Quand l'informatique s'effondre : expérience infirmière et résilience face à la cyberattaqu

Auteur : Hébrant, Mathilde
Promoteur(s) : Briganti, Giovanni
Faculté : Faculté de Médecine
Diplôme : Master en sciences de la santé publique, à finalité spécialisée en praticien spécialisé de santé publique
Année académique : 2025-2026
URI/URL : http://hdl.handle.net/2268.2/25445

LIÈGE université
Médecine
Sciences de la santé publique

Quand l'informatique s'effondre : expérience infirmière et résilience face à la cyberattaque

Mémoire présenté par **Mathilde HEBRANT**

En vue de l'obtention du grade de

Master en Sciences de la Santé publique

Finalité spécialisée en praticien en santé publique

Année académique 2025-2026

Quand l'informatique s'effondre : expérience infirmière et résilience face à la cyberattaque

Mémoire présenté par **Mathilde HEBRANT**

En vue de l'obtention du grade de

Master en Sciences de la Santé publique

Finalité spécialisée en praticien en santé publique

Année académique 2025-2026

Promoteur : Giovanni Briganti

LIÈGE université
Médecine
Sciences de la santé publique

Engagement de non plagiat

Je soussigné(e) **HEBRANT Mathilde**

Matricule étudiant : **S2300308**

Déclare avoir pris connaissance de la charte anti-plagiat de l'Université de Liège et des dispositions du Règlement général des études et des évaluations. Je suis pleinement conscient(e) que la copie intégrale ou d'extraits de documents publiés sous quelque forme que ce soit (ouvrages, publications, rapports d'étudiant, internet, etc…) sans citation (i.e. mise en évidence de la citation par des guillemets) ni référence bibliographique précise est un plagiat qui constitue une violation des droits d'auteur relatifs aux documents originaux copiés indûment ainsi qu'une fraude. En conséquence, je m'engage à citer, selon les standards en vigueur dans ma discipline, toutes les sources que j'ai utilisées pour produire et écrire le mémoire que je dépose.

Fait le 24/05/2026

Signature

Remerciements

La réalisation de ce mémoire n’aurait jamais été possible sans le soutien et la bienveillance de nombreuses personnes que je tiens à remercier du fond du cœur.

Je tiens d’abord à adresser mes remerciements les plus sincères à mon promoteur, Monsieur Briganti, pour son implication dans ce travail de recherche. Je le remercie pour son engagement, sa motivation et ses échanges tout au long de ce travail. Je le remercie de sa patience et de ne m’avoir jamais abandonnée.

Je souhaite également avoir une pensée pour mes collègues du master, avec qui j’ai partagé ces années intenses. J’y ai fait de magnifiques rencontres, avec des personnes bienveillantes et solidaires, qui ont contribué à rendre ce parcours plus humain et plus riche.

Un merci tout particulier aux participants d’avoir pris le temps pour ces entretiens. Merci pour la confiance et la bienveillance témoignées. Sans eux, ce travail n’aurait pas pu aboutir.

Je remercie aussi la direction du Centre Hospitalier Régional Sambre & Meuse pour m’avoir permis de réaliser ce travail de recherche au sein de l’établissement.

Ma gratitude va à ma famille et mes collègues de travail, qui ont toujours cru en moi et m’ont soutenu tout au long de mon parcours académique, en partageant chacun de mes succès, petits et grands.

Enfin, je souhaite accorder un merci particulier à mon époux, Aurélien, qui durant ces années, m’a toujours soutenue, épaulée, encouragée dans les moments de doute. Son soutien a été essentiel tout au long de ce parcours.

Table des matières

Abréviations

DPI : Dossier patient informatisé

PMI : Prescription médicale informatisée

OMS : Organisation Mondiale de la Santé

ONU : Organisation des Nations unies

ENISA : Agence de l’Union européenne pour la cybersécurité

OCDE : Organisation de coopération et de développement économiques

CHRSM : Centre Hospitalier Régional Sambre & Meuse

ANS : Agence du Numérique en Santé

Résumé

Introduction

L'informatique occupe une place centrale dans le fonctionnement des institutions de santé et dans la qualité des soins. Cette dépendance expose les institutions à des cyberattaques pouvant perturber l'organisation des soins. Le personnel infirmier est directement impacté par cela. L'objectif de cette étude est de s'interroger sur les besoins, les ressources et les obstacles que les infirmiers identifient afin de maintenir la qualité des soins lors d'une cyberattaque en milieu hospitalier.

Matériel et méthodes

Une étude qualitative phénoménologique a été menée auprès d'infirmiers ayant vécu une cyberattaque dans un hôpital. Les données ont été collectées grâce à des entretiens individuels semi-dirigés. Les entretiens ont été retranscrits et analysés dans le but d'identifier les axes d'expérience et de perception des soignants.

Résultats

Les résultats mettent en évidence une désorganisation des soins liée à l'indisponibilité de l'informatique. Les infirmiers décrivent une augmentation de la charge de travail et un risque d'erreurs. Un stress important et un sentiment d'insécurité sont également abordés. Cependant, les participants évoquent des stratégies d'adaptation comme la communication orale, l'entraide et la priorisation des soins.

Conclusion

Cette étude souligne que les cyberattaques sont une menace pour la qualité et la sécurité des soins. Elle met en évidence le rôle central des infirmiers dans la continuité des soins en situation de crise et leur résilience. Les résultats suggèrent la nécessité de la préparation des institutions par la formation des soignants et la mise en place de protocoles adaptés.

Mots-clés

Cyberattaque ; qualité des soins ; résilience ; pratique infirmière ; organisation des soins

Abstract

Introduction

Information technology plays a central role in the functioning of healthcare institutions and in the quality of care. This dependence exposes institutions to cyberattacks that can disrupt the organization of care. Nurses are directly affected by these events. The aim of this study is to explore the needs, resources, and obstacles identified by nurses in maintaining the quality of care during a cyberattack in a hospital setting.

Materials and Methods

A qualitative phenomenological study was conducted among nurses who experienced a cyberattack in a hospital. Data were collected through individual semi-structured interviews. The interviews were transcribed and analyzed, allowing the identification of key themes related to healthcare professionals' experiences and perceptions.

Results

The results highlight a disruption in care organization due to the unavailability of information systems. Nurses reported an increased workload and a higher risk of errors. Significant stress and a sense of insecurity were also described. However, participants identified coping strategies such as verbal communication, teamwork, and prioritization of care.

Conclusion

This study highlights that cyberattacks pose a threat to the quality and safety of care. It emphasizes the central role of nurses in maintaining continuity of care during crisis situations, as well as their resilience. The findings demonstrate the need for institutional preparedness through healthcare professional training and the implementation of appropriate protocols.

Keywords

Cyberattack ; Quality of care ; Resilience ; Nursing practice ; Care organizati

1. Préambule

Mon parcours en tant qu'infirmière m'a permis de prendre conscience de la place essentielle qu'occupent l'informatique dans l'organisation et la sécurisation des soins : dossiers patients informatisés (DPI), prescriptions électroniques (PMI), système de communication interne. Si ces technologies contribuent à améliorer la qualité et la continuité des soins, elles rendent également les institutions de santé dépendantes à leur bon fonctionnement.

Cette réalité a pris une dimension particulière lorsque l'institution hospitalière dans laquelle je travaille a été confrontée à une cyberattaque en mai 2023. À ce moment-là, cela faisait un peu moins de deux ans que j'exerçais dans le service de chirurgie générale. J'ai ainsi été directement confrontée aux conséquences de la cyberattaque sur mon travail. Cette expérience a contribué à ma réflexion pour cette recherche. Les échanges entre collègues, les adaptations mises en place et les difficultés évoquées ont suscité chez moi de nombreuses interrogations quant à la capacité des soignants à maintenir des soins de qualité dans un contexte aussi déstabilisant.

Cette expérience m'a amenée à réfléchir à la dépendance des soins à l'informatique et aux conséquences concrètes de son indisponibilité.

Dans un contexte où les cyberattaques visant les établissements de santé sont en constante augmentation, ces questionnements s'inscrivent pleinement dans une problématique de santé publique. Au-delà de l'incident technique, ces événements mettent en lumière des enjeux organisationnels et humains impactant directement la qualité et la sécurité des soins ainsi que les conditions de travail des professionnels.

Ce travail de recherche se situe à la croisée de mon expérience professionnelle et de mon parcours académique. Il vise à mieux comprendre les besoins, les ressources et les obstacles identifiés par les infirmiers pour maintenir la qualité des soins lors d'une cyberattaque en milieu hospitalier.

2. Introduction

2.1. Etat de la question

Les technologies numériques sont omniprésentes dans le monde actuel et principalement dans le secteur de la santé avec l'imagerie médical, les DPI ou encore les PMI afin d'améliorer la qualité des soins (1,2). Les données résultant de tout cela circulent sur des réseaux afin d'être stockées ou partagées entre professionnels de santé ce qui demande un système de sécurité informatique fort aux institutions de soins (1).

En effet, ces dernières sont sujettes aux cyberattaques qui mettent en péril la sécurité des soins (2). Les piratages informatiques à l'encontre des institutions de santé se sont multipliés ces dernières années, car ce sont des cibles de choix pour plusieurs raisons. D'un côté, les institutions de soins disposent de données confidentielles de valeur qui peuvent être échangées contre de grosses sommes d'argent. Ensuite, les institutions de soins sont facilement piratables parce qu'elles utilisent des systèmes d'exploitation souvent plus anciens. Enfin, une cyberattaque peut engendrer un ralentissement du fonctionnement des institutions de soins qui ne peuvent se le permettre financièrement (3).

Tout cela a des conséquences pour les institutions de soins tels que l'impossibilité d'accéder aux dossiers médicaux, la déprogrammation des interventions ou encore des perturbations non négligeables qui entraînent une surcharge de travail pour le personnel soignant (4). Les cyberattaques ont diverses conséquences sur la qualité et la sécurité des soins. Cela peut aller d'un blocage du système informatique à la fermeture complète d'un établissement de soins (5).

