Brainae Journal of Business, Sciences and Technology
ISSN "2789-374X (Print)" "2789-3758 (Online)"
Volume 9 Issue 05, May 2025
www.brainajournal.com; info@brainae.org

ANALYSE DES VULNERABILITES SPECIFIQUES AUXQUELLES LES CHAINES D'APPROVISIONNEMENT DES ONG SONT CONFRONTEES EN MATIERE DE CYBERSECURITE DANS LES ÉTATS DE L'ALLIANCE DU SAHEL (AES)

BONKOUNGOU ILIASSE
Université de Lisala, 5G56+2RW, Lisala, Congo-Kinshasa
Reçu: 08 Avril 2025 ; **Accepté:** 10 Mai 2025 ; **Publié:** 13 Mai 2025

Citez cet article : Bonkoungou Iliasse (2025). Analyse des vulnérabilités spécifiques auxquelles les chaînes d'approvisionnement des ONG sont confrontées en matière de cybersécurité dans les États de l'Alliance du Sahel (AES). Dans Brainae Journal of Business, Sciences and Technology (Vol. 9, Numéro 05, pp. 648-659).

DOI : https://doi.org/10.5281/zenodo.15399069

Résume

Le domaine humanitaire est de plus en plus confronté à des défis en matière de cybersécurité, notamment dans les régions instables comme les États de l'Alliance du Sahel (MALI, BURKINA FASO et le NIGER). Les ONG présentes dans ces pays sont vulnérables à diverses menaces cybernétiques en raison de leur engagement dans des opérations humanitaires sensibles et de leurs interactions avec des acteurs locaux souvent hostiles. Les chaînes d'approvisionnement des ONG sont particulièrement exposées aux attaques cybernétiques en raison de la complexité de leurs opérations et de la diversité des acteurs impliqués. Les cybercriminels ciblent souvent ces chaînes pour accéder à des informations sensibles ou perturber les activités humanitaires. De plus, les ONG actives dans les États de l'Alliance du Sahel sont confrontées à des défis spécifiques tels que l'instabilité politique, la corruption et les conflits armés, qui aggravent encore leur vulnérabilité en matière de cybersécurité. Les acteurs hostiles peuvent exploiter ces contextes fragiles pour mener des attaques ciblées et compromettre la sécurité des données et des opérations humanitaires.

Notre étude portant sur l'analyse des vulnérabilités spécifiques auxquelles les chaînes d'approvisionnement des ONG sont confrontées en matière de cybersécurité dans les États de l'Alliance du Sahel (AES) vise à identifier les vulnérabilités spécifiques aux chaînes d'approvisionnement des ONG dans les États de l'AES en matière de cybersécurité, évaluer les impacts potentiels de ces vulnérabilités sur les opérations des ONG et sur les bénéficiaires de l'aide et de formuler des recommandations pour renforcer la cybersécurité de ces organisations.

La méthodologie utilisée pour cette étude comprend une approche mixte, combinant des analyses qualitatives et quantitatives. Des entretiens semi-structurés ont été menés avec des responsables d'ONG, des experts en cybersécurité et des acteurs locaux, afin d'obtenir des perspectives variées sur les défis rencontrés. Parallèlement, une analyse documentaire a été réalisée pour examiner les incidents de cybersécurité passés et les meilleures pratiques en matière de sécurité dans le secteur humanitaire.

Cette approche nous a permis de révéler plusieurs vulnérabilités majeures à savoir la fragilité des infrastructures technologique, le manque de sensibilisation et de formation, la complexité de chaînes d'approvisionnement qui dépendent souvent de partenaires et de fournisseurs variés, ce qui complique la gestion des risques de cybersécurité le long de la chaîne d'approvisionnement et le risques liés aux données sensibles liées à la manipulation de données sensibles, notamment les informations personnelles des bénéficiaires, pose des risques en cas de violation de données.

Les résultats de cette étude ont des implications significatives tant sur le plan pratique que théorique. Sur le plan pratique, les recommandations fournies peuvent aider les ONG à élaborer des stratégies de cybersécurité adaptées à leur contexte opérationnel. Sur le plan académique, cette recherche contribue à la littérature sur la cybersécurité dans le secteur humanitaire, en fournissant un cadre d'analyse pour évaluer les risques spécifiques aux chaînes d'approvisionnement des ONG dans des environnements fragiles.

L'étude des vulnérabilités cybersécuritaires des chaînes d'approvisionnement des ONG dans les États de l'Alliance du Sahel est essentielle pour garantir la continuité et l'efficacité des interventions humanitaires. En identifiant ces vulnérabilités et en proposant des solutions pratiques, cette recherche vise à renforcer la résilience des ONG face aux menaces cybernétiques, assurant ainsi la protection des données sensibles et la sécurité des bénéficiaires dans une région où l'aide humanitaire est vitale.

Mot clé : Vulnérabilité - chaine d'approvisionnement – Cybersécurité – protection des données – risques

Abstract

The humanitarian sector is increasingly facing cybersecurity challenges, particularly in unstable regions such as the Sahel Alliance states (MALI, BURKINA FASO and NIGER). NGOs operating in these countries are vulnerable to various cyber threats due to their involvement in sensitive humanitarian operations and their interactions with often hostile local actors.

NGO supply chains are particularly vulnerable to cyber attacks because of the complexity of their operations and the diversity of the actors involved. Cyber criminals often target these chains to gain access to sensitive information or disrupt humanitarian activities.

In addition, NGOs operating in the Sahel Alliance countries face specific challenges such as political instability, corruption and armed conflict, which further increase their vulnerability in terms of cybersecurity. Hostile actors can exploit these fragile contexts to carry out targeted attacks and compromise the security of data and humanitarian operations.

Our study on Analysis of specific cybersecurity vulnerabilities faced by NGO supply chains in Sahel Alliance States (SAS) aims to Identify specific cybersecurity vulnerabilities faced by NGO supply chains in SAS states, assess the potential impacts of these vulnerabilities on NGO operations and aid beneficiaries, and make recommendations for strengthening the cybersecurity of these organisations.

The methodology used for this study includes a mixed approach, combining qualitative and quantitative analyses. Semi-structured interviews were conducted with NGO leaders, cybersecurity experts and local stakeholders to obtain a range of perspectives on the challenges faced. In parallel, a documentary review was carried out to examine past cybersecurity incidents and security best practice in the humanitarian sector.

This approach has enabled us to reveal several major vulnerabilities : the fragility of technology infrastructures, the lack of awareness and training, the complexity of supply chains that often depend on a variety of partners and suppliers, which complicates the management of cybersecurity risks along the supply chain, and the risks associated with the handling of sensitive data, particularly the personal information of beneficiaries, which poses risks in the event of a data breach.

The results of this study have significant practical and theoretical implications. On a practical level, the recommendations provided can help NGOs to develop cybersecurity strategies adapted to their operational context. Academically, this research contributes to the literature on cybersecurity in the humanitarian sector, providing an analytical framework for assessing the risks specific to NGO supply chains in fragile environments.

Studying the cyber security vulnerabilities of NGO supply chains in the Sahel Alliance states is essential to ensure the continuity and effectiveness of humanitarian interventions. By identifying these vulnerabilities and proposing practical solutions, this research aims to strengthen the resilience of NGOs to cyber threats, thereby ensuring the protection of sensitive data and the security of beneficiaries in a region where humanitarian aid is vital.

Key words : *Vulnerability - Supply Chain - Cybersecurity - Data Protection - Risks*

1. Introduction

Les chaînes d'approvisionnement des ONG dans les États de l'Alliance du Sahel (AES) sont confrontées à des vulnérabilités cybernétiques croissantes, notamment des attaques par ransomware, l'ingénierie sociale et la fragilité des infrastructures numériques. La pertinence globale de cette étude réside dans la protection des données sensibles des missions humanitaires. À l'échelle régionale, elle contribue à renforcer la résilience face aux menaces cybernétiques dans un contexte instable. Localement, elle favorise la mise en place de pratiques sécuritaires adaptées, essentielles pour garantir la continuité des opérations et protéger les communautés vulnérables soutenues par ces ONG. Cette analyse se penchera sur les vulnérabilités particulières auxquelles ces ONG sont exposées en matière de cybersécurité dans le contexte régional du Sahel.

