En facilitant, par exemple, l'accès à l'éducation, à la santé et à de nouvelles opportunités économiques aux Africains, internet leur ouvre la voie à une croissance économique améliorée et au développement durable. Toutefois, R. Diarra (2021, p.4) fait remarquer que l'accès à internet expose les Africains à de réelles menaces et attaques cybercriminelles qui constituent un défi majeur aussi bien pour les individus que pour les entreprises et les gouvernements. Ainsi, les enjeux liés à la sécurité numérique et à la cybercriminalité, sur le continent africain, sont au cœur des préoccupations sociales, économiques, politiques et géopolitiques actuelles et nourrissent de nombreuses réflexions et écrits produits aussi bien par les Africains eux-mêmes que par des non-Africains (T. Holt et A. Bossler, 2017, p.38). Si ces écrits offrent une perspective variée sur la cybercriminalité en Afrique et servent à la fois de point d'ancrage et de rampe de lancement pour explorer la littérature sur la cybercriminalité sur le continent africain, ils font, la plupart du temps, abstraction des pistes de solutions pour prévenir, limiter ou mettre un terme aux défis cybersécuritaires.

À propos, il est important de faire constater que ce n'est pas assez souvent que les hommes se tournent vers les œuvres de science-fiction pour rechercher des solutions aux problèmes qu'ils rencontrent dans leur rapport avec la techno-science en

ISBN : 978-2-493659-12- 5 COLLECTION RECHERCHES & REGARDS D'AFRIQUE VOL 4 N ° 15 Novembre 2025

général, et de façon spécifique dans le cyber espace. Pourtant, plusieurs œuvres de science-fiction, représentent, comme le démontrent J. Clute et P. Nicholls (1993, p.189), un réservoir inépuisable de solutions exploitables en vue d'annihiler de nombreux défis contemporains auxquels l'humanité est confrontée. *Forteresse digitale* (2007) de l'auteur américain Dan Brown, se classe dans la catégorie des œuvres de science-fiction qui présentent des solutions réalistes aux problèmes de cybercriminalité auxquels sont confrontés les individus, les organisations et les gouvernements.

La numérisation rapide en Afrique ouvre de nouvelles opportunités, mais expose également le continent à de sérieuses menaces cybercriminelles, ce qui nécessite des solutions durables et adaptées ; le présent article s'appuie sur le roman *Forteresse digitale* (2007) comme source d'inspiration pour explorer ces réponses. En effet, avec l'essor rapide de la numérisation des services et l'expansion fulgurante d'internet en Afrique, le continent bénéficie de nouvelles opportunités économiques, éducatives et sociales ouvrant la voie au développement durable. Cependant, cette transformation digitale expose également les individus, les organisations et les États africains à une multiplication des risques et des menaces cybercriminelles, qui sapent la stabilité sociale, économique et politique. Face à ces défis sécuritaires complexes, souvent exacerbés par des attaques provenant tant de l'extérieur que de l'intérieur des systèmes, il est crucial d'identifier des solutions durables et efficaces adaptées au contexte africain. C'est dans ce cadre que cette recherche s'appuie sur le roman de science-fiction de Dan Brown, considéré comme une source d'inspiration pour proposer des stratégies innovantes de lutte contre la cybercriminalité, interrogeant ainsi le rôle des imaginaires littéraires pour répondre à des enjeux technologiques réels.

ISBN : 978-2-493659-12-5 COLLECTION RECHERCHES & REGARDS D'AFRIQUE VOL 4 N ° 15 Novembre 2025

Les arguments développés dans cet article sont construits autour de la principale question de recherche suivante : comment les solutions proposées dans *Forteresse digitale* (2007) peuvent-elles éclairer et inspirer la lutte contre les défis de cybersécurité en Afrique ? Par ailleurs, ces arguments reposent sur une hypothèse centrale : les stratégies de cybersécurité présentées dans Forteresse Digitale offrent un cadre conceptuel adaptable et pertinent pour développer des réponses efficaces aux cybermenaces spécifiques au contexte africain.