La Belgique est concernée par l'augmentation des cyberattaques visant les institutions de santé. En 2021, le Centre Hospitalier de Wallonie Picarde (CHwapi) a été victime d'une cyberattaque entrainant une interruption des systèmes informatiques (6). En mai 2022, le réseau hospitalier Vivalia a également subi une cyberattaque ayant perturbée les activités de soins (7). Plus récemment, en mai 2023, le CHRSM a été confronté à une cyberattaque majeure impactant l'ensemble des systèmes informatiques durant plusieurs semaines. Les DPI, les PMI et la téléphonie ont été fortement perturbés ce qui a entrainé une réorganisation des soins et une limitation de l'activité de l'institution (8).

Par ce fait, la cybersécurité des institutions de santé semble être un déterminant de qualité et de sécurité des soins. C'est pourquoi, depuis plusieurs années, les gouvernements investissent dans la cybersécurité avec le soutien de l'Organisation Mondiale de la Santé (OMS), de l'Organisation des Nations Unies (ONU) et de l'Organisation de coopération et de développement économiques (OCDE) (10, 11). Les politiques ont lancé divers plans d'action pour faire face aux cyberattaques comme des programmes visant à mettre à niveau les systèmes informatiques des institutions de santé, des financements ainsi que la formation des acteurs de terrain afin de renforcer la protection des données et d'anticiper les impacts organisationnels qu'une cyberattaque peut engendrer (12).

Selon l'OMS, la qualité des soins se définie comme étant des soins qui améliorent les résultats de santé souhaités et reposent sur plusieurs dimensions : l'efficacité, la sécurité, l'accessibilité, la continuité, la rapidité, l'efficience et les soins centrés sur la personne (13). Dans un contexte de cyberattaque, plusieurs de ces dimensions peuvent être compromises, notamment la sécurité et la continuité des soins.

En tant qu'acteurs de première ligne dans la prise en soins des patients, les infirmiers sont directement affectés. Les technologies numériques permettent aux infirmiers de prodiguer des soins de qualité et sécuritaire aux patients. Quand cet environnement numérique est compromis suite à une cyberattaque, la capacité des infirmiers à tracer, coordonner et sécuriser des soins est remis en question ce qui entraine une désorganisation de la prise en soins des patients. Ceci venant s'ajouter à un climat de terrain déjà tendu suite à la surcharge de travail élevée, à la pénurie de personnel soignant et à des attentes croissantes des institutions en matière de qualité et de sécurité des soins (14).

De plus, la cybersécurité est un levier pour lutter contre les inégalités en santé qui demeure dans le monde actuel. En effet, les institutions de santé ne sont pas impactées de la même manière en fonction de leur taille. Il en va de même pour les personnes plus vulnérables comme les personnes âgées, handicapées ou précaires qui sont plus impactées par une cyberattaque. La problématique est donc également un problème de santé globale et d'équité (8).

Si les conséquences techniques et organisationnelles des cyberattaques sont aujourd'hui largement reconnues, leurs impacts sur le vécu des soignants et sur la pratique infirmière restent encore peu documentés.

2.2. Connaissances actuelles

Les institutions de santé sont confrontées à une nouvelle forme de vulnérabilité : les cyberattaques. Ces dernières semblent mettre en difficulté le système de santé en perturbant le travail du personnel soignant, car la sécurité des soins est mise en péril (14). Ce phénomène se multiplie de jour en jour (15). Selon l'Agence de l'Union européenne pour la cybersécurité (ENISA), cela fait quatre années consécutives que le secteur de la santé est le plus touché par des incidents de cybersécurité. Entre janvier 2021 et mars 2023, 42 % des cyber incidents touchant le secteur de la santé concernaient des hôpitaux (16). Les infirmiers sont en première ligne pour assurer la qualité et la sécurité des soins dans ce contexte défaillant (17).

Lors d'une cyberattaque, la pharmacie, les DPI, la téléphonie, les PMI sont inaccessibles. Le personnel soignant, et principalement les infirmiers, sont obligés de revenir à des méthodes manuelles sur papier pour assurer la continuité des soins (18). Ce changement inattendu met les infirmiers face à un risque d'augmentation d'erreurs, d'oublis, mais aussi à une surcharge mentale importante (19).

Les témoignages d'infirmiers ayant vécus une cyberattaque sont nombreux et rapportent un sentiment d'impuissance face à une qualité des soins diminuant à vue d'œil (20). Les diagnostics retardés, les erreurs de prescriptions et les perturbations des dispositifs médicaux mettent les infirmiers dans une situation où ils sont obligés de s'adapter (21, 22). Les services de gestion des risques commencent à intégrer les cyberattaques dans les risques institutionnels (22).

Les travaux réalisés sur ce sujet relèvent des perturbations dans les soins avec le passage au format papier, une communication altérée ainsi que des problèmes dans la qualité et la sécurité des soins à cause des retards et des risques d'erreurs suite à l'impact émotionnel d'un tel événement (23). Dans de telles situations, le personnel soignant doit utiliser des stratégies d'adaptation souvent improvisées et faire preuve de résilience (24).

Des rapports comme celui de l'Organisation de coopération et de développement économiques (OCDE) expliquent que l'humain est un facteur essentiel dans la résilience des institutions de soins face à une cyberattaque (25). Le rapport ENISA insiste également sur le rôle essentiel du personnel soignant lors d'une cyberattaque mais spécifie aussi le manque d'informations et de formations de ceux-ci, faisant d'eux un point vulnérable à la cybersécurité (26).

Du point de vue scientifique, la littérature sur la cybersécurité en santé est en augmentation constante. Cependant, elle est souvent abordée du point de vue technique et organisationnel (25). Les publications traitent principalement des vulnérabilités informatiques, de la protection des données de santé et de la prévention des intrusions (27).

Par contre, peu d'études se consacrent aux impacts d'une cyberattaque sur la pratique infirmière (23). Une ignorance existe encore sur la manière dont les infirmiers s'organisent en l'absence d'accès informatique et sur la façon dont ils arrivent à prodiguer des soins de qualité et sécuritaires tout en assurant la traçabilité de ceux-ci (27).

Les cyberattaques visant les institutions de soins sont en croissance constante mais certains points restent en suspens comme les conséquences concrètes sur la pratique infirmière et la qualité des soins qui en découle.

Il existe également peu d'intérêt pour la dimension humaine lors d'une cyberattaque. Or, les infirmiers se retrouvent avec une charge mentale et des responsabilités supplémentaires (27). Les besoins spécifiques des infirmiers en matière de ressources et de formation lors de ce type d'événement restent peu connus.

Suite aux nombreuses cyberattaques dans les institutions de soins, des recommandations de gestion de crises ont été élaborées. Cependant, il n'existe pas encore un assez grand recul pour vérifier leur faisabilité sur le terrain (29).

En somme, plusieurs points sont encore peu abordés dans la littérature : la pratique infirmière lors d'une cyberattaque, l'impact sur la qualité et la sécurité des soins, les conséquences humaines ainsi que les leviers permettant de gérer ce type de crise.

2.3. Approche théorique et méthodologique

Ce travail interroge la pratique infirmières lors d'une cyberattaque. Il va tenter de documenter l'expérience vécue par les infirmiers lors d'une cyberattaque qui met en péril la qualité et la sécurité des soins.

L'objet de la recherche se focalise donc sur la pratique infirmière de qualité étant les actions mises en place pour prodiguer, le plus possible, la sécurité, la continuité et la pertinence des soins lors d'une cyberattaque (30). La recherche ne cherche pas à évaluer l'efficacité des systèmes informatiques des institutions de santé. Elle ne veut pas non plus mesurer l'impact technique ou économique d'une cyberattaque sur les institutions de santé.

La recherche est centrée sur l'expérience de terrain en essayant de comprendre comment et avec quelles ressources les infirmiers font face à une cyberattaque. Mais également mettre en évidence les obstacles qui les empêchent de réaliser des soins de qualité. Cette approche s'appuie sur divers concepts comme la résilience, la qualité des soins. Selon Hollnagel, la résilience des systèmes de santé se définit comme étant la capacité d'une organisation à anticiper, s'adapter, répondre et continuer à fonctionner malgré des situations imprévues (31). Sur le plan individuel, Bonanno définit la résilience comme la capacité d'une personne à maintenir un fonctionnement psychologique et professionnel stable malgré un événement fortement stressant (32). La recherche suppose que la qualité des soins ne dépend pas seulement du numérique mais aussi de la capacité des soignants à s'adapter à toutes situations.

Cet angle d'approche exclu donc le point de vue technique d'une cyberattaque. La recherche ne cherchera pas non plus à mesurer la qualité des soins et elle ne portera pas non plus sur la cybersécurité.

La recherche s'intéressera à une analyse humaine et professionnelle de la pratique infirmière lors d'une cyberattaque.

2.4. Objectifs du travail

Ce travail s'inscrit dans une approche qualitative phénoménologique inspirée de la phénoménologie existentielle de Thomas & Polio (33). Cette approche vise à comprendre l'expérience vécue des infirmiers confrontés à une cyberattaque en milieu hospitalier.

La phénoménologie existentielle a pour but d'explorer la manière dont les individus perçoivent, interprètent et vivent une expérience. Cette approche semble donc pertinente puisqu'elle permet d'appréhender les dimensions humaines, émotionnelles et organisationnelles (33).

La question de recherche de ce travail est la suivante : « *Comment les infirmiers identifient-ils les besoins, ressources et obstacles pour maintenir la qualité des soins lors d'une cyberattaque en milieu hospitalier ?* ».

L'objectif principal de cette étude est de comprendre l'expérience vécue des infirmiers confrontés à une cyberattaque en milieu hospitalier et la façon dont ils maintiennent la qualité des soins dans un contexte de fonctionnement dégradé.

Les objectifs secondaires de cette étude sont les suivants :

- Identifier les ressources individuelles, collectives et organisationnelles mobilisées par les infirmiers pour faire face à cette situation
- Explorer les difficultés rencontrées par les infirmiers dans l'organisation a continuité et la sécurité des soins lors d'une cyberattaque
- Comprendre les stratégies d'adaptation et de résilience développées par les infirmiers afin de maintenir des soins de qualité

3. Matériel et méthodes

3.1. Type d'étude

Le choix s'est donc orienté vers une étude qualitative. Ce phénomène nécessite d'explorer le vécu des infirmiers face à une situation de crise. Le choix s'est porté plus précisément vers une étude phénoménologique pour comprendre l'expérience telle qu'elle est vécue.