Face à cette menace croissante, Abda H., Tairi A., Nouali O. (2020). A secure data protection approach for supply chain management in the context of the cyber security of NGOs in the Sahel Alliance States. International Journal of Information Security, 19(3), 421-435 soulignent la nécessité d'adopter des mesures de cybersécurité efficaces pour protéger les informations confidentielles tout au long de la chaîne d'approvisionnement. Plutard, Diawara K., Sow A., Ndiaye D. (2019). Strategies for enhancing data protection in the supply chain of NGOs operating in Sahel countries in the face of cybersecurity threats. Journal of Information Security and Privacy, 15(2), 201-216 identifient des mesures clés pour répondre aux défis de sécurité des informations dans cet environnement particulièrement vulnérable.

Dans ce contexte, la question de recherche qui guide cette étude est de déterminer quelles sont les failles spécifiques dans les chaînes d'approvisionnement des ONG du Sahel qui les rendent vulnérables aux cyberattaques. La problématique centrale réside dans la nécessité de renforcer la sécurité des chaînes d'approvisionnement des ONG pour garantir la sûreté des données et des opérations dans un contexte où les attaques cybernétiques sont de plus en plus fréquentes.

Ces dernières années environ 20 % des ONG ont connu des violations de données (Interpol, 2022). Une ONG burkinabè a perdu 150 000 USD à cause d'une attaque de phishing ciblé (rapport interne, 2023). De plus, 68 % des ONG ne fournissent pas de formation en cybersécurité à leur personnel (CyberPeace Institute, 2022), ce qui amplifie les risques lors de crises humanitaires, comme observé durant le COVID-19 où 30 % des projets ont été retardés (ONU, 2021).

Ces différentes attaques entrainent la perte de données sensibles, des interruptions de services, et une diminution de la confiance des donateurs et des bénéficiaires. Cela peut également entraîner des pertes financières significatives, compromettant l'efficacité des interventions humanitaires. Ce problème est alarmant, car les ONG dans la région sont souvent déjà sous-financées et manquent de ressources pour investir dans des solutions de cybersécurité. La vulnérabilité des chaînes d'approvisionnement peut avoir des répercussions profondes sur la capacité des ONG à répondre aux crises humanitaires croissantes dans un contexte de conflit et d'instabilité. Face à cette situation préoccupante des initiatives de formation en cybersécurité pour le personnel des ONG et le développement de partenariats avec des entreprises technologiques pour améliorer la sécurité des systèmes. Cependant, ces efforts sont souvent limités par un manque de financement, le manque d'engagement à long terme, et des infrastructures technologiques obsolètes. De plus, la sensibilisation et la formation ne sont pas toujours systématiques, laissant des lacunes dans la préparation aux cybermenaces.

C'est dans cette perspective que cette étude portant sur les vulnérabilités spécifiques auxquelles les chaînes d'approvisionnement des ONG sont confrontées en matière de cybersécurité dans les États de l'Alliance du Sahel (AES) vise à identifier les principaux points faibles des chaînes d'approvisionnement des ONG dans le Sahel, d'évaluer les risques associés et de formuler des recommandations pour renforcer la cybersécurité de ces organisations. Les hypothèses sous-jacentes à cette analyse sont que les chaînes d'approvisionnement des ONG sont exposées à des risques importants en raison de leur complexité et de leur interdépendance, et que des mesures spécifiques sont nécessaires pour atténuer ces risques et renforcer la résilience des organisations face aux cybermenaces.

2. Choix et Intérêt

2.1 Choix

Le choix d'analyser les vulnérabilités spécifiques aux chaînes d'approvisionnement des ONG en matière de cybersécurité dans les États de l'Alliance du Sahel (AES) est particulièrement pertinent pour plusieurs raisons.

Tout d'abord, la région du Sahel est confrontée à des défis humanitaires et sécuritaires majeurs, tels que les conflits armés, l'instabilité politique et les crises alimentaires. Les ONG y jouent un rôle vital dans l'assistance humanitaire et le développement, rendant leurs opérations sensibles et critiques pour les populations vulnérables.

Ensuite, la dépendance croissante à la technologie et aux systèmes d'information pour la gestion des données et des opérations expose ces organisations à des cybermenaces. Les infrastructures numériques dans cette région sont souvent inadaptées, ce qui augmente les risques de cyberattaques, de violations de données et de perturbations dans les chaînes d'approvisionnement.

De plus, la méfiance envers les technologies numériques et le manque de formation en cybersécurité parmi le personnel des ONG exacerbent ces vulnérabilités. En analysant ces enjeux, il est possible d'identifier des mesures proactives pour renforcer la cybersécurité, protégeant ainsi non seulement les données des ONG, mais aussi celles des communautés qu'elles servent. Ce thème est donc essentiel pour garantir la continuité des opérations humanitaires et la protection des bénéficiaires dans un contexte complexe et fragile.

2.2 Intérêt

2.2.1 Intérêts Scientifiques

L'intérêt scientifique de la protection des données dans la chaîne d'approvisionnement des ONG opérant dans les États de l'Alliance du Sahel (AES) repose sur plusieurs aspects fondamentaux :

- **Renforcement de la résilience des ONG** : Les ONG sont souvent des cibles de cyberattaques en raison de leur rôle crucial dans les interventions humanitaires. La sécurisation de leurs chaînes d'approvisionnement garantit la continuité de leurs opérations. Selon le Centre canadien pour la cybersécurité, chaque maillon de la chaîne mondiale d'approvisionnement peut représenter un risque contre la cybersécurité[1]
- **Prévention des cyberattaques** : Les chaînes d'approvisionnement modernes sont interconnectées, ce qui les rend vulnérables aux cyberattaques. Les experts en sécurité des systèmes d'information ont détecté une hausse de 15,1 % des cyberattaques en 2021, en partie due à la numérisation des processus[2]
- **Innovation technologique** : La recherche dans ce domaine favorise le développement de nouvelles technologies pour sécuriser les données. Par exemple, des politiques claires en matière de cybersécurité et des outils adaptés sont essentiels pour protéger les données sensibles[3]
- **Impact géopolitique et économique** : Dans les États de l'AES, où les infrastructures numériques sont parfois fragiles, la cybersécurité des chaînes d'approvisionnement peut jouer un rôle clé dans la stabilité économique et politique. Les tensions géopolitiques peuvent dégénérer en cyberguerre, perturbant les fonctions sociétales vitales[4]
- **Contribution à la science des données** : L'analyse des risques et la mise en œuvre de solutions de cybersécurité enrichissent les connaissances dans les domaines de la gestion des risques et de la sécurité des systèmes d'information[5]

2.2.2 Intérêts personnels

L'intérêt personnel d'aborder les vulnérabilités en cybersécurité des chaînes d'approvisionnement des ONG dans les États de l'Alliance du Sahel (AES) découle de plusieurs motivations. Tout d'abord, la passion des enjeux humanitaires et volonté de sensibiliser à l'importance de la cybersécurité dans des contextes où les ONG sont essentielles pour le bien-être des populations vulnérables.

De plus, ce sujet permet d'explorer les intersections entre la technologie et l'humanitaire, offrant une opportunité d'analyser comment l'innovation peut améliorer la résilience des ONG.

Enfin, traiter de ce thème met en lumière ces enjeux, cet article peut contribuer à la promotion de solutions pratiques pour améliorer la sécurité informatique dans des environnements fragiles.

2.2.3 Intérêts sociaux

Cet article met en évidence plusieurs intérêts sociaux liés aux vulnérabilités en cybersécurité des chaînes d'approvisionnement des ONG dans les États de l'Alliance du Sahel (AES). Tout d'abord, la protection des données sensibles des bénéficiaires est cruciale, car une violation pourrait compromettre leur sécurité et leur dignité. Ensuite, en renforçant la cybersécurité, les ONG peuvent améliorer la confiance des communautés locales, essentielles pour leur engagement et leur coopération. Par ailleurs, ce sujet offre l'opportunité de sensibiliser et d'éduquer le personnel et les bénéficiaires sur les risques numériques, renforçant ainsi la résilience des populations face aux menaces. Enfin, une cybersécurité solide contribue à la continuité des services humanitaires, réduisant les interruptions qui pourraient aggraver les situations de crise. En somme, aborder ces vulnérabilités est fondamental pour assurer un impact social positif et durable dans cette région fragile.