Cet article est structuré autour de trois parties majeures. La première partie explore comment *Forteresse digitale* (2007) questionne les enjeux éthiques du rapport de l'humain à la technoscience d'une manière générale et au cyberespace en particulier. Ensuite, la seconde, lève le voile sur les menaces cybercriminelles induites par l'usage d'internet en Afrique. Quant à la troisième et dernière partie, elle présente les solutions proposées par ce roman de science-fiction de Dan Brown en vue de résoudre les problèmes de cyber sécurité et freiner la cybercriminalité.

1. *Forteresse digitale* : questionnement des enjeux éthiques du rapport de l'humain au cyberespace

L'intrigue du roman de science-fiction *Forteresse digitale* (2007) de Dan Brown a pour cadre l'agence nationale de sécurité étasunienne NSA (National Security Agency). L'héroïne, Susan Fletcher, y est confrontée à une crise majeure inédite, lorsque 'Digital Fortress', le code de cryptage de l'agence, supposé infaillible, est compromis par un mystérieux cybercriminel. Ce code censé protéger les informations les plus sensibles du gouvernement américain, a été dérobé par un cybercriminel qui l'utilise comme un moyen de chantage et une menace contre la sécurité nationale. Susan et son équipe travaillent sans relâche

ISBN : 978-2-493659-12- 5 COLLECTION RECHERCHES & REGARDS D'AFRIQUE VOL 4 N ° 15 Novembre 2025

pour neutraliser la menace cybercriminelle et protéger le code 'Digital Fortress'.

Paru pour la première fois, en anglais (sous le titre *Digital Fortress)*, soit plusieurs années avant l'essor véritable d'internet et des menaces sécuritaires qui s'y rattachent aujourd'hui, le roman *Forteresse digitale* (2007) aborde de manière lucide la question des attaques cybercriminelles. Aussi met-elle en lumière l'importance de la sécurité informatique et de la collaboration des individus et des organisations pour annihiler ces attaques. Déjà en 1998, cette œuvre avait le mérite, d'enjamber le réel, pour projeter ses lecteurs dans un futur fictionnel ; d'imaginer des menaces et des attaques potentielles liées à internet et de proposer une batterie de mesures pour s'en prémunir. Ce futur fictionnel d'alors se trouve être l'instant présent que vivent les peuples du monde entier aujourd'hui. À l'époque de la parution initiale de cette œuvre, sa trame était considérée comme relevant du domaine de la science-fiction parce qu'elle abordait un sujet purement futuriste, quasi-utopique. Mais à présent, elle offre aux lecteurs une perspective précieuse sur un sujet crucial et d'actualité pour les nations du monde entier. Aussi, faut-il lui reconnaître le mérite de questionner le rapport de l'humain à la technoscience et plus singulièrement au cyberespace.

S. Lem (2012, p.53), théoricien de la science-fiction, démontre avec force que la science-fiction est un outil précieux pour anticiper les enjeux éthiques, moraux et sociaux liés à l'évolution technologique et pour promouvoir un dialogue critique et constructif sur ces questions cruciales pour l'avenir de l'humanité. *Forteresse digitale* (2007) en est une illustration parfaite. À travers ce roman de science-fiction, Dan Brown a abordé de manière visionnaire les enjeux éthiques, sociaux et

ISBN : 978-2-493659-12-5 COLLECTION RECHERCHES & REGARDS D'AFRIQUE VOL 4 N ° 15 Novembre 2025

existentiels posés par les avancées technologiques, notamment ceux observés dans le cyber espace aujourd'hui.

À propos, la question centrale autour de laquelle est construite l'intrigue de *Forteresse digitale* (2007) est bien celle que soulève le personnage Greg Hale, informaticien et expert en cryptologie, lorsque ce dernier, en s'adressant à Susan, sa collaboratrice de la NSA, déclare : « Nous qui sommes les gardiens de la société, qui nous surveillera et qui veillera à ce que nous ne devenions pas des citoyens dangereux ? » (2007, p.102) Cette question soulève un dilemme éthique sur la surveillance et le contrôle du cyber espace. Plus spécifiquement, elle remet en question la capacité, mais aussi la garantie de la responsabilité des informaticiens, des cryptographes et experts en sécurité informatique, à agir de manière juste et à ne pas abuser de leur autorité. Somme toute, la question de Greg Hale pointe du doigt le défi que représente la prévention des abus de pouvoir des informaticiens et de manière général le personnel en charge des questions de cybersécurité.