3.2. Population étudiée

La population cible a été constituée d'infirmiers travaillant au Centre Hospitalier Régional Sambre & Meuse (CHRSM) site Meuse qui a subi une cyberattaque en 2023 travaillant avec des patients adultes, ce qui a permis d'obtenir des données le plus exact possible étant donné que c'est encore très présent dans l'esprit des équipes soignantes. Ce choix a reposé aussi sur des critères de faisabilité : proximité géographique, contacts existants et expérience de terrain de la chercheuse.

<u>Critères d'inclusion</u> : être infirmier, avoir été présent lors d'une cyberattaque, travailler dans l'hôpital

<u>Critères d'exclusion</u> : travailler dans le secteur mère-enfants, aux soins intensifs, aux urgences

Les soins intensifs n'ont pas été inclus car ils travaillent avec des dossiers patients au quotidien. De ce fait, ils ont moins ressenti les conséquences de la cyberattaque. Le service des urgences a été exclu en raison de son organisation des soins particulière et un laps de temps de prise en charge plutôt court. Enfin, le secteur mère-enfant a été exclu afin de centrer la recherche sur des infirmiers travaillant auprès d'une patientèle adulte ce qui permet de maintenir une homogénéité dans les situations de soins.

Un échantillonnage raisonné a assuré une diversité culturelle, générationnelle et de genre pour tenter d'atteindre une saturation qualitative. La saturation qualitative a été considérée comme atteinte lorsque l'analyse des derniers entretiens ne permettaient plus l'identification de nouveaux thèmes. Le recrutement a été facilité par les cheffes d'unités dans le respect du volontariat et du consentement éclairé.

3.3. Paramètres étudiés et outils de collecte des données

La collecte des données s'est faite sous forme d'entretiens semi-structurés. Les entretiens étaient individuels, semi-structurés, grâce à des questions ouvertes qui ont permis une liberté dans les propos de la personne. Le guide d'entretien (Annexe 1) était composé de 17 questions principales organisées autour de différents axes : l'expérience vécue, les impacts sur l'organisation des soins, les difficultés rencontrées, les ressources mobilisées ainsi que les stratégies d'adaptation mises en place. Les questions ont été construites et validées par l'ensemble du groupe de recherche, mais également par le comité éthique de l'université.

3.4. Organisation et planification de la collecte des données

Avant que la collecte de données ne débute, l'autorisation de mener la recherche dans l'institution a été demandée à la direction. Suite à l'accord de cette dernière, des affiches (Annexe 2) qui ont été créées par le groupe de recherche et validées par le comité d'éthique de l'université ont été placées aux différentes valves d'informations de l'hôpital ainsi que distribuées dans les différents services. A la suite de cette étape, des personnes ont contacté la chercheuse pour fixer une date d'entretien. Les entretiens ont été réalisés et enregistrés en face à face. Ils ont duré, en moyenne, 25 minutes. La collecte des données a débuté après l'accord du comité d'éthique (Annexe 3) fin janvier 2026 et s'est terminée mi-mars 2026. L'analyse a été réalisée en parallèle.

3.5. Traitements des données et méthodes d'analyse

A la suite des entretiens, les données ont été analysées selon les principes de l'analyse thématique de Braun et Clarke (34). Cette analyse a été réalisée progressivement afin de faire émerger les thèmes significatifs liés à l'expérience vécue des participants. Cela s'est fait au fur et à mesure et en plusieurs étapes, selon les étapes les méthodes d'analyse (34) :

- Retranscription mot à mot des entretiens
- Vérification des transcriptions par une nouvelle écoute
- Lecture et relecture en décelant les unités de sens
- Identification des thèmes sur base des unités de sens mis en évidences
- Un tableau a été réalisé afin d'associer les différentes thématiques et afin d'améliorer la vision d'ensemble

Le codage des données a été réalisé manuellement par la chercheuse, seule, sans utilisation de logiciel d'analyse ce qui a permis une familiarisation progressive avec les verbatims.

3.6. Critères de qualité

Les critères de qualité en recherche qualitative décrits par Lincoln et Cuba (35), puis repris par Ayton (36), ont été pris en compte afin de renforcer la rigueur méthodologique de cette étude :

- Fiabilité : le processus de recherche a été décrit en détail afin de garantir que la démarche soit claire et reproductrice par d'autres chercheurs.
- Crédibilité : la confiance accordée aux résultats repose sur la fidélité des données obtenues auprès des participants, grâce à un recueil rigoureux et un respect des conditions d'entretien.
- Confirmabilité : les résultats reflètent les points de vue des professionnels interviewés, limitant au maximum les influences subjectives de la chercheuse.
- Transférabilité : la description précise du contexte permet à d'autres chercheurs d'évaluer si les conclusions peuvent s'appliquer à leur propre environnement.
- Authenticité : les résultats et expériences des participants sont restitués de manière fidèle et détaillée sous forme de verbatim.

La proximité de la chercheuse avec le terrain étudié, puisqu'elle a exercé au sein de l'établissement étudié lors de la cyberattaque, constituait une richesse pour la compréhension du phénomène étudié et une source de biais possible dans l'interprétation. Pour limiter l'influence des représentations personnelles, la chercheuse a tenté de prendre du recul lors des entretiens et l'analyse de ceux-ci. L'analyse a été réalisée en restant attentive aux propos exprimés par les participants et en s'appuyant sur les verbatim afin de privilégier une interprétation fidèle de l'expérience des participants.

3.7. Aspects éthiques et réglementations

Cette étude respecte les normes du Règlement général sur la Protection des Données (RGPD) : la confidentialité des données a été garantie. Les transcriptions ont été anonymes et codées. L'accès aux données a été limité à la chercheuse. Les enregistrements ont été supprimés un fois que les transcriptions ont été réalisées. Le processus de consentement éclairé a été soigneusement élaboré, approuvé par le comité d'éthique (Annexe 3), puis signé par les participants. Un document détaillant le déroulement de la recherche, l'utilisation des résultats, ainsi que les droits des participants a été remis à chacun. Il y était clairement indiqué que la participation était volontaire. Le respect de la vie privée et la protection des données personnelles ont également été garantis. Enfin, une autorisation pour l'enregistrement des interviews a été sollicitée. Les modalités ont été clairement expliquées aux participants. Une attention particulière a été portée au vécu émotionnel des participants. Un temps d'échange et de débriefing était proposé à la fin de chaque entretien pour permettre aux participants d'exprimer les éventuelles difficultés émotionnelles suscitées par l'évocation de la cyberattaque. Les participants avaient la liberté de retirer leur consentement à tout moment, sans impact sur leur vie professionnelle. Le document a été daté et signé (Annexe 4).

4. Résultats

4.1. Caractéristiques des participants

L'échantillon est composé de douze professionnels de santé interrogés au sein du CHRSM site Meuse. Les professionnels de santé sont des infirmier(ère)s exerçant dans différents services de l'institution lors de la cyberattaque de mai 2023. L'échantillon est représenté par une majorité de femmes (8 participantes) ce qui reflète la féminisation de la profession infirmière. Même si l'objectif de la recherche n'est pas d'explorer les différences liées au genre, cela peut avoir influencé les discours recueillis. Cependant, aucune différence importante semble apparaître entre les participants masculins et féminins. Il comprend des professionnels d'âges offrant ainsi une diversité générationnelle. L'ancienneté professionnelle des participants varie également ce qui permet d'intégrer à l'analyse des points de vue divers.

Le tableau 1 reprend les données socio-démographiques des participants.

Tableau 1 Caractéristiques socio-démographiques des participants.

Participant	Sexe	Nombre d'années d'expérience	Service
1	F	10 ans	Gériatrie
2	F	5 ans	Gastrologie
3	F	23 ans	Cardiologie
4	M	5 ans	Equipe volante
5	M	3 ans	Médecin interne
6	F	36 ans	Pneumologie
7	F	17 ans	Gériatrie
8	M	26 ans	Chirurgie générale
9	M	6 ans	Gastrologie
10	F	4 ans	Médecine interne
11	F	4 ans	Equipe volante
12	F	11 ans	Equipe volante de nuit

<u>Illustration de profils contrastés</u>

Certains profils illustrent particulièrement la diversité des expériences vécues lors de la cyberattaque et les différentes manières de faire face à cette situation.

La participante 10, infirmière en médecine interne depuis quatre ans, décrit une perte de repères professionnels puisqu'elle n'a jamais travaillé avec des dossiers papiers avant la cyberattaque. Elle évoque un sentiment de stress et d'insécurité.

A l'inverse, la participante 6, cheffe d'unité en pneumologie avec trente-six années d'expérience, avait déjà connu le fonctionnement papier avant l'informatisation des soins. Elle décrit donc une adaptation plus rapide à la situation. Son expérience semble avoir constitué une ressource dans la réorganisation des soins et dans la transmission des méthodes de travail.

Enfin, le participant 4, infirmier au sein de l'équipe volante, rapporte avoir ressenti une instabilité organisationnelle. Il explique avoir été confronté à des modes de fonctionnement différents selon les services.

4.2. Présentation des thèmes

Une analyse thématique a été réalisée à partir des données issues des entretiens, Cette analyse a permis de faire émerger des catégories thématiques structurées en sous-thèmes et dimensions.

Afin de rendre compte de sa récurrence des thématiques dans les interviews, des descripteurs qualitatifs ont été utilisés.