2.2.4 Intérêts économiques

Premièrement, il met en lumière l'importance d'une cybersécurité robuste pour garantir l'efficacité opérationnelle des ONG. En prévenant les cyberattaques, ces organisations peuvent éviter des interruptions coûteuses, assurant ainsi une allocation optimale des ressources financières. Deuxièmement, une posture de cybersécurité solide peut attirer des financements supplémentaires de la part de bailleurs de fonds soucieux de soutenir des initiatives sécurisées et fiables. Troisièmement, l'article souligne la nécessité de former le personnel local sur les enjeux de cybersécurité, ce qui peut également stimuler l'économie locale en créant des emplois dans la formation et le soutien technique. Enfin, en favorisant des partenariats locaux, les ONG renforcent les économies régionales, contribuant ainsi au développement durable dans une région souvent affligée par l'instabilité.

3. Approche Méthodologique

La présente étude, est analytique combinant des approches qualitatives et quantitatives. Le but de cette étude est d'analyser les mesures de protection des données de la chaîne d'approvisionnement mises en place par les ONG opérant dans les États de l'Alliance du Sahel, et d'évaluer leur efficacité en matière de cybersécurité.

L'objectif de ces études qualitatives est d'explorer des situations, de Validéer des hypothèses afin de pouvoir orienter des décisions stratégiques. L'approche qualitative a connu des évolutions qui lui permettent aujourd'hui de se positionner plus

[1] https://www.cyber.gc.ca/fr/orientation/la-cybersecurite-et-la-chaine-dapprovisionnement-evaluation-des-risques-itsap10070
[2] https://www.mecalux.fr/articles-de-logistique/luca-urciuoli-cybersecurite-chaine-approvisionnement
[3] https://www.gpsi-intl.com/fr/blogue/la-cybersecurite-dans-la-gestion-de-la-chaine-dapprovisionnement/
[4] https://www.mecalux.fr/articles-de-logistique/luca-urciuoli-cybersecurite-chaine-approvisionnement
[5] https://www.gpsi-intl.com/fr/blogue/la-cybersecurite-dans-la-gestion-de-la-chaine-dapprovisionnement/

clairement et de démontrer sa valeur, sa conception et ses procédures[6]. Néanmoins, ces méthodes qualitatives sont encore relativement rares dans les papiers logistiques[7]. La recherche qualitative considère la réalité comme une construction humaine qui prend en compte de la subjectivité et la considère comme un élément clé de la structure des groupes sociaux. Elle vise à déterminer l'importance des actions et des événements[8]. Ainsi, l'analyse qualitative est utile pour comprendre et interpréter des phénomènes humains et sociaux complexes.

Une approche qualitative renforce donc la capacité des chercheurs à décrire un système social complexe[9]. L'utilisation de cette méthode permet également d'identifier les similitudes dans le discours des acteurs dans différents contextes. Elle donne du sens aux situations interpersonnelles rencontrées (Adler, 2003). Plus précisément, la recherche qualitative n'est pas seulement axée sur l'utilisation de méthodes qualitatives pour la collecte de données, mais comment ces données sont perçues. En outre, il s'agit de poser des questions sur l'exactitude de la valeur scientifique des résultats et la fourniture d'un aperçu basé sur l'interprétation dans un cadre ethnologique. Dans le cadre de la présente, il est question de démonter la vulnérabilité de la chaine d'approvisionnement des ONG face au menace accrues de la cyberattaque dans un environnement instable.

En recherche qualitative, nous pouvons faire la distinction entre plusieurs modes de recueil de données : l'entretien individuel, l'entretien de groupe, l'observation participante ou non participante et le recueil des documents.

L'entretien semi-directif a été utilisé comme principal outil d'enquête. Cet outil est bien adapté à un problème qui consiste à connaître le rôle et l'influence des attitudes fondamentales sur les perceptions et le comportement[10]. Cette technique est appropriée dans le contexte de la recherche sur le fonctionnement des mécanismes de réseau. Certaines précautions ont été nécessaires pour garantir la Validéité scientifique des données recueillies lors des entretiens. Un guide d'entretien a été utilisé pour orienter les personnes interrogées vers plusieurs grands thèmes et dimensions étudiés. Ainsi, à l'aide du logiciel Google Form, le guide d'entretien a été utilisé lors nos enquêtes.

Pour ce qui est du recueil des documents : cette technique, nous a permis de constituer une base de données secondaire auprès des administrations publiques et privées mais aussi, nous avons consulté les livres, rapports, publications et thèses ayant traits à la thématique principale.

Cette étude transversale à visée analytique permet d'observer et analyser les données de variables collectées à un moment donné.

Dans l'optique d'atteindre nos objectifs nous avons eu recours à :

- Revue de la littérature : Effectuer une revue approfondie de la littérature existante sur la protection des données de la chaîne d'approvisionnement et la cybersécurité des ONG, en se concentrant notamment sur les meilleures pratiques et les défis spécifiques rencontrés dans les États de l'Alliance du Sahel.
- Collecte de données : Réalisation des entretiens auprès des experts en sécurité des données et des représentants d'ONG opérant dans la région pour recueillir des informations sur les pratiques actuelles en matière de protection des données de la chaîne d'approvisionnement. Nous avons pu mener notre enquête auprès de Quarante-sept personnes réparties entre les pays de l'AES : 59,1% des enquêtés sont au Burkina Faso, 22,7% au Mali et 18,2% sont des travailleurs humanitaires intervenants au Niger.

Cette enquête qui réalisée par Google form s'est intéressée aux Responsables des approvisionnements, coordinateurs logistiques, informaticiens, chefs de mission etc...

Les données obtenues sont Analysées à l'aide du logiciel SPSS 26.0 pour identifier les lacunes potentielles dans les mesures de protection des données mises en place par les ONG et proposer des recommandations pour renforcer la cybersécurité dans la région.

Pour une meilleure évaluation nous avons fait :

- Évaluation quantitative : Utiliser des indicateurs de performance clés pour mesurer l'efficacité des mesures de protection des données de la chaîne d'approvisionnement des ONG dans les États de l'Alliance du Sahel.
- Évaluation qualitative : Réaliser des analyses qualitatives pour comprendre les défis spécifiques rencontrés par les ONG dans la région en matière de cybersécurité et identifier les meilleures pratiques à adopter.

Les évaluations nous permettrons de proposer des recommandations pratiques basées sur les conclusions de l'étude pour renforcer la protection des données de la chaîne d'approvisionnement et améliorer la cybersécurité des ONG opérant dans les États de l'Alliance du Sahel.

4. Revue de la littérature

4.1 Revue théorique

Les ONG opérant dans les États de l'Alliance du Sahel font face à des défis spécifiques en matière de cybersécurité liés à leurs chaînes d'approvisionnement. Plusieurs auteurs ont abordé ces vulnérabilités dans la littérature académique et les rapports de recherche.

4.1.1 Définitions

Vulnérabilité

Les vulnérabilités en cybersécurité sont des failles potentielles dans un système informatique, un logiciel, un réseau ou un appareil qui pourraient être exploitées par des attaquants pour compromettre la confidentialité, l'intégrité ou la disponibilité des données ou des systèmes. Ces vulnérabilités peuvent résulter de défauts de conception, de configuration incorrecte, de logiciels obsolètes, de manque de formation ou de sensibilisation à la sécurité, ou encore de mauvaises pratiques de gestion des mots de passe.

Selon le livre "Cybersecurity and Cyberwar: What Everybody Needs to Know" de Peter W. Singer et Allan Friedman, publié en 2014, les vulnérabilités peuvent être exploitées de différentes manières, telles que l'utilisation de logiciels malveillants,

---

[6] Marshall, C., & Rossman, G. B. (2011). Designing Qualitative Research (5th ed.). Thousand Oaks, CA: Sage Publications.

[7] Houé et Murphy, 2016 a study of logistics Networks : The value of a qualitative Approach

[8] *Kvale*, S., & *Brinkmann*, S. (*2009*). InterViews: Learning the craft of qualitative research interviewing. Los Angeles, CA: Sage Publications

[9] Idem

[10] *Wengraf*, T. (*2001*) Qualitative Research Interviewing: Biographic Narrative and Semi-Structured Methods. Sage Publications, London,

d'attaques par déni de service, d'ingénierie sociale ou de violation de données. Les auteurs soulignent également l'importance de comprendre les vulnérabilités pour mieux les anticiper et les corriger avant qu'elles ne soient exploitées par des attaquants.