Il y a que, parfois, les attaques cybercriminelles sont souvent des attaques considérées comme endogènes, en ce sens qu'elles proviennent du personnel même qui est en charge de la sécurité des systèmes informatiques des organisations victimes desdites attaques. C'est d'ailleurs le cas dans *Forteresse digitale* (2007). La National Security Agency (NSA) dispose d'un nouvel ordinateur nommé TRANSLTR, capable de déchiffrer n'importe quel code et de déverrouiller son message secret, et plus important encore, de prévenir les attaques terroristes. Mais personne en dehors du personnel de la NSA n'a connaissance de l'existence de cet ordinateur. C'est Ensei Tankado, un employé frustré de la NSA, qui, grâce à ces codes d'accès personnels en prend le contrôle. Il crée ensuite, un virus indétectable par TRANSLTR et menace désormais de divulguer au public des

ISBN : 978-2-493659-12- 5 COLLECTION RECHERCHES & REGARDS D'AFRIQUE VOL 4 N ° 15 Novembre 2025

informations sensibles et des données personnelles à caractère privée ; toute chose qui mettrait à mal la sécurité des États-Unis et des citoyens américains. Les personnages Trevor Strathmore, David Becker et Susan Fletcher, tous des collègues de Tankado, essaient d'empêcher ce dernier de ruiner l'avenir de la NSA et de mettre en péril la vie de millions de leurs concitoyens et la stabilité de leur pays.

L'une des leçons à retenir ici c'est que, bien souvent, les mesures de sécurité informatiques ont tendance à se concentrer sur la prévention et la neutralisation des menaces externes, négligeant ainsi les menaces émanant de l'intérieur ; des menaces qui ne sont pas pour autant moins dommageables. Loin des scénarii fictionnels, et dans la vie réelle, le cas d'Edward Snowden, un ancien employé de la NSA, qui a eu accès, par des voies détournées, à des informations de la NSA classées top secret, et qui a organisé la fuite de ces informations, et les a fait publier par la presse en juin 2013, est une preuve irréfutable que la menace cybercriminelle peut être endogène (provenir de l'intérieur du système). Dan Brown y avait songé plus tôt, avant tout le monde. C'est certainement à titre prémonitoire et préventif qu'il a écrit dans son roman de science-fiction, qui a également pour cadre la NSA *:* « […] dans le monde de la sécurité numérique, la frontière entre l'ami et l'ennemi peut être poreuse. » (2007, p. 287) En effet, des agents chargés de la sécurité informatique des entreprises et ou des organisations peuvent soudainement retourner leur veste et devenir des ennemis ou des menaces létales pour les mêmes entreprises qu'ils sont censés protéger contre les cyberattaques.

L'une des contributions majeures de la science-fiction réside dans sa capacité à anticiper les évolutions de la technologie et à en envisager ses implications sur la société, mais aussi et surtout à questionner les enjeux éthiques du rapport de

ISBN : 978-2-493659-12-5 COLLECTION RECHERCHES & REGARDS D'AFRIQUE VOL 4 N ° 15 Novembre 2025

l'humain à la technoscience et au cyberespace (M. Tymn, 1985, p.32). *Forteresse digitale* (2007) n'y déroge pas. En effet, ce roman joue un rôle essentiel dans le questionnement des enjeux éthiques du rapport de l'humain au cyber espace. Aussi offre-t-il des perspectives sur les risques inhérents à l'utilisation du numérique et sur les moyens de les prévenir, tout en interrogeant les responsabilités individuelles et collectives dans la préservation de la sécurité numérique.