Tableau 2. Thèmes, sous-thèmes et dimensions émergents des interviews réalisés au CHRSM site Meuse

Thèmes	Sous thèmes	Dimensions	Verbatim
Dépendance au système informatique	Perte d'accès aux données **(L'ensemble des participants)**	Accès à l'information et continuité de l'information	"On n'avait plus aucune trace des traitements, on devait se fier aux patients ou à notre mémoire." (Int. 3)
	Informatique = sécurité **(La majorité des participants)**	Rôle de l'informatique dans la sécurité	"Quand tout fonctionne, on n'a pas ce genre d'erreur, donc oui ça sécurise énormément." (Int. 1)
	Désorganisation **(La quasi-totalité des participants)**	Perturbation du fonctionnement	"Plus rien ne fonctionnait, on était complètement perdus au début." (Int. 11)
Charge de travail	Surcharge administrative **(L'ensemble des participants)**	Retranscription, dossiers papier	"Ça prenait plus d'une heure à recopier tous les traitements." (Int. 1)
	Gestion du temps **(La quasi-totalité des participants)**	Moins de temps pour les soins	"On faisait vite les soins pour pouvoir faire l'administratif derrière." (Int. 10)
	Réorganisation des pratiques **(L'ensemble des participants)**	Adaptation des méthodes de travail	"On a dû tout recréer en papier, dossier par dossier." (Int. 2)
Qualité des soins	Diminution du temps patient **(La majorité des participants)**	Moins d'écoute, relation altérée	"On était moins présent pour le patient, moins à l'écoute." (Int. 1)
	Priorisation des tâches **(Plusieurs participants)**	Focalisation sur l'essentiel	"On faisait l'essentiel, le reste passait après." (Int. 9)
	Déshumanisation du soin **(Certains participants)**	Moins de relationnel	"On n'avait plus le temps de discuter avec les patients." (Int. 10)
Sécurité des soins	Erreurs médicamenteuses **(L'ensemble des particpants)**	Dosage, oubli, retranscription	"Il y a des patients qui n'ont pas reçu leur traitement pendant plusieurs jours." (Int. 2)

	Manque d'informations critiques **(La quasi-totalité des participants)**	Absence de données clinique	"On ne savait même pas les allergies ou les antécédents." (Int. 9)
	Sentiment d'insécurité **(La quasi-totalité des participants)**	Peur de l'erreur	"On marchait sur des œufs." (Int. 7)
Communication	Communication orale dominante **(L'ensemble des participants)**	Passage à l'oral	"Tout se faisait à l'oral, on allait voir les médecins directement." (Int. 10)
	Perte d'informations **(La quasi-totalité des participants)**	Informations non tracées	"C'était un peu le téléphone sans fil." (Int. 4)
	Coordination pluridisciplinaire altérée **(La majorité des participants)**	Difficultés avec les médecins	"Il fallait courir après tout le monde pour avoir les infos." (Int. 2)
Facteurs humains et expérience	Différences générationnelles **(Plusieurs participants)**	Anciens vs jeunes	"Les plus anciennes savaient faire, les nouvelles étaient perdues." (Int. 1)
	Stress et charge mentale **(L'ensemble des participants)**	Fatigue, pression	"C'était très stressant, on avait peur de se tromper." (Int. 10)
	Apprentissage en situation de crise **(La majorité des participants)**	Développement de compétences	"Ça nous a appris à travailler autrement." (Int. 6)
Travail d'équipe et entraide	Solidarité **(L'ensemble des participants)**	Entraide renforcée	"On s'entraidait beaucoup, on vérifiait ensemble." (Int 4)
	Vérification collective **(La majorité des participants)**	Double contrôle	"On demandait toujours à quelqu'un de vérifier." (Int. 10)
	Soutien des anciens **(Plusieurs participants)**	Transmissions des savoirs	"Les anciennes nous ont expliqué comment faire." (Int. 10)

Organisation institutionnelle	Manque de préparation **(La quasi-totalité des participants)**	Absence de protocoles	“L’hôpital n’était pas prêt à ce genre de situation.” (Int. 5)
	Ressources disponibles **(La majorité des participants)**	Dossiers papiers	“On a reçu des dossiers papiers mais pas tout de suite.” (Int.10)
	Homogénéité des pratiques **(La majorité des participants)**	Différences entre services	“Chaque service faisait à sa manière.” (Int. 11)
Impact organisationnel	Perturbation hospitalière **(Certains participants)**	Annulations actes/examens	“Des opérations ont été annulées.” (Int. 3)
	Gestion des admissions **(Certains participants)**	Difficultés d’accueil	“On a renvoyé des patients chez eux.” (Int. 9)
	Fonctionnement dégradé **(La quasi-totalité des participants)**	Mode crise généralisé	“On fonctionnait vraiment en mode dégradé.” (Int. 9)
Adaptation et résilience	Mise en place progressive de solutions **(La majorité des participants)**	Amélioration dans le temps	“Au début c’était chaotique, puis on s’est organisé.” (Int. 4)
	Stratégies d’adaptation **(La quasi-totalité des participants)**	Ajustements individuels	“On a mis en place nos propres méthodes.” (Int. 2)
	Résilience des équipes **(L’ensemble des participants)**	Maintien des soins	“Malgré tout, les soins ont continué.” (Int. 9)

4.3. Analyse thématique

4.3.1. Dépendance au système informatique

Les entretiens mettent en évidence une forte dépendance aux outils informatiques. Les participants décrivent l'informatique comme étant un élément central de leur travail. La cyberattaque a provoqué une perte des habitudes de travail.

Cette perte de repères met en évidence la forte dépendance de la pratique infirmière aux outils informatiques. Ceux-ci apparaissent comme des éléments essentiels à l'organisation, la sécurisation et la continuité des soins. L'absence des outils informatiques transforme leur manière de travailler et provoque un sentiment de vulnérabilité. Cette dépendance questionne la capacité des hôpitaux à maintenir une continuité des soins en situation de défaillance technologique. L'informatisation des soins améliore la sécurité des soins mais elle emble avoir réduit les capacités de fonctionnement autonome des professionnels.

Plusieurs participants expliquent que l'indisponibilité des DPI et des PMI a perturbé la prise en charge des patients.

Une infirmière de cardiologie explique « *Tout ce qui était traitement médicamenteux, il n'y avait plus aucune trace écrite en fait* » (Int. 3).

D'autres participants expliquent que même les patients étaient habitués au fait que leurs traitements et leurs antécédents soient archivés dans l'ordinateur et ne voyaient donc pas l'intérêt de les connaître.

Pour les participants plus âgés, le fait d'avoir déjà connu le fonctionnement du travail en version papier a été un avantage comparé aux plus jeunes diplômés qui ont toujours connu l'utilisation de l'informatique.

4.3.2. Charge de travail

L'augmentation de la charge de travail est un des éléments le plus souvent évoqué par les participants. La cyberattaque a entraîné un retour au papier et par conséquent une importante charge administrative supplémentaire.

Les participants mentionnent qu'ils devaient consacrer du temps à la retranscription manuelle des traitements médicaux, à la préparation des dossiers, aux commandes de pharmacie. Cette situation montre la charge cognitive du personnel.

Une infirmière de gériatrie explique « *Ça prenait plus d'une heure de recopier chaque fois les traitements »* (Int. 1).

Cette surcharge cognitive illustre que la sécurisation des soins dépend essentiellement des professionnels lorsque les outils informatiques sont indisponibles. Les infirmiers doivent alors compenser des fonctions habituellement automatisées par le système informatique. Ils doivent simultanément mémoriser, vérifier, retranscrire et coordonner des informations habituellement gérées par les outils informatiques. Cette situation semble entraîner une sensation permanente de retard et d'urgence.

Une jeune infirmière explique « *On se dépêchait de faire notre travail en chambre auprès du patient pour pouvoir faire tout ce qui était administratif »* (Int. 10)

Les infirmiers volants expliquent qu'il y avait une charge de travail spécifique étant donné qu'ils devaient constamment s'adapter aux organisations variables d'un services à l'autre.

De manière générale, les participants expriment une augmentation de la charge physique, mentale et organisationnelle.

4.3.3. Qualité des soins

Les participants estiment que les soins essentiels ont pu être maintenus. Cependant, plusieurs participants expriment que certaines dimensions de la qualité des soins ont été altérées comme le relationnel et l'individualisation de la prise en charge.

Face à la surcharge administrative et organisationnelle, certains participants expriment qu'ils ont dû prioriser les soins ce qui a entraîné une diminution du temps d'écoute et d'accompagnement des patients.

Une participante explique « *On était moins présents pour le patient, moins pour l'écouter, pour prendre le temps* » (Int. 1)

Plusieurs participants expliquent que la prise en charge des patients se faisait de manière urgente avec une continuité immédiate et non avec une approche globale.

Malgré cela, certains participants estiment que les soins techniques ont pu être assurés grâce à l'entraide des membres de l'équipe.

La qualité de la prise en charge des patients semble tout de même avoir diminué suite aux difficultés d'organisation, de fatigue.

Au-delà des difficultés organisationnelles, les participants décrivent une transformation du sens même du soin qui devient davantage centrée sur la gestion de l'urgence. Les soins semblent alors se recentrer sur les actes techniques considérés comme indispensables à la survie organisationnelle au détriment des dimensions relationnelles associées à la qualité des soins. Certains participants décrivent néanmoins que le répartissement du fonctionnement hospitalier a parfois favorisé la communication entre collègues.

4.3.4. Sécurité des soins

La sécurité des soins constitue une préoccupation importante dans l'ensemble des entretiens. Les participants décrivent un sentiment d'insécurité lié à la gestion des traitements et à l'absence d'accès aux données médicales. Ce sentiment d'insécurité semble révéler la place centrale des outils informatiques dans les mécanismes de sécurisation des soins.

La retranscription manuelle des prescriptions semble être une source importante d'erreurs suite aux écritures manuscrites, aux oublis de médicaments ou aux erreurs de recopiage.

Plusieurs participants donnent le sentiment de devoir soigner à l'aveugle sans accès aux informations permettant habituellement de sécuriser les soins.

Une infirmière explique « *Il y a eu beaucoup d'erreurs que j'ai vues, même au niveau des médicaments. Malheureusement, des collègues qui n'ont peut-être pas une bonne écriture. Il est mis cinq milligrammes, tu lis un quinze* » (Int. 2)

Une autre participante explique « *On marchait sur des œufs* » (Int. 7)

Les équipes ne se sentaient pas en confiance étant donné qu'elles n'avaient pas accès aux allergies, aux antécédents médicaux, aux résultats biologiques.

Différentes stratégies ont été mises en place pour limiter les risques d'erreurs : la relecture, la vérification entre collègues. Les stratégies de vérification développées par les équipes montrent une culture de sécurité informelle visant à compenser l'absence des outils informatiques. Les résultats mettent en évidence le rôle souvent invisible des infirmiers dans la sécurisation quotidienne des soins. Malgré cela, un climat de vigilance constant et de peur existait.