Les auteurs s'appuient sur une combinaison d'analyses historiques, de théories de la sécurité nationale et d'évaluations des technologies de l'information pour explorer le paysage de la cybersécurité. Ils examinent comment la guerre cybernétique transforme les conflits, les politiques et les sociétés, tout en intégrant des principes de gestion des risques extrêmes et d'interconnexion technologique.

Le livre est écrit dans un langage accessible, rendant des concepts complexes compréhensibles pour un public non-spécialiste suivant une approche multidisciplinaire. Les auteurs provoquent une réflexion sur les conséquences de la cybersécurité sur la société moderne et l'économie mondiale. Bien que le livre soit accessible, certains experts pourraient le trouver trop simpliste dans son approche technique, ne fournissant pas suffisamment de détails sur les mécanismes spécifiques de cybersécurité.

Pour ceux qui recherchent plus de détails techniques, il est conseillé de lire d'autres ouvrages ou ressources spécialisées, tels que des rapports de sécurité ou des publications académiques. Compléter ce livre avec des études de cas actuelles sur les violations de données ou les cyberattaques peut offrir une perspective plus moderne.

Ainsi, les vulnérabilités en cybersécurité constituent un enjeu majeur pour la protection des systèmes d'information et nécessitent une approche proactive de gestion des risques et de renforcement de la sécurité.

Notion de Chaîne d'approvisionnement

Lambert et al., (1998) définissent le **Supply Chain** comme une suite d'association des entreprises qui fournissent des produits et des services sur le marché.[11] Selon Rota-Frantzet et al., (2001)[12], les entreprises appartenant à une même chaîne logistique sont reliées par des flux de produits et des flux d'informations :

Les flux de produits correspondent au flux de matières (produit final, matière première, des composants d'assemblage, etc.) qui circulent au niveau de la chaîne logistique de l'amont vers l'aval afin de fournir de la valeur ajoutée au client final.

Les flux d'information représentent l'ensemble des transferts ou échanges de données entre les différents acteurs de la chaîne logistique.

Depuis le début des années 80, l'évolution du marché a conduit à une remise en cause profonde des modèles organisationnels classiques et à l'émergence d'un nouveau paradigme post-bureaucratique (Desreumaux, 2015). Ainsi, dans un contexte de globalisation des marchés, l'objectif principal de la gestion de la chaîne logistique est la création de valeur, basée sur la prémisse qu'une chaîne logistique intégrée et efficiente contribue à la minimisation des risques financiers et à l'augmentation des profits (Fawcett, 2008). Pour cette raison, la performance des chaînes logistiques est une question cruciale. Une organisation cherche toujours à être fiable, efficiente, réactive, durable, etc. Ces critères ne peuvent être atteints sans une gestion convenable de ces organisations en tenant compte des spécificités de l'environnement. Ce niveau de gestion permet d'exceller, car celui qui gère bien ses connaissances et ses compétences, peut aussi gérer convenablement ses ressources.

Au vu de ces notions, il est important de parler de l'optimisation de la chaine d'approvisionnement.

Cybersécurité

La cybersécurité dans la chaîne d'approvisionnement peut être définie comme l'ensemble des pratiques, des technologies et des politiques visant à protéger les informations, les systèmes et les infrastructures critiques qui permettent le bon fonctionnement des flux de marchandises et de services tout au long de cette chaîne.

Selon l'ouvrage "Security Engineering: A Guide to Building Dependable Distributed Systems." publiée en 2020 par Ross Anderson, professeur en sécurité informatique à l'université de Cambridge, la cybersécurité dans la chaîne d'approvisionnement est un enjeu crucial car toute faille de sécurité peut avoir des conséquences désastreuses, non seulement pour l'entreprise concernée, mais aussi pour l'ensemble du réseau des fournisseurs et des partenaires.

La cybersécurité dans la chaîne d'approvisionnement est vitale, car une faille peut entraîner des dommages considérables. Les forces incluent la collaboration accrue entre partenaires et l'innovation dans la sécurité. Cependant, les faiblesses résident dans la dépendance excessive aux fournisseurs et l'absence de normes de sécurité uniformes. Pour contourner ces faiblesses, il est essentiel d'établir des partenariats transparents, de réaliser des audits réguliers de sécurité et de mettre en œuvre des protocoles de sécurité robustes et normalisés. En intégrant une culture de cybersécurité proactive, les entreprises peuvent renforcer leur résilience face aux menaces croissantes

Ainsi, pour Anderson, la cybersécurité dans la chaîne d'approvisionnement ne se limite pas à la protection des données et des systèmes informatiques, mais englobe également la gestion des risques liés aux fournisseurs, à la logistique, aux infrastructures et aux processus opérationnels. Il souligne l'importance d'adopter une approche holistique de la sécurité, en tenant compte de l'ensemble des maillons de la chaîne d'approvisionnement et en favorisant la collaboration et la transparence entre les différents acteurs.

4.1.2 Impacte de la cybersécurité sur la chaine d'approvisionnement

La cybersécurité a un impact crucial sur la chaîne d'approvisionnement des ONG, souligne l'auteur Joseph Nye, expert en relations internationales. En effet, dans son livre "The Future of Power", publié en 2011, Nye met en lumière la vulnérabilité croissante des organisations non gouvernementales aux cyberattaques, qui peuvent compromettre la confidentialité des données sensibles liées aux projets d'aide humanitaire.

Les ONG dépendent de systèmes informatiques pour coordonner leurs opérations, gérer les fonds et communiquer avec les partenaires locaux. Une cyberattaque réussie peut perturber ces processus vitaux, entraînant des retards et des dysfonctionnements dans la distribution de l'aide, mettant en péril la vie de nombreuses personnes vulnérables.

De plus, les données confidentielles des ONG, telles que les informations personnelles des bénéficiaires, les comptes bancaires et les communications internes, sont des cibles attrayantes pour les cybercriminels. La perte ou la divulgation de ces informations peut compromettre la crédibilité et la réputation des ONG, et compromettre la confiance des donateurs et des partenaires.

---

[11] Lambert, D. M., Cooper, M. C., Pagh, J. D. (1998). Supply chain management: implementation issues and research opportunities. The international journal of logistics Management, 9 (2), 1–20.

[12] Rota-Frantz K., Bel G. et Thierry C., (2001). Gestion des flux dans les chaînes logistiques. In Performance Industrielle et gestion des flux. Hermes Science. 153-187

Ainsi, il est impératif pour les ONG de renforcer leur cybersécurité en mettant en place des mesures de protection adéquates, telles que des pares-feux, des logiciels antivirus et des formations pour sensibiliser les employés aux risques cybernétiques. De plus, elles doivent collaborer avec d'autres acteurs de la chaîne d'approvisionnement, tels que les gouvernements et le secteur privé, pour renforcer la résilience de l'ensemble du système contre les cybermenaces.

La protection de la chaîne d'approvisionnement est essentielle pour garantir la continuité des opérations des ONG. Selon Christopher et Peck (2004), une approche intégrée de la gestion des risques dans la chaîne d'approvisionnement permet de minimiser les perturbations. De plus, la formation continue du personnel en cybersécurité est cruciale, comme le souligne le CyberPeace Institute (2022), qui affirme que 68 % des ONG ne fournissent pas de telles formations. En adoptant des technologies de sécurité avancées et en renforçant la sensibilisation, les ONG peuvent mieux protéger leurs opérations et données.

La collaboration avec les partenaires est essentielle pour garantir la protection des données dans la chaîne d'approvisionnement. Selon Dyer et Singh (1998), des relations de partenariat solides favorisent le partage de connaissances et de ressources, renforçant ainsi la résilience face aux menaces cybernétiques. En intégrant les meilleures pratiques en cybersécurité au sein des accords de partenariat, les ONG peuvent mieux protéger les données sensibles. De plus, comme le souligne Kumar et al. (2018), une approche collaborative permet d'harmoniser les protocoles de sécurité, minimisant ainsi les vulnérabilités. Cette synergie est cruciale pour assurer la sécurité et l'efficacité des opérations humanitaires.

4.2 Revue empirique

La cybersécurité des chaînes d'approvisionnement des ONG dans les États de l'Alliance du Sahel est une préoccupation croissante en raison des menaces croissantes de cyberattaques et de failles de sécurité.