Les œuvres de science-fiction, qu'il s'agisse de romans, de films, ou de séries télévisées, mettent souvent en lumière les risques et les menaces liés à l'usage de la technologie, tout en proposant des pistes de réflexion et des solutions (M. Tymn, 1985, p.72). Ces propositions sont souvent faites pour prévenir de l'imminence d'un danger et surtout éviter qu'il ne se produise vraiment. Cela, l'auteur d'oeuvres de science-fiction R. Bradbury (2001, p.108) le traduit si bien lorsqu'il écrit: « *the function of science fiction is not always to predict the future but sometimes to prevent it.* » [Notre traduction : La science-fiction n'a pas pour seul but de prédire un avenir apocalyptique, mais elle vise également à l'éviter.] En effet, en explorant des scénarii utopiques, la science-fiction offre un espace de réflexion critique sur les conséquences de nos choix technologiques, tout en stimulant l'imagination et la créativité dans la recherche de solutions aux problèmes (J-P. Richter, 2004) ou de prévention des problèmes de technoscience et plus particulièrement de cybersécurité. Quoique *Forteresse digitale* (2007) soit une œuvre de fiction, les solutions qu'elle propose pour contenir les menaces cybercriminelles peuvent être exploitées en vue de résoudre les défis cyber sécuritaires auxquels sont confrontés les citoyens africains, mais aussi et surtout les institutions et gouvernements africains pour qui endiguer la cybercriminalité demeure une véritable gageure.

ISBN : 978-2-493659-12-5 COLLECTION RECHERCHES & REGARDS D'AFRIQUE VOL 4 N ° 15 Novembre 2025

2. Menaces cybercriminelles en Afrique : nature des menaces et profil des auteurs

D'une manière générale et dans le contexte africain, les menaces et attaques cybercriminelles sont de nature hybride : elles ciblent aussi bien les personnes physiques que les personnes morales (A. Enzo, 2020). Par ailleurs, les auteurs de ces menaces et attaques ne sont pas toujours des bandes de cybercriminels organisés et extérieures aux structures ou organisations victimes desdites attaques. Il y a que, bien souvent, les auteurs des attaques cybercriminelles font partie du personnel même des structures visées par les attaques et opèrent depuis l'intérieur de ces structures (F. Djimgou, 2019).

Selon qu'ils ciblent des personnes physiques ou morales, les cybercriminels utilisent une variété de méthodes pour commettre leurs crimes. Ces méthodes, explique H. Lilen (2011), incluent le cyber harcèlement, l'usurpation d'identité numérique et le vol de données personnelles, en vue de commettre des actes frauduleux, comme l'ouverture de comptes bancaires ou encore la demande et l'obtention des crédits en ligne, au nom des victimes. Il arrive parfois que les cybercriminels, comme le démontrent G. Azema et M. Lenzen (2014), aient recours à des logiciels malveillants pour bloquer l'accès aux systèmes informatiques, ou encore pour s'y introduire et voler des données pour ensuite demander aux utilisateurs ou aux propriétaires de ces données de payer une rançon pour en retrouver l'accès.

La cybercriminalité en Afrique est un problème qui n'affecte pas que les seuls citoyens, elle impacte également la performance des entreprises privées et publiques, mais aussi et surtout des institutions qu'elle cible (T. Holt et A. Bossler, 2017, p.19). Les cybercriminels s'attaquent souvent à des institutions

ISBN : 978-2-493659-12-5 COLLECTION RECHERCHES & REGARDS D'AFRIQUE VOL 4 N ° 15 Novembre 2025

financières ou des organisations privées ou étatiques importantes, en exploitant les vulnérabilités des systèmes informatiques et en utilisant des techniques sophistiquées pour mener à bien leurs attaques. À l'échelle du continent africain, il n'y a pas un seul pays qui ne soit pas confronté à des défis spécifiques liés à la protection des données personnelles, à la sécurité des transactions en ligne et à la prévention de la cybercriminalité liée aux réseaux sociaux et à la communication mobile (P. Bellanger, 2014, p.208). Le renforcement des systèmes de sécurité informatique, pour empêcher les cybercriminels d'accéder à des informations sensibles et de les altérer est devenu une priorité pour les gouvernements africains (N. Kshetri, 2013, p.187).