Le manque d'expérience du fonctionnement papier augmentait le sentiment d'insécurité des jeunes professionnels.

4.3.5. Communication

La communication est un élément central dans le maintien de la continuité des soins surtout lors d'une cyberattaque. Pour se faire, les équipes ont dû revenir à une communication principalement orale.

Les transmissions orales entre équipes sont essentielles afin d'assurer le suivi des patients.

Une infirmière explique « *C'était beaucoup plus des échanges verbaux »* (Int. 1)

Le retour à une communication orale modifie la coordination hospitalière. Cette situation révèle à quel point les outils informatiques sont essentiels à la fluidité organisationnelle et à la sécurisation des informations. Une communication orale engendre une augmentation des déplacements physiques afin de transmettre les informations aux médecins, aux kinésithérapeutes, aux logopèdes.

Le risque exprimé par certains participants est une perte d'informations, des oublis ou des malentendus. Cela montre que l'informatique a un rôle de mémoire organisationnelle au sein de l'hôpital. La disparition des outils informatiques semble avoir rendu visibles certaines fonctions de coordination, de vérification et de régulation intégrées de manière invisible dans le système informatique. La cyberattaque semble avoir rendu visible une partie du travail de coordination habituellement gérée par les outils informatiques.

Une participante compare cette situation à « *Un jeu du téléphone sans fil »* (Int. 4)

L'absence de téléphonie interne a également compliqué la communication. Certains participants expliquent avoir dû utiliser leurs téléphones personnels pour maintenir les contacts avec les médecins.

4.3.6. Facteurs humains et expérience

Les entretiens mettent en évidence un contraste générationnel important dans le vécu de la cyberattaque. L'expérience professionnelle et la connaissance du fonctionnement papier par les plus anciens participant semblent être des éléments ayant influencés la gestion de la cyberattaque.

Les participants ayant connu les dossiers papier décrivent une adaptation plus rapide et un niveau de stress moins important que les jeunes diplômés. Les différences générationnelles observées semblent refléter une transformation progressive des compétences infirmières. Ils ont été un élément important dans l'accompagnement des jeunes collègues en leur transmettant les méthodes d'organisation, le fonctionnement des dossiers. Les différences générationnelles observées suggèrent une transformation des compétences des infirmiers avec l'instauration des outils informatiques. Les professionnels plus expérimentés mobilisent une mémoire organisationnelle du fonctionnement papier devenue moins présente au fur et à mesure du temps. La cyberattaque a mis en évidence la disparition progressive de certaines compétences liées au fonctionnement papier au profit des outils informatiques.

Une jeune infirmière explique « *Je n'avais jamais travaillé en version papier avant ça* » (Int. 10)

Et en comparaison à cela, une cheffe d'unité explique *« Moi, j'ai connu le papier* » (Int. 6)

Les entretiens mettent en évidence l'impact émotionnel de la cyberattaque. Les participants décrivent du stress, de la fatigue, un sentiment d'incertitude. Ces émotions traduisent une fragilisation du sentiment de contrôle professionnel habituellement soutenu par les outils informatiques.

Une participante rapporte « *C'était un peu la panique »* (Int. 1)

Les entretiens mettent également en évidence des différences entre les services. Les unités comme la gériatrie ou la cardiologie décrivent des difficultés dans la gestion des traitements médicaux et dans la sécurisation des soins. A l'inverse, des services de chirurgie évoquent plus les perturbations organisationnelles et les difficultés de coordination interdisciplinaire. Les infirmiers volants expliquent que pour eux c'était compliqué de s'adapter aux différents fonctionnements des services car chaque unité avait sa propre organisation.

4.3.7. Travail d’équipe et entraide

Le travail d’équipe et l’entraide semblent être des ressources essentielles durant la cyberattaque. Les participants décrivent une mobilisation collective et une solidarité importante.

Plusieurs participants expriment l’importance de l’aide apportée par les infirmiers plus âgés aux plus jeunes.

Une infirmière explique « *Heureusement qu’il y avait les anciennes pour nous expliquer* » (Int. 4)

Les chefs d’unité sont également décrits comme très présents sur le terrain en participant à la gestion administrative, à la préparation des dossiers.

Les infirmiers volants semblent avoir joué un rôle de soutien entre les services en partageant certaines méthodes d’organisation observées dans d’autres unités.

Malgré le stress et la fatigue, les participants décrivent une volonté de maintenir la continuité des soins grâce à la cohésion d’équipe. Les résultats suggèrent que les infirmiers jouent un rôle de régulation invisible permettant de compenser les défaillances organisationnelles liées à l’indisponibilité des outils informatiques.

4.3.8. Organisation institutionnelle

Selon les participants, l’institution a mis diverses mesures organisationnelles afin de maintenir l’activité hospitalière pendant la cyberattaque. Parmi ces ressources, il y a les dossiers papiers, les protocoles de continuité d’activité, les téléphones temporaires et les systèmes de sauvegarde permettant de récupérer certaines données.

Plusieurs participants expliquent malgré tout que certaines ressources n’étaient pas adaptées à leur service.

Un infirmier explique « *on a dû adapter quelques-uns parce qu’ls étaient faits pour les soins intensifs* » (Int. 8)

Il y a des limites organisationnelles qui ont été évoquées comme le manque de personnel, les difficultés de coordination ou l’absence de préparation à ce type de crise. Cependant, selon certains participants, la cyberattaque aurait permis à l'institution d'identifier les faiblesses organisationnelles et de développer de nouveaux outils.

Une cheffe d'unité explique que des « *kits de reprise d'activité* » ont été créés après la cyberattaque pour améliorer la préparation future (Int. 6).

4.3.9. Impact organisationnel

La cyberattaque a eu des conséquences sur l'organisation de l'hôpital. Certaines consultations, opérations ont dû être reportées suite à l'impossibilité d'accéder aux données médicales des patients.

Une infirmière en cardiologie explique « *Toutes les admissions sont rentrées à domicile* » (Int. 3)

Plusieurs participants expliquent que certains patients ont été transférés afin de permettre aux équipes de réorganiser les soins. Le manque d'accès aux radiologies, aux biologies compliquait les décisions médicales et limitait la prise en charge des patients.

Malgré ces difficultés, les équipes ont développé des modes de fonctionnement alternatifs pour assurer un maintien de l'activité.

4.3.10. Adaptation et résilience

Les entretiens mettent en évidence de nombreuses difficultés mais malgré cela, les stratégies développées par les infirmiers peuvent être interprétées comme des mécanismes des résilience organisationnelle. Malgré la désorganisation du système hospitalier, les infirmiers adaptent leurs pratiques afin de maintenir le bon fonctionnement des soins.

Cette résilience ne repose pas uniquement sur des protocoles institutionnels mais sur des ajustements permanents réalisés par les professionnels de terrain afin de maintenir un fonctionnement acceptable des hôpitaux malgré la dégradation des conditions de travail.

Les professionnels ont progressivement développé de nouvelles habitudes de travail afin de maintenir la continuité des soins.

Plusieurs participants pensent que cette expérience à renforcer la communication, l'organisation et l'entraide dans les équipes tout en développant une forme de résilience organisationnelle et professionnelle.

5. Discussion

5.1. Analyse et interprétation des résultats

Les résultats obtenus mettent en évidence qu'une cyberattaque chamboule l'organisation des soins, affectant plusieurs dimensions : techniques, organisationnelles et humaines.

L'indisponibilité de l'informatique, principalement des DPI et des PMI, oblige les infirmiers à utiliser des dossiers papiers ce qui génère une désorganisation des soins. Cette situation entraîne une augmentation de la charge de travail et des risques d'erreurs.

Les participants expliquent également la difficulté d'assurer la continuité des soins et de l'information entraînant un plus grand risque d'erreurs. Cette difficulté à maintenir la continuité des soins illustre la dépendance des institutions hospitalières aux outils informatiques. La continuité des soins semble dépendre des compétences des professionnels mais aussi de la stabilité des outils informatiques. Les résultats mettent en évidence un paradoxe : les outils numériques renforcent la sécurité des soins, mais leur indisponibilité semble fragiliser l'organisation hospitalière devenues dépendantes des outils informatiques. Cette situation met en évidence une tension entre sécurisation technologique et dépendance organisationnelle. Les résultats suggèrent que l'arrivée de l'informatique dans les soins a déplacé certaines fonctions de sécurisation du travail infirmier vers les outils informatiques. Les participants de l'étude décrivent un fonctionnement marqué par l'incertitude et la nécessité de s'adapter en permanence pour préserver la sécurité des soins.

De plus, les résultats mettent en évidence la capacité des infirmiers à s'adapter face à des contraintes. Les participants expliquent développer des stratégies comme renforcer la communication orale, l'entraide ou la priorisation des soins.

Cette capacité d'adaptation peut être interprétée à travers le modèle du Safety-II développé par Hollnagel (30). Dans une perspective Safety-II, la continuité des soins ne repose pas uniquement sur l'absence d'erreurs mais sur la capacité des professionnels à ajuster leurs pratiques face aux perturbations. Le Safety-II s'intéresse à la manière dont les professionnels adaptent leurs pratiques pour maintenir le fonctionnement du système. Dans une logique Safety-II, ces ajustements traduisent la capacité des professionnels à maintenir un bon fonctionnement malgré la dégradation du système. Les résultats montrent que les infirmiers développent différentes stratégies d'adaptation afin de maintenir une continuité des soins. Ces ajustements illustrent les mécanismes de résilience organisationnelle décrits par Hollnagel (30). Les résultats mettent en évidence une forme de résilience organisationnelle et humaine reposant sur les capacités d'adaptation des professionnels.

5.2. Confrontation à la littérature

Les résultats obtenus sont dans la continuité des connaissances concernant les impacts des cyberattaques sur le système de santé.

L'inaccessibilité aux DPI et aux PMI semble être un élément central de la désorganisation de soins. Van Boven et al. (2023) expliquent également que les cyberattaques obligent le personnel soignant à revenir au papier et à développer des stratégies afin de maintenir la continuité des soins (28). Les résultats de cette étude confirment ces observations soulignant les difficultés rencontrées par les infirmiers dans la gestion des traitements et des informations médicales.