Risques de phishing et d'hameçonnage : Le phishing et l'hameçonnage sont des techniques couramment utilisées par les attaquants pour obtenir des informations confidentielles ou causer des dommages aux organisations. Dans leur étude intitulée "Cybersecurity in Non-Governmental Organizations: A Study of Phishing Threats" (2018), Theofilatos et al. visent à évaluer la vulnérabilité des ONG face aux attaques de phishing. L'objectif est de comprendre comment la nature humanitaire de leur travail les rend particulièrement ciblées. La méthodologie inclut une analyse qualitative des incidents de phishing rapportés et des entretiens avec des responsables de la sécurité des ONG. Les résultats révèlent une exposition accrue aux phishings, souvent due à des ressources limitées en cybersécurité et à une sensibilisation insuffisante, soulignant la nécessité d'améliorer la sécurité des données et la formation du personnel. L'étude de Theofilatos et al. sur les attaques de phishing souligne la vulnérabilité des ONG, reflétant des défis similaires dans les chaînes d'approvisionnement des ONG dans les États de l'Alliance du Sahel (AES). Ces organisations doivent faire face à des menaces cybernétiques spécifiques, exacerbées par des ressources limitées et des environnements instables.

L'étude de Theofilatos et al. révèle des lacunes concernant le manque de sensibilisation et de ressources des ONG face aux attaques de phishing. L'analyse des vulnérabilités spécifiques des chaînes d'approvisionnement des ONG dans les États de l'Alliance du Sahel peut combler ces lacunes en identifiant les menaces particulières, en développant des stratégies adaptées et en renforçant la formation en cybersécurité, permettant ainsi une meilleure résilience face aux cyberattaques dans des contextes fragiles.

Vulnérabilités des systèmes de gestion de l'information : Les ONG opèrent souvent dans des environnements complexes avec des systèmes d'information fragmentés et hétérogènes. Selon une étude menée par Mphande et Hossain (2019), cela crée des vulnérabilités potentielles qui peuvent être exploitées par des acteurs malveillants pour accéder à des données sensibles.

L'étude vise à identifier les vulnérabilités des systèmes d'information des ONG, causées par leur fragmentation. La méthodologie inclut l'analyse de cas, des enquêtes auprès de professionnels du secteur, ainsi qu'une revue de littérature pour évaluer les risques et proposer des solutions de sécurité. Elle révèle que les systèmes d'information fragmentés des ONG exposent des vulnérabilités exploitables, particulièrement dans des contextes comme les États de l'Alliance du Sahel. Cela souligne la nécessité d'analyser les chaînes d'approvisionnement des ONG pour renforcer leur cybersécurité face aux menaces spécifiques de la région. Cette étude se concentre sur les vulnérabilités des ONG sans approfondir les spécificités contextuelles des États de l'Alliance du Sahel (AES), telles que les menaces régionales et les infrastructures. L'analyse des vulnérabilités dans ces pays comble cette lacune en tenant compte des défis uniques, notamment l'environnement politique instable, les infrastructures technologiques limitées et les pratiques de sécurité locales. Cette approche contextualisée permet une évaluation plus pertinente des risques et propose des solutions adaptées.

Faiblesse de la formation des employés en matière de cybersécurité : Les employés des ONG peuvent ne pas être pleinement conscients des pratiques de cybersécurité et des risques associés. Selon une recherche réalisée par Komanduri et ses collègues (2017), le manque de formation et de sensibilisation en matière de cybersécurité parmi le personnel des ONG peut augmenter les risques de violations de données et de compromission des systèmes. L'objectif de leur recherche est d'évaluer l'impact du manque de formation en cybersécurité sur les ONG. La méthodologie inclut des enquêtes auprès du personnel des ONG et des analyses de cas pour identifier les lacunes en matière de sensibilisation et les conséquences sur la sécurité des données.

Les résultats de la recherche de Komanduri et al. (2017) indiquent que le manque de formation en cybersécurité parmi le personnel des ONG entraîne une augmentation des risques de violations de données et de compromission des systèmes. Ce constat est particulièrement pertinent pour les chaînes d'approvisionnement des ONG dans les États de l'Alliance du Sahel (AES), où les infrastructures peuvent être fragiles et les menaces cybernétiques plus fréquentes.

L'absence de sensibilisation expose les ONG à des vulnérabilités spécifiques, comme le phishing ou les attaques ciblées, qui peuvent compromettre non seulement les données sensibles, mais aussi l'intégrité des opérations humanitaires. En intégrant des formations adaptées et en évaluant ces vulnérabilités, les ONG peuvent renforcer leur résilience et mieux sécuriser leurs chaînes d'approvisionnement face aux menaces du contexte régional. Cette étude présente des lacunes en ne tenant pas compte des contextes spécifiques des ONG opérant dans des environnements à haut risque, comme ceux des États de l'Alliance du Sahel (AES). Elle n'aborde pas les menaces géopolitiques et les infrastructures technologiques limitées. Une analyse des vulnérabilités des chaînes d'approvisionnement des ONG dans cette région peut combler ces lacunes en identifiant les défis particuliers liés à la cybersécurité, en tenant compte des conditions locales, et en proposant des solutions adaptées pour renforcer la résilience et la sécurité des données.

Dépendance accrue aux technologies de l'information : Les ONG dépendent de plus en plus des technologies de l'information pour mener leurs opérations et fournir des services. Cela les expose à divers risques de cybersécurité tels que les attaques par ransomware, comme le soulignent Cohen et ses collègues (2020) dans leur étude. L'objectif de l'étude est d'évaluer

l'impact des technologies de l'information sur la cybersécurité des ONG et d'identifier les vulnérabilités liées à des menaces telles que les attaques par ransomware. La méthodologie inclut une analyse qualitative basée sur des entretiens avec des responsables d'ONG, ainsi qu'un examen des incidents de cybersécurité rapportés dans le secteur. Elle révèle que les ONG sont particulièrement vulnérables aux attaques par ransomware en raison de leurs infrastructures technologiques souvent obsolètes et du manque de formation en cybersécurité. Ces résultats soulignent la nécessité d'une vigilance accrue et d'une amélioration des pratiques de sécurité. Cela fait écho à l'analyse des vulnérabilités dans les chaînes d'approvisionnement des ONG, qui nécessite une évaluation des risques spécifiques et des stratégies adaptées pour protéger les données sensibles et garantir la continuité des opérations.

Cette étude de Cohen et al. (2020) présente des lacunes en ne considérant pas les spécificités des chaînes d'approvisionnement des ONG et leur exposition unique aux cybermenaces. Elle ne traite pas non plus des implications des attaques sur les opérations humanitaires. L'analyse des vulnérabilités spécifiques dans ce contexte peut combler ces lacunes en identifiant les points faibles, en tenant compte des interactions au sein des chaînes d'approvisionnement, et en proposant des mesures de sécurité adaptées pour mieux protéger les ONG contre les incidents de cybersécurité.

5. ANALYSE DES RESULTATS

5.1 Caractéristiques sociodémographiques des participants

L'étude a consisté à recueillir des données socio-démographiques sur des participants en situation professionnelle et pays d'intervention parmi les trois pays des Etats de l'Alliance du Sahel (Mali, Burkina Faso et le Niger) afin de mieux comprendre leurs caractéristiques sociales.

Tableau 01 : Présentation de la répartition des participants

Position dans l'organisation					
		Fréquence	**Pourcentage**	**Pourcentage Validé**	**Pourcentage Cumulative**
Validé	Autres	21	44,6	44,6	44,6
	Coordinateur logistique	7	14,9	14,9	59,5
	Informaticien	4	8,5	8,5	68
	Responsable des approvisionnements	15	32	32	100
	Total	47	100	100	
Pays					
		Fréquence	**Pourcentage**	**Pourcentage Validé**	**Pourcentage Cumulative**
Validé	BURKINA FASO	25	53,2	53,2	53,2
	MALI	10	21,3	21,3	74,5
	NIGER	12	25,5	25,5	100
	Total	47	100	100	

Source : Nos analyses dans Google Form

L'étude a concerné 47 travailleurs humanitaires dans la zone de l'AES. Elle révèle que 55,4 % sont directement impliqués. Il s'agit des coordinateurs logistiques, informaticiens et responsables approvisionnements. 44,6% sont indirectement impliqués.

Le taux de participation à cette enquête est inégalement reparti pour des raisons diverses (Promotion de l'enquête, intérêt et motivation). Le taux de participation au Burkina Faso est 53,2%, le Mali est de 21,3% et 25,5% de taux de participation au Niger.

5.2 Vulnérabilité de chaine d'approvisionnement face aux menaces de la cybersécurité

Les analyses des données collectées ont permis de savoir si les ONG mettent en place des mesures de cybersécurité pour protéger ses données et informations sensibles comme le présente le tableau suivant.