S. Brenner (2012, p. 67) explique que dans les imaginaires collectifs africains, l'évocation des menaces et des attaques cybercriminelles renvoie le plus souvent à une intrusion d'acteurs extérieurs au système informatique cible des menaces ou attaques. Toutefois, il est bien établi que les auteurs des menaces et des attaques cybercriminelles en Afrique se présentent sous divers profils et qu'un grand nombre de menaces et d'attaques cybercriminelles sont de nature endogène (G. Blokdyk, 2019, p.27), en ce sens qu'elles proviennent de membres du personnel des entreprises ou organisations qui sont victimes de ces attaques. Par ailleurs, M. Maras (2014, p.21) démontre que les auteurs d'attaques cybercriminelles qui proviennent de l'extérieur des structures ciblées par ces attaques sont soit des individus opérant seuls, soit des cybercriminels organisés en bande et motivés, entre autres, par des gains financiers, des idéologies politiques ou sociales, ou simplement par le désir de défier les systèmes de sécurité existants. La prise de conscience de la diversité de ces profils est essentielle pour développer des stratégies de cybersécurité efficaces.

ISBN : 978-2-493659-12-5 COLLECTION RECHERCHES & REGARDS D'AFRIQUE VOL 4 N ° 15 Novembre 2025

3. Solutions concrètes aux menaces cybercriminelles

Pour lutter efficacement contre les menaces et les attaques cybercriminelles, *Forteresse digitale* (2007) propose une approche systémique et holistique qui repose sur au moins trois points. Il y a d'abord l'éducation et la sensibilisation des utilisateurs d'internet aux meilleures pratiques en matière de cyber sécurité et un cryptage robuste et sécurisé des réseaux informatisée. Il y a ensuite l'établissement d'un plan de réponse et de confinement des cyber incidents, encadré par la conduite de tests de piratage éthique et d'évaluation continue des potentielles cyber menaces, et enfin, la collaboration et le partage d'informations entre les agences gouvernementales, les organisations du secteur privé et les partenaires internationaux.

Dan Brown suggère que les États renforcent l'éducation des utilisateurs d'internet aux meilleures pratiques, en matière de cyber sécurité, afin qu'ils puissent reconnaître des sites internet malveillants, qu'ils apprennent comment encoder un mot de passe de sorte à le rendre plus résistant, et surtout que les États, au-delà des simples déclarations d'intention et des effets d'annonce sans lendemain, promeuvent de véritables curricula de formation sur la cybersécurité à dispenser dans les écoles et universités. Pour Dan Brown, la mise en œuvre de protocoles de cryptage solides peut aider à protéger les données sensibles contre tout accès non autorisé, contre tout piratage ou corruption de données. Mais ces cryptages pour être solides devront être implémentés avec beaucoup de précision et de justesse. Comme le recommande l'auteur de *Forteresse digitale* (2007), il faudra toujours garder à l'esprit que « dans le domaine du cryptage des données numériques, une seule erreur peut entraîner des conséquences catastrophiques.» (2007, p.79) Ainsi, la robustesse du cryptage des données, comme mesure de prévention des attaques cybercriminelles, devra tenir compte de l'exactitude des algorithmes de cryptage avancés, mais elle

ISBN : 978-2-493659-12-5 COLLECTION RECHERCHES & REGARDS D'AFRIQUE VOL 4 N ° 15 Novembre 2025

devra également observer la mise à jour régulière des clés de cryptage (D. Ziani & M. Ruba 2017). Car, comme le souligne le personnage Ensei Tankado, dans *Forteresse digitale* : « Le cryptage relève certes du langage du secret, mais il peut aussi devenir la porte du salut.» (2007, p.37) En effet, la mise à jour des algorithmes de cryptage des données est aussi bien nécessaire pour anticiper les cyberattaques potentielles que pour maintenir l'intégrité, l'authenticité et la confidentialité des informations.

La trame de *Forteresse digitale* (2007) laisse entrevoir en filigrane que l'établissement d'un plan clair de réponse aux cyber incidents peut également permettre une détection et un confinement rapides des attaques, et surtout une récupération rapide après lesdites attaques. Mais, cela implique, comme Dan Brown le fait savoir à travers le personnage de Susan, de disposer d'une équipe motivée capable d'effectuer régulièrement des tests de simulation et de mettre en œuvre des mécanismes de sauvegarde et de récupération de données. À propos, Susan déclare que « […] dans le domaine du déchiffrement des données numériques, chaque énigme peut être résolue, si l'on est prêt à creuser suffisamment et profondément.» (*2007*, p.189) En clair, toute équipe disposant de la bonne formation et des bons outils peut accomplir à peu près tout, si elle dispose d'un plan de réponse aux incidents cybersécuritaires assez clair, amélioré par des tests réguliers. Le plan de réponse aux incidents doit demeurer un élément essentiel de tout programme de cybersécurité, fournissant un cadre structuré pour détecter, répondre et se remettre des cyberattaques.