Les participants de l'étude rapportent une augmentation de la charge de travail et de la charge mentale. Ces résultats sont en accord avec ceux de Jalali et Kaiser (2018) qui mettent en évidence que les cyberattaques ont un impact sur l'organisation suite aux tâches administratives supplémentaires et la perte d'accès aux informations médicales (27).

La question de la sécurité des soins apparaît dans cette étude. Les participants de l'étude décrivent un risque accru d'erreurs médicamenteuses, un manque d'accès aux informations médicales. Ces résultats sont en cohérence avec les travaux de Dameff et al., qui mettent en évidence les conséquences possibles d'une cyberattaque sur la sécurité des patients (17). La Joint Commission souligne aussi que les cyberattaques sont une menace pour la sécurité des soins et qu'il est nécessaire de préparer les institutions (22).

Les résultats suggèrent l'importance des facteurs humains et la résilience des équipes. Contrairement à certaines études centrées sur les impacts techniques des cyberattaques, les résultats de cette étude mettent en évidence les dimensions émotionnelles et relationnelles vécues par les infirmiers. Les participants décrivent le rôle essentiel de la communication, de l'entraide pour maintenir la continuité des soins. L'OCDE aborde également ces éléments dans son rapport (32). ENISA souligne également les capacités d'adaptation du personnel soignant lors d'une cyberattaque (12).

Pour finir, cette étude confirme que les cyberattaques ne sont pas uniquement un problème technique mais également un problème humain et organisationnel. Franks (2024) explique que cette expérience peut entraîner une fatigue professionnelle et une augmentation de stress (23). Les résultats obtenus sont en accord avec cela en mettant en évidence l'impact émotionnel important vécu par les participants.

5.3. Analyse des biais et limites de l'étude

Plusieurs limites doivent être prises en compte dans l'interprétation des résultats.

Tout d'abord, le choix d'une approche qualitative phénoménologique donne une compréhension du vécu des infirmiers mais ne permet pas la généralisation des résultats. Les données recueillies représentent une expérience spécifique. Pour renforcer la transférabilité des résultats, une description détaillée du contexte de l'étude des participants et du déroulement de la recherche a été réalisée.

Ensuite, il existe un biais de sélection car les participants étant volontaires, ils sont plus sensibles à la problématique étudiée ou plus marqués par l'expérience de la cyberattaque. Il peut donc y avoir une surreprésentation de vécus particulièrement négatifs. Pour limiter ce biais, une diversité de profils a été recherchée en termes de services, d'ancienneté professionnelle, d'expérience et de genre.

Un biais de mémoire est aussi possible car les entretiens ont été réalisés un peu moins de trois ans après l'événement étudié. Certains éléments ont pu être oubliés ou reconstruits par les participants. Cependant, le caractère marquant et inhabituel de la cyberattaque semble favorisé la persistance des souvenirs.

Enfin, la posture de la chercheuse peut constituer une source de biais d'interprétation des données puisqu'elle fait partie du terrain étudié. Cette proximité pouvait favoriser certains biais d'interprétation ou influencer la conduite des entretiens. Cependant, la connaissance du terrain a également été une ressource facilitante dans la compréhension du contexte et la création d'un climat de confiance avec les participants. Pour limiter ce biais, une posture réflexive a été adoptée tout au long de la collecte et durant l'analyse des données.

5.4. Implication en santé publique

Cette étude met en évidence que les cyberattaques en milieu hospitalier dépassent le cadre de l'incident technique. Elles constituent un problème de santé publique suite à leurs impacts sur la sécurité des patients, la continuité des soins, l'organisation des établissements et les conditions de travail des professionnels de santé.

Les résultats montrent la dépendance des hôpitaux aux outils informatiques ainsi que leurs vulnérabilités face à l'interruption de ces derniers. Cette dépendance peut donner l'impression d'une sécurité permanente des soins, alors qu'elle semble fragiliser les capacités de fonctionnement des équipes en situation de défaillance informatique. Les résultats obtenus dépassent le cadre du CHRSM et mettent en évidence une vulnérabilité plus large du système de santé fortement numérisé. Les cyberattaques révèlent plus largement la vulnérabilité du système de santé face à la généralisation de l'informatique dans les soins. Les cyberattaques interrogent la capacité du système de santé à maintenir leurs missions dans un contexte de dépendance informatique croissante. C'est pourquoi, la cybersécurité apparaît comme un déterminant de la qualité et la sécurité des soins.

Cette étude souligne également que la gestion d'une cyberattaque repose sur les capacités d'adaptation des professionnels de santé. Les infirmiers deviennent des acteurs grâce à leurs capacités de réorganisation. Les résultats mettent en évidence l'importance d'intégrer les dimensions humaines et organisationnelles dans les politiques de cybersécurité.

Les résultats soulignent la nécessité de renforcer la préparation des hôpitaux face à une cyberattaque afin de limiter les impacts sur les soins.

Enfin, cette étude soulève des enjeux d'équité en santé. Certains services accueillant des patients plus vulnérables ou fortement dépendants de l'informatique sont plus exposés aux conséquences d'un fonctionnement dégradé. La cybersécurité concerne donc la capacité du système de santé à garantir des soins sécuritaires et accessibles pour l'ensemble de la population.

5.5. Perspectives

Les résultats de cette étude permettent de proposer plusieurs pistes d'amélioration afin de renforcer la préparation des hôpitaux face à une cyberattaque. Les perspectives identifiées concernent la formation des professionnels, le développement de protocole organisationnel, les exercices de simulation et l'intégration de la cyber-résilience dans les plans d'urgence hospitaliers. Les perspectives proposées peuvent s'orienter grâce aux kits d'exercice de crise cyber de l'Agence du Numérique en Santé (ANS) dans le cadre du programme CaRe (37) et avec le Cyber Disruption Toolkit du Greater New York Hospital Association (26) qui insiste sur l'importance de la préparation et des simulations.

La première perspective concerne le développement de formation pour les professionnels de santé. Les résultats montrent que nombreux sont les professionnels qui n'ont jamais travaillé sans informatique. La mise en place d'une formation sur le cyber-résilience pourrait permettre de renforcer les capacités d'adaptation des professionnels. Cette formation pourrait aborder différents points comme la gestion du mode dégradé, l'utilisation des dossiers papiers, la sécurisation des traitements médicamenteux, la priorisation des soins mais aussi la gestion du stress.

La seconde perspective concerne le développement de protocoles standardisés en mode dégradé. Les participants de l'étude décrivent une importante hétérogénéité des pratiques entre services. Les recommandations soumises dans le kit de l'ANS expliquent l'importance de protocoles structurés (37). L'élaboration de protocoles institutionnels incluant des checklists, des modèles standardisés de dossiers, des procédures de retranscription des médicaments pourrait permettre de sécuriser davantage les soins.

Les résultats soulignent l'importance des exercices de simulation. Ils questionnent la préparation réelle des hôpitaux face à des scénarios pourtant devenu fréquent dans le secteur hospitalier. Les kits d'exercice de crise cyber du programme CaRE sont des scénarios simulés qui permettent aux établissements de se préparer (37). L'organisation régulière de simulation de cyberattaque pourrait permettre aux équipes de développer des automatismes.

Le rôle des cadres intermédiaires semble être une dimension à renforcer. Les chefs d'unité sont décrits comme des acteurs clés. Des formations spécifiques pourraient être proposées afin de renforcer leurs compétences en gestion de crise, la communication organisationnelle et la coordination des équipes en contexte de fonctionnement dégradé.

Sur le plan scientifique, des recherches pourraient être faites afin d'explorer l'expérience d'autres professionnels de santé comme les médecins, les pharmaciens, les aides-soignantes mais aussi les patients.

6. Conclusion

Cette étude avait pour objectif d'explorer le vécu des infirmiers confrontés à une cyberattaque en milieu hospitalier ainsi que les impacts sur la qualité et la sécurité des soins. Grâce à une approche qualitative phénoménologique, l'étude a permis de mettre en évidence la manière dont les infirmiers ont vécu la situation et les adaptations mises en place afin d'assurer la continuité des soins.

Les résultats montrent qu'une cyberattaque perturbe l'organisation des soins en affectant plusieurs dimensions : technique, organisationnelle, relationnelle et humaine. L'inaccessibilité à l'informatique entraîne une désorganisation de la pratique infirmière en augmentant la charge de travail et la charge mentale. Les participants de l'étude décrivent une diminution de la sécurité des soins suite aux difficultés d'accéder aux données médicales des patients et au retour des dossiers en version papier.

Cette étude met également en évidence les capacités d'adaptation des infirmiers face à une situation de crise comme la communication orale, l'entraide, la priorisation des soins. L'expérience professionnelle apparaît aussi comme une ressource importante pour maintenir le fonctionnement des soins. Les résultats illustrent l'existence de contraste entre services face à une cyberattaque.

L'originalité de cette étude est l'exploration du vécu infirmier lors d'une cyberattaque en milieu hospitalier. Les travaux existants abordent principalement les aspects techniques et organisationnels alors que cette étude laisse penser que l'impact humain et émotionnelle sur le personnel soignant est tout aussi important.

Enfin, cette étude met en évidence l'importance de la cyber-résilience comme un enjeu de santé publique. Les résultats montrent la nécessité de renforcer la préparation des hôpitaux grâce à des formations, des protocoles de fonctionnement, des simulations. Des recherches complémentaires pourraient permettre d'explorer le vécu d'autres profils impactés par une cyberattaque en milieu hospitalier.

Au-delà de la question technologique, cette étude montre que les cyberattaques interrogent la capacité des hôpitaux à préserver une qualité et une sécurité des soins lorsque l'informatique est défaillante.