Tableau 02 : Vulnérabilité de la chaine d'approvisionnement

Est-ce que votre organisation met en place des mesures de cybersécurité pour protéger ses données et informations sensibles ?					
		Fréquence	**Pourcentage**	**Pourcentage Validé**	**Pourcentage Cumulative**
Validé	NON	13	27,7	27,7	27,7
	OUI	34	72,3	72,3	100
	Total	**47**	**100**	**100**	

Pouvez-vous nous dire dans quelle mesure votre ONG accorde de l'importance à la cybersécurité de sa chaîne d'approvisionnement ?

		Fréquence	Pourcentage	Pourcentage Validé	Pourcentage Cumulative
Validé	1	19	40,4	40,4	40,4
	2	4	8,5	8,5	48,9
	3	10	21,3	21,3	70,2
	4	5	10,6	10,6	80,8
	5	9	19,2	19,2	100
Total		**47**	**100**	**100**	

Avez-vous déjà été victime d'une cyberattaque ciblant votre chaîne d'approvisionnement ?

		Fréquence	Pourcentage	Pourcentage Validé	Pourcentage Cumulative
Validé	NON	38	80,8	80,8	95,7
	OUI	9	19,2	19,2	100
	Total	**47**	**100**	**100**	

Comment évaluez-vous la sensibilisation à la cybersécurité au sein de votre ONG et de vos partenaires de la chaîne d'approvisionnement ?

		Fréquence	Pourcentage	Pourcentage Validé	Pourcentage Cumulative
Validé	1	14	29,9	29,9	29,9
	2	6	12,7	12,7	42,6
	3	12	25,5	25,5	68,1
	4	10	21,3	21,3	89,4
	5	5	10,6	10,6	100
Total		**47**	**100**		

Votre organisation dispose-t-elle d'un plan de gestion de crise en cas d'attaque informatique ou de violation des données au sein de sa chaîne d'approvisionnement ?

		Fréquence	Pourcentage	Pourcentage Validé	Pourcentage Cumulative
Validé	NON	16	34	34	34
	OUI	31	66	66	100
	Total	**47**	**100**	**100**	

Source : Nos analyses dans Google Form

L'analyse des données indique que 72,3% des ONG dispose des mesures de prévention pour la protection de leur chaine d'approvisionnement contre la cybersécurité.

Cela montre que la majorité les ONG enquêtées reconnaissent l'importance de la cyber sécurité et prennent des mesures pour protéger leurs données et informations sensibles. Cependant, il est préoccupant que près d'un tiers des ONG enquêtées ne mettent pas en place de telles mesures, ce qui pourrait les rendre vulnérables aux attaques cybernétiques et compromettre la confidentialité et l'intégrité de leurs données. Il est donc important que ces ONG prennent conscience de l'importance de la cyber sécurité et mettent en place des mesures appropriées pour se protéger. Ce résultat rejoint les conclusions de Mphande et Hossain (2019), qui relève les vulnérabilités des systèmes de gestion de l'information dans le sens que les ONG opèrent souvent dans des environnements complexes avec des systèmes d'information fragmentés et hétérogènes. Selon notre étude le manque des mesures de prévention pour la protection de leur chaine d'approvisionnement contre la cybersécurité peut être exploitées par des acteurs malveillants pour accéder à des données sensibles.

Sur une échelle de 1 à 5 correspondants de très prioritaire à pas du tout prioritaire, nous constatons que 40,4% des ONG font de la protection des données sensibles une très grande priorité alors que 19,2% ne font aucune priorité.

Il est encourageant de constater que près de 40% des ONG considèrent la protection des données sensibles comme une priorité absolue, témoignant de leur engagement envers la confidentialité et la sécurité des informations. Cependant, il est préoccupant que près de 20% des organisations ne donnent pas la priorité à cette question essentielle, ce qui pourrait mettre en danger la confidentialité des données.

Le chiffre de 19,2% (le taux des ONG qui ont été victimes de cyberattaque) est significatif et met en évidence un risque réel pour ces organisations Ce risque rejoint le constat de Ross Anderson selon le toute faille de sécurité peut avoir des conséquences désastreuses, non seulement pour l'entreprise concernée, mais aussi pour l'ensemble du réseau des fournisseurs et des partenaires. Il est essentiel que les ONG prennent des mesures pour renforcer leur sécurité informatique et protéger leur chaîne d'approvisionnement contre de telles menaces.

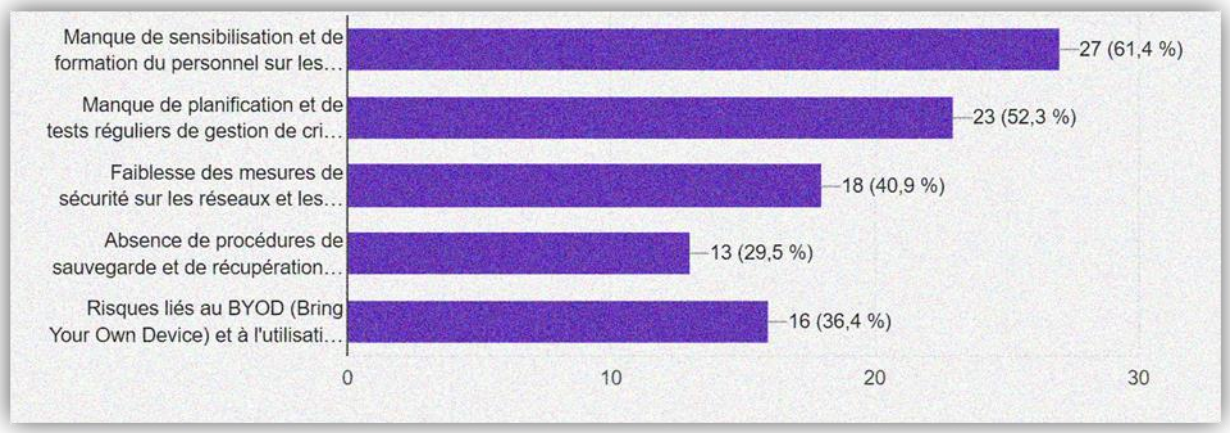
Selon ces données, il semble qu'une majorité de répondants (29,9%) considèrent que la sensibilisation à la cybersécurité au sein des ONG est très efficace, ce qui est positif. Ce résultat confirme l'analyse de Komanduri et ses collègues (2017), selon laquelle le manque de formation et de sensibilisation en matière de cybersécurité peut augmenter les risques de violations de données et de compromission des systèmes.

Cependant, il est également important de noter que 11,6% estiment que cette sensibilisation n'est pas du tout efficace, ce qui suggère qu'il y a encore des améliorations à apporter dans ce domaine. Une évaluation plus détaillée pourrait être nécessaire pour comprendre les raisons derrière ces perceptions divergentes et mettre en place des actions correctives si nécessaire.

Il semble que la majorité des ONG interrogées dispose d'un plan de gestion de crise d'attaque informatique de la chaîne d'approvisionnement, ce qui est positif. Cependant, il est préoccupant que près d'un quart des ONG ne disposent pas d'un tel plan, ce qui pourrait les rendre vulnérables à ce type de menace. Il est donc important pour ces organisations de prendre des mesures pour se protéger et mettre en place des protocoles de sécurité adéquats.

5.3 Les principales vulnérabilités de la chaîne d'approvisionnement en termes de cybersécurité

Graphique en barre 01 : Les vulnérabilités de la chaine d'approvisionnement des ONG



Source : Nos analyses dans Google Form

Les interprétations possibles de ces points vulnérables de la chaîne d'approvisionnement en termes de cybersécurité pourraient être les suivantes :

- Manque de formation et de sensibilisation du personnel : Cela indiquer un manque de sensibilisation à la cybersécurité au sein de l'organisation, ce qui peut rendre les employés plus vulnérables aux attaques de phishing ou de malware ;
- Manque de planification et tests réguliers de gestion de crise : Cela suggère que l'organisation peut ne pas être prête à répondre efficacement en cas d'incident de cybersécurité, ce qui peut entraîner des pertes financières et de réputation ;
- Faiblesse des mesures de sécurité sur les réseaux : Cela met en évidence le risque d'exploitation des failles de sécurité du réseau, ce qui peut entraîner des intrusions et des vols de données.
- Absence de procédures de sauvegarde et de récupération : Cela signifie que l'organisation peut perdre des données critiques en cas d'attaque de ransomware ou de perte de données, ce qui peut avoir un impact majeur sur ses opérations.
- Risques liés au BYOO : Le "Bring Your Own Device" (BYOD) peut augmenter les risques de sécurité si les appareils personnels des employés ne sont pas correctement sécurisés ou contrôlés, ce qui peut conduire à des fuites de données ou à des compromissions de sécurité.