Dans *Forteresse digitale* (2007), c'est la conduite régulière d'exercices de piratage éthique et de tests préventifs d'intrusion dans le système informatique de la NSA qui a permis, aux informaticiens de la NSA et, plus particulièrement, à Jabba, d'identifier les vulnérabilités du système avant qu'elles ne puissent être exploitées par des acteurs malveillants. Jabba avait

ISBN : 978-2-493659-12- 5 COLLECTION RECHERCHES & REGARDS D'AFRIQUE VOL 4 N ° 15 Novembre 2025

fait de la conduite des tests de piratage éthique un credo. Il était assuré que « […] La prévention était le meilleur remède.» (*2007,* p.199). Ainsi avait-il privilégié une approche préventive et proactive. Sous sa direction aucun cyber délinquant n'avait pu réussir à infiltrer le système de l'agence nationale de sécurité étasunienne, et il tenant à garder cette réputation intacte, comme le souligne Susan : « Aucun ordinateur de la NSA n'avait jamais fait l'objet de piratage sous le règne de Jabba; il avait l'intention que les choses demeurent ainsi.» (2007, p.200). À travers la conduite et la supervision de tests de piratage éthique et d'évaluation continue des potentielles cyber menaces, Jabba joue la carte de la proactivité pour se préserver d'attaques malveillantes et de situation désastreuse, en gardant bien à l'esprit qu'aucun système informatique aussi robuste soit-il n'est éternellement inébranlable s'il n'est révisé et actualisé constamment, au moyen des tests de piratage éthique. Ainsi que le fait remarquer Commandant Trevor, « [Jamais rien] n'est vraiment et totalement en sécurité. La forteresse numérique pouvait être détruite, et les conséquences pourraient être dévastatrices.» (*2007,* p.109) À propos, B. Gordijn et K. Weber (2017, p.71) insistent pour dire qu'il n'y a que les tests de piratage éthique qui puissent permettent aux organisations de remédier de manière proactive aux faiblesses des systèmes informatiques et numériques et d'en renforcer les défenses. Par ailleurs, la mise en œuvre de systèmes d'évaluation de cybermenaces potentielles permet la détection, en temps réel, desdites menaces. À propos, il ne s'agit pas seulement pour les experts en charge de la sécurité informatique et numérique de savoir, mais d'être proactifs, de planifier et de se préparer à des attaques éventuelles, mais aussi et surtout d'apprendre à réfléchir comme les cyber délinquants, ainsi que le recommande le personnage Jabba : « La véritable force d'un agent chargé de décoder les données cryptées réside non seulement dans ses connaissances, mais dans sa capacité à penser comme son

ISBN : 978-2-493659-12- 5 COLLECTION RECHERCHES & REGARDS D'AFRIQUE VOL 4 N ° 15 Novembre 2025

adversaire et surtout sa capacité à anticiper les actions de ce dernier. » (2007, p.87)

Encourager la collaboration et le partage d'informations entre les agences gouvernementales, les organisations du secteur privé et les partenaires internationaux peut améliorer la capacité collective à détecter les cybermenaces et à y répondre de manière coordonnée et efficace, à travers un plan commun de réponse aux incidents cybersécuritaires. En effet, le pouvoir de la collaboration et du partage rapide d'informations est essentiel pour élaborer des stratégies contre les cyberattaques qui ciblent les États, comme le recommande le personnage Commandant Trevor Strathmore : « […] Le pouvoir que confère l'information peut être aussi bien bénéfique que maléfique ; il peut autant aider à sauver des vies qu'à en détruire.» (*2007*, p.89) En travaillant ensemble, les États peuvent développer des solutions de cyber sécurité efficaces qui les protègent contre les cybermenaces et garantissent la sécurité et la stabilité de leurs gouvernements. C'est bien cette idée que Susan traduit à travers cette allégorie : « […] Lorsque de nombreuses mains se mettent à la tâche, l'ouvrage avance plus rapidement.» (2007, p.178) Autrement dit, l'engagement constant de tous les États dans la lutte contre les menaces cybercriminelles, dans un élan collégial, allégerait assurément la charge individuelle de chaque État.