7. Bibliographie

1. Barth M. Les systèmes de santé. Annales des Mines - Enjeux numériques. 2024 ; 27(3) : 174-184. Disponible sur : https://stm.cairn.info/revue-enjeux-numeriques-2024-3page-174?lang=fr&tab=texte-integral
2. Vijayakumar KP, Pradeep K, Balasundaram A, Prusty MR. Enhanced Cyber Attack Detection Process for Internet of Health Things (IoHT) Devices Using Deep Neural Network. Processes. 2023 ; 11(4) : 1072. Disponible sur : https://www.mdpi.com/22279717/11/4/1072
3. Owens B. How hospitals can protect themselves from cyber attack. CMAJ. 2020 Jan 27 ; 192(4) : E101–E102. Disponible sur : https://www.cmaj.ca/content/192/4/E101.short
4. Muthuppalaniappan M, Stevenson K. Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. Int J Qual Health Care. 2021 ; 33(1) : mzaa117. Disponible sur https://academic.oup.com/intqhc/article/33/1/mzaa117/5912483
5. Organisation mondiale de la Santé (OMS). Cyberattaques contre les infrastructures de santé critiques. Organisation mondiale de la Santé [Internet]. 2024 Feb 6 [cité 2025 mai 20] ; Disponible sur : https://www.who.int/fr/news-room/questions-andanswers/item/cyber-attacks-on-critical-health-infrastructure
6. Habberey-Knuessi V, Heeb JL, Paula EDM. L'enjeu communicationnel dans le système hospitalier. Recherche en soins infirmiers. 2013 ; 115(4) : 8-18 DOI : 10.3917/rsi.115.0008
7. Belgique : Lockbit revendique l'attaque contre le groupe hospitalier Vivalia. 2022 Mai 20. [Cité 2026 avril 25] Disponible sur : https://incyber.org/article/belgique-lockbit-revendique-lattaque-contre-le-groupe-hospitalier-vivalia/
8. Cyberattaque : Vol de données, chrsm.be. [Cité 2025 avril 25] Disponible sur : https://www.chrsm.be/cyberattaque
9. Abbas HSM, Qaisar ZH, Ali G, Alturise F, Alkhalifah T. Impact of cybersecurity measures on improving institutional governance and digitalization for sustainable healthcare. PLoS One. 2022 Nov 15 ; 17(11) : e0274550. Disponible sur : https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0274550

10. Conseil International des Infirmières. Transformation numérique de la santé et pratique infirmière. Genève (Suisse) : Conseil International des Infirmières ; 2023. 10 p. Disponible sur : https://www.icn.ch/
11. Abbas HSM, Qaisar ZH, Ali G, Alturise F, Alkhalifah T. Impact of cybersecurity measures on improving institutional governance and digitalization for sustainable healthcare. PLoS One. 2022 Nov 15 ; 17(11) : e0274550. Disponible sur : https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0274550
12. European Union Agency for Cybersecurity (ENISA). ENISA threat landscape : health sector (January 2021 to March 2023). Heraklion (Greece) : ENISA ; 2023 Jul. Report No. : TP-04-23-546-EN-N. ISBN : 978-92-9204-638-5. Disponible sur : https://www.enisa.europa.eu/publications/enisa-threat-landscape-health-sector
13. Ministère du Travail, de la Santé, des Solidarités et des Familles. Appui inédit à la cybersécurité des établissements de santé : lancement du deuxième volet du programme de financement CaRE dédié à la stratégie de continuité et de reprise d'activité. Ministère du Travail, de la Santé, des Solidarités et des Familles [Internet]. 2025 Mars 11 [cité 2025 mai 20] ; Disponible sur https://sante.gouv.fr/actualites/presse/communiques-de-presse/article/appui-inedit:a-la-cyber-securite-des-etablissements-de-sante-lancement-du
14. Tisdale N. The hidden injustice of cyberattacks. WIRED [Internet]. 2024 Feb 12 [cité 2025 mai 20] ; Disponible sur : https://www.wired.com/story/cybersecuritymarginalized-communities-problem/
15. Organisation mondiale de la Santé (OMS). Cyberattaques contre les infrastructures de santé critiques. Organisation mondiale de la Santé [Internet]. 2024 Feb 6 [cité 2025 mai 20] ; Disponible sur : https://www.who.int/fr/news-room/questions-andanswers/item/cyber-attacks-on-critical-health-infrastructure
16. Pelletreau B, Riggi J, Gale B, Mossburg SE. Cybersecurity and how to maintain patient safety. PSNet [Internet]. Rockville (MD) : Agency for Healthcare Research and Quality, US Department of Health and Human Services ; 2024 Mar 27 [cité 2025 mai 20] ; Disponible sur : https://psnet.ahrq.gov/perspective/cybersecurity-and-how-maintainpatient-safety

17. Argaw ST, Bempong NE, Eshaya-Chauvin B, Flahault A. The state of research on cyberattacks against hospitals and available best practice recommendations : a scoping review. BMC Med Inform Decis Mak. 2019 Jan 11 ; 19(1) : 10. Disponible sur : https://link.springer.com/article/10.1186/s12911-018-0724-5
18. CNI College. Empowering nurses to combat cyber threats in healthcare. CNI College [Internet]. 2024 Apr 4 [cité 2025 mai 20] ; Disponible sur : https://cnicollege.edu/blog/nursing/nurses-combat-cyber-threats-in-healthcare/
19. Aldridge O. Ascension Seton regains access to electronic health records after ransomware attack. KUT [Internet]. 2024 Jun 4 [cité 2025 mai 20] ; Disponible sur : https://www.kut.org/health/2024-06-04/ascension-seton-regains-access-toelectronic-health-records-after-ransomware-attack
20. The Joint Commission. Preserving patient safety after a cyberattack. Sentinel Event Alert. 2023 Aug 15 ; (67) : 1–6. Disponible sur : https://www.jointcommission.org/
21. Franks A. Cyberattacks : A Recipe for Nurse Burnout and Compromised Patient Care. HIT Consultant [Internet]. 2024 Aug 6 [cité 2025 mai 20] ; Disponible sur : https://hitconsultant.net/2024/08/06/cyberattacks-a-recipe-for-nurse-burnout-andcompromised-patient-care/
22. Devillers O. Cybersécurité des établissements de santé : une réponse tardive et incomplète juge la Cour des comptes. Banque des Territoires. 2025 Jan 8. Disponible sur : https://www.banquedesterritoires.fr/cybersecurite-des-etablissements-desante-une-reponse-tardive-et-incomplete-juge-la-cour-des
23. Boyle K. The Impact of Cyberattacks on Hospital Patients [Internet]. Access Point Consulting ; [cité le 20 mai 2025]. Disponible sur : https://www.accesspointconsulting.com/resources/the-impact-of-cyberattacks-onhospital-patients
24. Greater New York Hospital Association. Cyber disruption toolkit : guidance for hospitals to develop and implement strategies to mitigate cyber disruption impacts [Internet]. New York : Greater New York Hospital Association ; 2024 [cité 2025 mai 20]. Disponible sur : https://www.gnyha.org/toolkit/cyber-disruption-toolkit
25. Jalali MS, Kaiser JP. Cybersecurity in hospitals: a systematic, organizational perspective. J Med Internet Res. 2018 May 28 ; 20(5) : e10059. Doi : 10.2196/10059. PMID : 29807882 ; PMCID : PMC5996174.

26. Van Boven LS, Kusters RWJ, Tin D, van Osch FHM, De Cauwer H, Ketelings L, Rao M, Dameff C, Barten DG. Hacking Acute Care : A Qualitative Study on the Healthcare Impacts of Ransomware Attacks Against Hospitals. medRxiv [Preprint]. 2023 Feb 21 : 2023.02.13.23285854. doi : 10.1101/2023.02.13.23285854. PMID : not assigned.
27. Kwon JM, Kim J, Lee S, Park H, Choi J, Kim Y, et al. Cybersecurity in healthcare : a narrative review of trends, threats, and challenges. J Med Internet Res. 2023 Oct 15. Disponible sur : https://pmc.ncbi.nlm.nih.gov/articles/PMC10583305/
28. Hollnagel E. Safety-I and Safety-II : The Past ant Future Of Safety Management. Farnham : Ashgate Publishing ; 2014
29. Bonanno GA. Loss, trauma, and human resilience : Have we underestimated the human capacity to thrive after extremely aversive events ? American Psychologist. 2004 ; 59(1) : 20-28.
30. Sutherland E, Keelara R, Eiszele S, Haugrud J. Fast-track on digital security in health. Paris (France) : Organisation for Economic Co-operation and Development ; 2023 Nov 21. (OECD Health Working Papers ; no. 164). Report No. : DELSA/HEA/WD/HWP (2023)16. Disponible sur : https://doi.org/10.1787/c3357f9f-en
31. Thomas SP, Pollio HR. Listening to Patients : A Phenomenological Approach to Nursing Research and Practice. Springer Publishing Company. New York, NY, US ; 2002. 294 p.
32. Braun V, Clarke V. Using thematic analysis in psychology. Qualitative Research in Psychology. 2006 ; 3(2) : 77-101.
33. Lincoln YS, Guba EG. Naturalistic Inquiry. Beverly Hills : Sage Publications ; 1985.
34. Dailah HG, Koriri M, Sabei A, Kriry T, Zakri M. Artificial intelligence in nursing : technological benefits to nurse’s mental health and patient care quality. Healthcare (Basel). 2024 Dec 18 ; 12(24) : 2555. Disponible : https://www.mdpi.com/22279032/12/24/2555
35. Agence du Numérique en Santé. Publication d’un nouveau kit d’exercice de crise cyber en établissement sanitaire et médico-social [Internet]. Paris : Agence du Numérique en Santé ; 2025 Avr 17 [cité 2025 mai 21]. Disponible sur : https://esante.gouv.fr/actualites/publication-dun-nouveau-kit-dexercice-de-crisecyber-en-etablissement-sanitaire-et-medico-social

36. Conseil International des Infirmières. L’avenir des soins infirmiers et de la santé numérique : la nouvelle prise de position du CII met en évidence les possibilités et les risques. Conseil International des Infirmières [Internet]. 2023 sept 1 [cité 2025 mai 21]. Disponible sur : https://www.icn.ch/fr/actualites/lavenir-des-soins-infirmiers-et-de-lasante-numerique-la-nouvelle-prise-de-position-du
37. Ayton D. Chapter 26 : Rigour [Internet]. Pressbooks. 2023. Disponible sur : https://oercollective.caul.edu.au/qualitative-research/chapter/__unknown__-26/