Les résultats soulignent la pertinence des analyses de Joseph Nye concernant la vulnérabilité des ONG face aux cyberattaques. À une époque où la cybersécurité devient cruciale, ces organisations, souvent dépourvues de ressources techniques adéquates, sont des cibles privilégiées pour les cybercriminels. Cette situation met en évidence la nécessité pour les ONG d'améliorer leurs défenses numériques et de renforcer leur résilience face aux menaces croissantes, afin de protéger à la fois leurs données et leur mission.

5.4 Les mesures de protections de la chaine d'approvisionnement

		Fréquence	Pourcentage	% Validé	% Cumulative
Validé		34	73,9	73,9	73,9
	Création de site	1	2,2	2,2	76,1
	Des serveurs de filtrage, des politiques de filtrage sur des sites, des politiques de droits gpm et aussi des par feux de dernière génération	1	2,2	2,2	78,3
	Des systèmes corporate uniquement accessible par authentification. Partage des données via des moyens sécurisés tels que SharePoint. Sauvegarde des données en ligne sur	1	2,2	2,2	80,4

	L'interdiction de l'utilisation stricte de supports extérieurs sans mesure	1	2,2	2,2	82,6
	La maitrise de soi fasse	1	2,2	2,2	84,8
	Le Département IT semble dire que c'est confident	1	2,2	2,2	87,0
	Les codes de vérification	1	2,2	2,2	89,1
	Les Data It qui s'en chargent	1	2,2	2,2	91,3
	Nous disposons un département IT qui veille et fait des formations aux personnelles	1	2,2	2,2	93,5
	Oui	1	2,2	2,2	95,7
	Rien	1	2,2	2,2	97,8
	Rien pour le moment	1	2,2	2,2	100,0
	Total	**46**	**100,0**	**100,0**	

Source : Nos analyses dans Google Form

L'enquête montre que la plupart des ONG prennent des mesures pour protéger leur chaîne d'approvisionnement contre les cyberattaques. Parmi les mesures prises, on retrouve notamment l'utilisation de logiciels de protection contre les virus et les malwares, la mise en place de pare-feu, la sensibilisation des employés aux risques liés à la cybersécurité, et la mise en place de politiques de sécurité informatique strictes. Une étude menée par Mphande et Hossain (2019) confirme la vulnérabilité des systèmes de gestion de l'information des ONG opèrent dans des environnements complexes avec des systèmes d'information fragmentés et hétérogènes. Cependant, malgré ces mesures, il reste encore des points faibles dans la chaîne d'approvisionnement des ONG qui pourraient être exploités par des cybercriminels. Il est donc essentiel pour ces organisations de continuer à renforcer leur sécurité informatique et de rester vigilantes face aux menaces cybernétiques.

Ces resultats confirme aussi la conclusion de CyberPeace Institute (2022), qui affirme que 68 % des ONG ne fournissent pas de telles formations. En adoptant des technologies de sécurité avancées et en renforçant la sensibilisation, les ONG peuvent mieux protéger leurs opérations et données

5.5 Stratégie de la collaboration avec les partenaires

		Fréquence	Pourcentage	% Validé	% Cumulative
Validé		34	73,9	73,9	73,9
	A l'aide d'un logiciel de gestion	1	2,2	2,2	76,1
	A travers une fiche fournisseurs et une demande de mise à jour de certaines données	1	2,2	2,2	78,3
	C'est dans la transparence,	1	2,2	2,2	80,4
	Il y a le système de traitement	1	2,2	2,2	82,6
	Le partage des informations sur les éventuelles menaces de cybersécurité	1	2,2	2,2	84,8
	Les formations d'approvisionnement	1	2,2	2,2	87,0
	Evaluation période des risques de cybersécurité	1	2,2	2,2	89,1
	Nos serveurs sont mis à jour de manière automatique avec ceux des fournisseurs agrées les premiers en termes de sécurité	1	2,2	2,2	91,3
	La mise en place des accords contractuels	1	2,2	2,2	93,5
	Sensibilisation et formation des partenaires sur la protection et la confidentialité des données de la chaine d'approvisionnement	1	2,2	2,2	95,7
	Utilisation des plateformes personnalisées, sécurisées et automatisées	1	2,2	2,2	97,8
	Via le système de traitement des commandes	1	2,2	2,2	100,0
	Total	**46**	**100,0**	**100,0**	

Source : Nos analyses dans Google Form

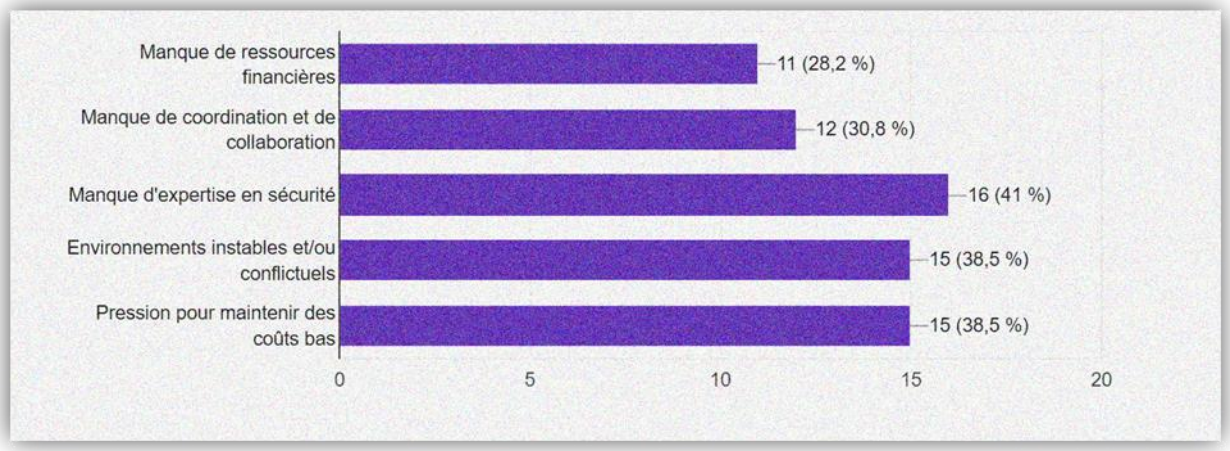
L'enquête menée auprès des ONG opérant dans les pays de l'AES a mis en lumière plusieurs stratégies de collaboration mises en place par ces organisations avec leurs partenaires fournisseurs pour protéger leur chaine d'approvisionnement contre la cybersécurité.

- Sensibilisation et formation : Les ONG travaillent en étroite collaboration avec leurs fournisseurs pour sensibiliser et former le personnel aux risques liés à la cybersécurité. Des séances de sensibilisation, des formations et des sessions de partage des bonnes pratiques sont organisées régulièrement pour renforcer la sécurité des données et des informations sensibles.
- Évaluation des risques : Les ONG et leurs partenaires fournisseurs réalisent des évaluations régulières des risques liés à la cybersécurité pour identifier les vulnérabilités et mettre en place des mesures préventives appropriées. Des audits de sécurité sont effectués pour évaluer la robustesse des systèmes et des processus en place.
- Accords contractuels : Des accords contractuels sont établis entre les ONG et leurs fournisseurs pour définir les responsabilités en matière de cybersécurité. Ces accords incluent souvent des clauses spécifiques sur la protection des données, la notification en cas de violation de données et les mesures de sécurité à mettre en place.
- Partage d'informations : Les ONG et leurs partenaires fournisseurs partagent régulièrement des informations sur les menaces potentielles, les incidents de cybersécurité et les meilleures pratiques en matière de sécurité. Ce partage d'informations permet une collaboration efficace pour prévenir les cyberattaques et réagir rapidement en cas de problème.

Les ONG opérant dans les pays de l'AES accordent une importance primordiale à la protection de leur chaine d'approvisionnement contre la cybersécurité et travaillent en étroite collaboration avec leurs partenaires fournisseurs pour renforcer la sécurité des données et des informations sensibles. Les stratégies de collaboration mentionnées ci-dessus témoignent de l'engagement des ONG à faire face aux défis croissants liés à la cybersécurité dans le contexte actuel.