Conclusion

Les œuvres de science-fiction, qu'elles soient littéraires ou cinématographiques, ont toujours permis d'explorer les implications de la technologie sur la société et sur l'humain. En s'inscrivant dans ces sillons, Dan Brown a abordé, dans *Forteresse digitale* (2007), de manière visionnaire, les enjeux éthiques, sociaux et existentiels liés à la cyber-sécurité que le monde entier connaît aujourd'hui. Ce roman de science-fiction

ISBN : 978-2-493659-12-5 COLLECTION RECHERCHES & REGARDS D'AFRIQUE VOL 4 N ° 15 Novembre 2025

interroge les responsabilités individuelles et collectives dans la préservation de la sécurité numérique globale. Aussi propose-t-il des pistes de solutions aux problèmes cybersécuritaires que rencontrent les individus, les organisations et les États. Le récit stimulant sur la résilience et la capacité d'innovation face aux menaces et aux attaques cybercriminelles narré dans *Forteresse digitale*, (2007) se déroule loin du contexte africain, dans un cadre américain notamment. Toutefois, les solutions aux problèmes de sécurité numérique qui y sont décrites peuvent être adaptées au contexte africain, et inspirer la formulation de solutions aux nombreux défis que pose la cybercriminalité en Afrique.

La première partie de cet article, consacrée aux questions éthiques fondamentales sur la relation entre l'humain et la technoscience, particulièrement dans le cyberespace, telle qu'exposée dans le roman de Dan Brown, a mis en exergue le défi qu'il y a à prévenir les abus de pouvoir internes aux organismes chargés de la cybersécurité. Elle a également insisté sur la nécessité d'une vigilance permanente contre les menaces internes. Cette réflexion éthique soulève la question de la responsabilité des professionnels de la sécurité numérique dans un monde de plus en plus numérisé.

La deuxième partie a révélé que les menaces cybercriminelles sont hybrides, visent les personnes et les institutions et proviennent de l'intérieur des organisations. Les cybercriminels, individuels ou organisés, utilisent des méthodes variées, du vol de données à la propagation de logiciels malveillants. Alors, connaître cette variété de profils d'attaquants est crucial pour élaborer des stratégies de cybersécurité adaptées au contexte africain, où la protection des données et la lutte contre la cybercriminalité demeurent des défis majeurs.

ISBN : 978-2-493659-12-5 COLLECTION RECHERCHES & REGARDS D'AFRIQUE VOL 4 N ° 15 Novembre 2025

Enfin, la troisième partie a montré que pour relever ces défis, Forteresse Digitale recommande une approche systémique qui intègre l'éducation des utilisateurs, un cryptage fort et adaptable, et des plans de réponse aux incidents avec des tests de piratage éthique réguliers. La coopération accrue entre les gouvernements, le secteur privé et les partenaires internationaux est également soulignée comme un moyen de détecter, prévenir et répondre aux cyberattaques. Ces solutions, bien que fictives, sont des pistes inspirantes pour améliorer la cybersécurité en Afrique.

Si *Forteresse digitale* (2007) permet d'entrevoir plusieurs solutions aux défis cybersécuritaires auxquels les Africains sont confrontés en ce moment, cette œuvre passe toutefois sous silence la législation robuste sur la cybercriminalité qui demeure l'une des mesures par lesquelles les États peuvent lutter efficacement contre les menaces et attaques cybercriminelles. Il y a que, dans la société africaine actuelle de plus en plus numérisée, où internet joue un rôle central dans la vie quotidienne des populations, la nécessité d'une législation efficace en matière de cybercriminalité ne peut être négligée. En effet, en criminalisant les cyberattaques ; en les punissant de peines relativement lourdes et en fournissant à la force publique les outils juridiques nécessaires pour enquêter et poursuivre les cybercriminels, les gouvernements africains pourraient aider à dissuader plusieurs cybercriminels et freiner ainsi la cybercriminalité qui constitue une menace sérieuse pour les individus, les entreprises et les États africains.