8. Annexes

Annexe 1 : Guide d’entretien

Annexe 2 : Affiche de recrutement

Annexe 3 : Avis du comité d’éthique

Annexe 4 : Consentement

Annexe 1 : guide d'entretien

Guide d'entretien

1. **Pouvez-vous me décrire votre rôle au sein de l'hôpital, votre ancienneté dans l'établissement, ainsi que votre parcours en tant qu'infirmier ?**
2. **Etiez-vous présent lors de la cyberattaque ? Dans quel service travaillez-vous à ce moment-là ?**
3. **Comment avez-ou appris qu'une cyberattaque était en cours ?**
4. **Quelles tâches de votre pratique ont été les plus affectées et estimer, pour chacune, le pourcentage d'impact correspondant. Veuillez préciser le pourcentage global d'impact sur votre activité professionnelle.**
5. **Comment avez-vous assuré la continuité des soins ?**
6. **Comment évalueriez-vous l'impact observé sur la qualité et la sécurité des soins dispensé ? Merci de préciser les aspects les plus touchés et d'illustrer, si possible, par des exemples concrets.**
7. **Quelles ressources ont été mises à votre disposition pendant la cyberattaque ?**
8. **Quelles ressources vous ont manqué et auraient facilité votre travail ?**
9. **Quel rôle vos collègues ont-ils joué dans la gestion de la situation ?**
10. **Quelles stratégies avez-vous mis en place pour faire face à la situation ?**
11. **Quels soutiens vous ont aidé ?**
12. **Aujourd'hui, pensez-vous que la cyberattaque vous a permis de développer de nouvelles compétences ? Si oui, lesquelles ?**
13. **Quelles mesures l'hôpital pourrait-il mettre en place pour mieux préparer les soignants ?**
14. **Comment pourrait-on limiter l'impact de ce type de crise sur la qualité des soins ?**
15. **Si cela devait se reproduire, qu'aimeriez-vous voir changer dans la gestion de la cyberattaque ?**
16. **Y-a-t-il autre chose que vous souhaiteriez partager ?**
17. **Comment avez-vous personnellement vécu la cyberattaque ?**

Annexe 2 : affiche de recrutement

Participer à une étude sur la pratique infirmière en cas de cyberattaque !

" Comment les infirmiers identifient les besoins, les ressources et les obstacles pour maintenir la qualité des soins lors d'une cyberattaque en milieu hospitalier ?"

Qui peut participer ?

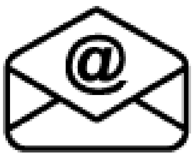
- Etre infirmier(ère) au CHRSM - site Meuse
- Avoir travaillé lors de la cyberattaque de 2023
- Travailler avec la patientèle adulte

Objectif de la recherche :

Comprendre comment les infirmiers vivent et s'adaptent lors d'une cyberattaque afin de maintenir la qualité et la sécurité des soins.

Votre participation :

- Participer à un entretien
- Durée : environ 45 minutes
- Participation volontaire et confidentielle



Intéressé(e) ?

Contactez : Mathilde Hebrant - infirmière au D10 et étudiant en Master en Sciences de la Santé Publique

mathilde.hebrant@student.uliege.be

Votre expérience compte !

Aidez à renforcer la résilience et la qualité des soins

LIÈGE université
Médecine
Sciences de la santé publique

Annexe 3 : avis du comité d'éthique

Comité d'Ethique Hospitalo-Facultaire Universitaire de Liège (707)

LIÈGE université

CHU de Liège

Sart Tilman, le 04/11/2025

Madame le **Prof. A-F. DONNEAU**
Madame **Mathilde HEBRANT**
Service des **SCIENCES DE LA SANTE PUBLIQUE**

Concerne: Votre demande d'avis au Comité d'Ethique
Notre réf: 2025/561

"Comment les infirmiers identifient les besoins, les ressources et les obstacles pour maintenir la qualité des soins lors d'une cyberattaque en milieu hospitalier ? "
Protocole :

Cher Collègue,

Le Comité d'Ethique constate que votre étude n'entre pas dans le cadre de la loi du 7 mai 2004 relative aux expérimentations sur la personne humaine.

Le Comité n'émet pas d'objection éthique à la réalisation de cette étude et sa publication. Il vous recommande toutefois de prendre contact avec le Délégué à la protection des données de l'ULiège, Monsieur P-F. PIRLET (dpo@uliege.be), afin de vous assurer du respect de la réglementation en matière de protection des données.

Vous trouverez, sous ce pli, la composition du Comité d'Ethique.

Je vous prie d'agréer, Cher Collègue, l'expression de mes sentiments les meilleurs.

Prof. D. LEDOUX
Président du Comité d'Ethique

C.H.U. de LIEGE – Site du Sart Tilman – Avenue de l'Hôpital, 1 – 4000 LIEGE
Président : Professeur D. LEDOUX
Vice-Présidents : Docteur G. DAENEN – Docteur E. BAUDOUX – Professeur P. FIRKET
Secrétariat administratif : 04/323.21.58
Coordination scientifique: 04/323.22.65
Mail : ethique@chuliege.be
Infos disponibles sur:http://www.chuliege.be/orggen.html#ceh

MEMBRES DU COMITE D'ETHIQUE MEDICALE
HOSPITALO-FACULTAIRE UNIVERSITAIRE DE LIEGE

Monsieur le Professeur **Didier LEDOUX** Intensiviste, CHU	**Président**
Monsieur le Docteur **Etienne BAUDOUX** Expert en Thérapie Cellulaire, CHU	**Vice-Président**
Monsieur le Docteur **Guy DAENEN** Honoraire, Gastro-entérologue, membre extérieur au CHU	**Vice-Président**
Monsieur le Professeur **Pierre FIRKET** Généraliste, membre extérieur au CHU	**Vice-Président**

Monsieur **Resmi AGIRMAN**
Représentant des volontaires sains, membre extérieur au CHU

Madame **Viviane DESSOUROUX** / Monsieur **Pascal GRILLI** (suppléant)
Représentant (e) des patients, membres extérieurs au CHU

Madame **Régine HARDY** / Madame la Professeure **Adélaïde BLAVIER** (suppléante)
Psychologue, CHU Psychologue, membre extérieure au CHU

Madame **Céline KEMPENEERS**
Pédiatre, CHU

Madame **Sophie KESSELER**
Infirmière, CHU

Monsieur le Professeur **Maurice LAMY**
Honoraire, Anesthésiste-Réanimateur, membre extérieur au CHU

Madame la Docteure **Marie-Paule LECART**
Rhumato-gériatre, membre extérieure au CHU

Madame **Marie LIEBEN**
Philosophe, membre extérieure au CHU

Monsieur **Jacques LOMBET**
Pédiatre, Citadelle

Madame **Patricia MODANESE**
Infirmière cheffe d'unité, CHU

Madame la Professeure **Anne-Simone PARENT**
Pédiatre, CHU

Monsieur **Stéphane ROBIDA**
Juriste, membre extérieur au CHU

Madame **Isabelle ROLAND**
Pharmacienne, CHU

Madame la Docteure **Isabelle RUTTEN**
Radiothérapeute, membre extérieure au CHU

Monsieur le Professeur **Vincent SEUTIN**
Pharmacologue, membre extérieure au CHU

Annexe 4 : consentement

<u>Titre de l'étude</u> : Les besoins, les ressources et les obstacles pour maintenir la qualité des soins dans la pratique infirmière lors d'une cyberattaque en milieu hospitalier

<u>Investigateur</u> : Hebrant Mathilde

<u>Encadrant du mémoire</u> : Professeur Giovanni Briganti

Introduction

Vous êtes invité à participer à une étude qualitative menée dans le cadre d'une mémoire de Master en Santé Publique de l'Université de Liège. Cette étude à pour but de comprendre *comment les infirmiers identifient les besoins, les ressources et les obstacles pour maintenir la qualité des soins lors d'une cyberattaque en milieu hospitalier.* Avant que vous n'acceptiez de participer à cette étude, nous vous invitons à prendre connaissances des points suivants afin que vous puissiez prendre une décision en toute connaissance de cause.

Si vous participez à cette étude, vous devez savoir que :

- Cette étude est soumise à l'évaluation du comité d'éthique de l'université de Liège.
- Votre participation est volontaire et doit rester libre de toute contrainte.
- Les données recueillies sont confidentielles, anonymisées et seront traitées uniquement dans le cadre de cette recherche académique.

Déroulement de l'étude

L'étude sera menée par Hebrant Mathilde, étudiante en master en Sciences de la santé publique dans le cadre de son mémoire. Le recrutement des participants se fera au Centre Hospitalier Régional Sambre et Meuse site Meuse.

Pour pouvoir participer à cette étude, vous devez être infirmier(ère) et avoir été présent lors de la cyberattaque qu'à subi l'hôpital.

L'étude sera réalisée via un entretien semi-directif à question ouverte en français. Il faut compter approximativement 30 minutes.

Contact

Si vous avez besoin d'informations complémentaires, mais aussi en cas de problèmes ou d'inquiétude, vous pouvez contacter le principal investigateur par e-mail mathilde.hebrant@student.uliege.be .

Consentement éclairé

Je déclare que j'ai été informé sur la nature de l'étude, son bu, sa durée et ce que l'on attend de moi. J'ai pris connaissance du document d'information.

J'ai eu l'occasion de poser toutes les questions qui me sont venues à l'esprit et j'ai obtenu une réponse favorable à mes questions.

J'ai compris que des données me concernant seront récoltées pendant toute ma participation à cette étude et que le principal investigateur se porte garant de la confidentialité de ces données.

J'accepte que les données de recherche récoltées pour les objectifs de la présente étude puissent être traitées ultérieurement pour autant que ce traitement soit limité au contexte de la présente étude.

Fait à ____________, le _____________ **Signature :**

Principal investigateur

Je soussigné, Mathilde Hebrant, principal investigateur confirme avoir fourni les informations nécessaires sur l'étude.

Je confirme qu'aucune pression n'a été exercée pour que le participant accepte de participer à l'étude et que je suis prête à répondre à toutes les questions supplémentaires, le cas échéant.