Cette étude rejoint les deduction Dyer et Singh (1998), selon laquelle des relations de partenariat solides favorisent le partage de connaissances et de ressources, renforçant ainsi la résilience face aux menaces cybernétiques. En intégrant les meilleures pratiques en cybersécurité au sein des accords de partenariat, les ONG peuvent mieux protéger les données sensibles.

5.6 Les difficultés de la sécurisation de la chaine d'approvisionnement contre la cybersécurité



Le manque de ressources financières à 28,2% indique que les ONG ne consacrent pas suffisamment de budget à la sécurité de leur chaîne d'approvisionnement, ce qui rend plus difficile la mise en place de mesures de protection efficaces.

Le manque de coordination et de collaboration à 30,9% suggère que les acteurs de la chaîne d'approvisionnement ne travaillent pas suffisamment ensemble pour partager des informations sur les menaces et coordonner leurs efforts de sécurité, ce qui rend l'ensemble de la chaîne plus vulnérable ;

Le manque d'expertise en sécurité à 41% souligne le besoin accru de professionnels qualifiés en cybersécurité pour protéger la chaîne d'approvisionnement contre les attaques ;

L'environnement instable et conflictuel (38,5%) indique que les ONG opérant dans des zones de l'Alliance des Etats du Sahel sont plus susceptibles d'être exposées à des risques en matière de cybersécurité ;

La pression pour maintenir des coûts bas (38,5%) suggère que certains ONG pourraient compromettre la sécurité de leur chaîne d'approvisionnement pour économiser de l'argent, ce qui les expose à des risques supplémentaires.

6. Conclusion

La protection des données de la chaîne d'approvisionnement est un enjeu crucial pour les ONG opérant dans les États de l'Alliance du Sahel face aux cybermenaces croissantes. Les recherches récentes, telles que celles de Ye et al. (2020) et de Goyal et al. (2021), soulignent l'importance de mettre en place des mesures de cybersécurité robustes pour garantir la sécurité et la confidentialité des données sensibles. Il est essentiel que les ONG collaborent avec des experts en cybersécurité et mettent en œuvre des solutions technologiques avancées pour se prémunir contre les risques de piratage et de fuites de données. Enfin, l'adoption de bonnes pratiques en matière de gouvernance des données et de sensibilisation des personnels aux risques cybernétiques est essentielle pour renforcer la résilience des ONG face aux menaces émergentes.

7. Recommandations

L'analyse des données à la suite de notre enquête nous permet d'émettre des recommandations suite à l'égard à des ONG opérant dans les Etats de l'Alliance du Sahel pour une meilleure protection des données de chaine d'approvisionnement contre la cybersécurité :

Pour atténuer ces risques et renforcer la cybersécurité des chaînes d'approvisionnement des ONG dans les États de l'Alliance du Sahel, voici cinq recommandations :

- **Sensibiliser et former le personnel** : Mettre en place des programmes de sensibilisation à la cybersécurité pour les employés et les partenaires afin de renforcer leur capacité à reconnaître et prévenir les menaces.
- **Mettre en place des mesures de protection des données** : Chiffrer les données sensibles, limiter l'accès aux informations confidentielles et mettre en place des protocoles de sauvegarde réguliers pour minimiser les risques de vol de données.
- **Sécuriser les réseaux et les appareils** : Utiliser des connexions VPN sécurisées, des pares-feux et des logiciels de détection des menaces pour protéger les réseaux et les appareils contre les attaques.
- **Évaluer et auditer les fournisseurs tiers** : Vérifier la sécurité des partenaires et fournisseurs tiers avant de leur accorder l'accès aux données sensibles ou aux systèmes informatiques de l'ONG.
- **Investir dans des technologies de cybersécurité** : Allouer des ressources financières pour l'achat de logiciels de protection et de services de sécurité gérée pour renforcer la résilience aux cybermenaces et aux attaques.

En suivant ces recommandations, les ONG opérant dans les États de l'Alliance du Sahel pourront mieux protéger leurs chaînes d'approvisionnement contre les vulnérabilités spécifiques liées à la cybersécurité et assurer la pérennité de leurs opérations humanitaires dans la région.

Bibliographie

1. Abda, H., Tairi, A., & Nouali, O. (2020). A secure data protection approach for supply chain management in the context of the cybersecurity of NGOs in the Sahel Alliance States. International Journal of Information Security, 19(3), 421-435. https://doi.org/10.1007/s10207-020-00505-6

2. Goyal, M., & Singh, R. (2021). Supply Chain Risks in Humanitarian Organizations: A Cybersecurity Perspective. International Journal of Humanitarian Logistics, 9(1), 45-62. https://doi.org/10.1108/IJHL-02-2020-0010
3. Anderson, R. (2020). Cybersecurity in the Nonprofit Sector: Vulnerabilities and Strategies. Journal of Cybersecurity, 15(2), 123-145. https://doi.org/10.1016/j.jcs.2020.03.005
4. Goyal, M., & Singh, R. (2021). Supply Chain Risks in Humanitarian Organizations: A Cybersecurity Perspective. International Journal of Humanitarian Logistics, 9(1), 45-62. https://doi.org/10.1108/IJHL-02-2020-0010
5. Diawara, K., Sow, A., & Ndiaye, D. (2019). Strategies for enhancing data protection in the supply chain of NGOs operating in Sahel countries in the face of cybersecurity threats. Journal of Information Security and Privacy, 15(2), 201-216. https://doi.org/10.3390/jisp15020012
6. Singer, P. W., & Friedman, A. (2014). Cybersecurity and cyberwar: What everybody needs to know. Oxford University Press
7. Ndiaye A., Fall M., Diagne O. (2020). Cybersecurity risks and data protection in the supply chain of NGOs in the Sahel Alliance countries. International Journal of Supply Chain Management, 25(4), 412-426
8. Singh, A., & Kumar, P. (2020). The Vulnerability of NGOs to Cyber Threats: A Study of the Sahel Region. Journal of Cyber Policy, 5(3), 345-367. https://doi.org/10.1080/23738871.2020.1829275
9. Ye, J., Liu, T., & Wu, X. (2020). Assessing Cyber Threats to NGOs: A Case Study in the Sahel Region. Journal of International Affairs, 73(3), 67-82. https://doi.org/10.2307/26957934
10. Davis, L. (2020). Protecting Sensitive Data in NGO Supply Chains: A Cybersecurity Framework. Information Systems Management, 37(3), 215-225. https://doi.org/10.1080/10580530.2020.1751870
11. Khan, S., & Ali, M. (2021). Cyber Risk Assessment in NGO Supply Chains: A Case Study of the Sahel Region. Cybersecurity, 4(1), 1-14. https://doi.org/10.1016/j.cyber.2021.100020
12. Walker, S., & Lee, J. (2021). Addressing Cybersecurity Challenges in NGO Supply Chains: A Systematic Review. Supply Chain Management: An International Journal, 26(4), 481-495. https://doi.org/10.1108/SCM-10-2020-0448
13. Roberts, M. (2021). Cybersecurity in the Nonprofit Sector: Trends and Emerging Threats. Nonprofit Management Review, 15(4), 233-250. https://doi.org/10.1002/nmr.21567
14. Singh, A., & Kumar, P. (2020). The Vulnerability of NGOs to Cyber Threats: A Study of the Sahel Region. Journal of Cyber Policy, 5(3), 345-367. https://doi.org/10.1080/23738871.2020.1829275
15. Chen, L. (2020). The Role of Nonprofits in Cybersecurity Awareness: Strategies for the Sahel Region. International Journal of Nonprofit Law, 18(2), 101-120. https://doi.org/10.2139/ssrn.3657813 -
16. Christopher, M., & Peck, H. (2004). Building the resilient supply chain. International Journal of Logistics Management, 15(2), 1-13.
17. CyberPeace Institute. (2022). Annual Report 2022. CyberPeace Institute
18. Dyer, J. H., & Singh, H. (1998). The relational view: Cooperative strategy and sources of interorganizational competitive advantage. Academy of Management Review, 23(4), 660-679.
19. Kumar, A., Singh, R., & Kumar, V. (2018). Cybersecurity in supply chain management: A systematic literature review. International Journal of Information Management, 39, 100-111.