ISBN : 978-2-493659-12-5 COLLECTION RECHERCHES & REGARDS D'AFRIQUE VOL 4 N ° 15 Novembre 2025

Références bibliographiques et webliographiques

AZEMA Guillaume et LENZEN Martial, « *Le dico du numérique : lexique des termes numériques* », https://blogpeda.ac-poitiers.fr/ent-lyc/files/2020/02/Lexique_numerique.pdf (Page consultée le 12 Juin 2025).

BELLANGER Pierre, 2014. *La souveraineté numérique*, Bruxelles, Socle Éditions.

BLOKDYK Gerardus, 2019. *Endpoint cybercriminals forensics: a complete guide*, Brendale, 5starCooks.

BRENNER Susan, 2012. *Cybercrime and the law: challenges, issues, and outcomes*, Boston, Northeastern University Press.

BRADBURY Ray, 2001. *The Halloween Tree Paperback*, New York, Yearling.

BROWN Dan, 2007. *Forteresse Digitale*, Trad. D. Defert, Paris, J-C. Lattès.

CLUTE John et NICHOLLS Peter, 1995. *The Encyclopedia of Science Fiction*, New York, St Martins Printing.

DIARRA Rosalie, 2021. *La répression de la cybercriminalité en Afrique de l'Ouest*, Paris, L'Harmattan.

DJIMGOU François-Xavier, 2019. *Souveraineté numérique et cyberdéfense : un enjeu de taille pour l'Afrique*, Paris, Edilivre.

ENZO Alain, 2020. *La cybersécurité en Afrique de l'Ouest : entre cyberinfluences étrangères et cybercriminalités endogènes*, Paris, Éditions du Cygne.

FRIEDERICI Nicolas et GRAHAM Mark, 2020. *Digital Entrepreneurship in Africa: how a Continent is Escaping Silicon Valley's Long Shadow*, Massachusets, The MIT press.

GORDIJN Bert et WEBER Karsten, 2017. *A Review of Value-Conflicts in Cybersecurity*,

ISBN : 978-2-493659-12-5 COLLECTION RECHERCHES & REGARDS D'AFRIQUE VOL 4 N ° 15 Novembre 2025

https://scite.ai/reports/10.29297/orbit.v1i1.28. (Page consultée le 27 Janvier 2025).

HOLT Thomas et BOSSLER Adam, 2017. *Cybercrime in Progress: Theory and Prevention of Technology-enabled Offenses*, Londres, Routledge.

HUET Jean-Michel, 2021. *Afrique et numérique : comprendre les catalyseurs du digital en Afrique*, Londres, Pearson.

KSHETRI Nir, 2013. *Cybercrime and Cybersecurity in the Global South*, Londres, Palgrave Macmillan.

LEM Stanisław, 2012. *Microworlds: Writings on Science Fiction and Fantasy*, Boston, Mariner Books.

LILEN Henri, 2011. *Dictionnaire Informatique et Numérique*, Paris, First Interactive.

MARAS Marie-Helen, 2014. *Computer Forensics: Cybercriminals, Laws, and Evidence*, Massachusets, Jones & Bartlett Learning.

NTE Nbgoawaji et TERU Vigo, « A comparative Analysis of Cyber Security Laws and Policies in Nigeria and South Africa », Law Research Review Quarterly, 2/2022, pp. 233-258.

NYABOLA Nanjala, 2018. *Digital Democracy, Analogue Politics: How the Internet Era is Transforming Politics in Kenya*, Londres, Zed Books.

RICHTER Friedrich Jean-Paul, 2004. *L'Éclipse de Lune,* Paris, Phébus.

TYMN Marshall, « Science Fiction: a Brief History and Review of Criticism », Mid-America American Studies Association, 1/1985, pp. 41-66.

ZIANI Djamal et RUBA Al-Muwayshir, « *Improving Privacy and Security in Multi-Tenant Cloud ERP Systems* », https://scite.ai/reports/10.5121/acij.2017.8501, (Page consultée le 11 Mai 2025).

ISBN : 978-2-493659-12-5 COLLECTION RECHERCHES & REGARDS D'AFRIQUE VOL 4 N ° 15 Novembre 2025