Innovation avec des microjeux pour la gestion hospitalière : utiliser des jeux sérieux pour élaborer des plans de réponse contre le cyberterrorisme

Innovation with microgames for hospital management: using serious games to generate response plans against cyberterrorism

Natalia Zwarts[1], Niek Jan van den Hout[2]

[1]The Hague University of Applied Sciences, correspondence address: n.h.zwarts@hhs

[2]The Hague University of Applied Sciences, correspondence address: n.j.vandenhout@hhs.nl

RÉSUMÉ. La cybersécurité est l'une des professions en pleine expansion, nécessitant un nombre croissant de décideurs compétents. Le besoin de prendre des décisions adéquates ne se limite pas seulement aux spécialistes des technologies de l'information et de la communication (TIC), mais relève également largement de la responsabilité de la direction. L'une des méthodes pour améliorer la prise de décision est de s'exercer à travers des jeux sérieux basés sur des scénarios offrant une révision de la préparation avant qu'une crise ne se matérialise. Le champ de décision change également avec l'arrivée de nouveaux acteurs : des groupes motivés politiquement, financièrement et psychologiquement ciblant les actifs cybernétiques. Les jeux sérieux traitent souvent la sécurité en termes rouge (offensif) et bleu (défensif). Ce chapitre cartographie les différences potentielles qui apparaissent lorsque le profil de l'acteur menaçant est présenté en plus du scénario, permettant ainsi d'adapter les plans de réponse des hôpitaux à la menace spécifique. En conséquence, deux scénarios contrastés sont présentés, générant un plan de réponse pour un groupe de pirates informatiques motivé géopolitiquement et un hacktiviste motivé idéologiquement. Cette approche pourrait être davantage appliquée à la préparation cybernétique dans les hôpitaux, en utilisant le processus décrit dans cette étude.

ABSTRACT. Cybersecurity is one of the fastest growing professions, requiring a growing number of competent decision-makers. The need to make adequate decisions is not limited only to Information and Communication Technology (ICT) specialists, but is also largely the responsibility of management. One of the methods to improve decision-making is to exercise through scenario-based serious games offering a preparedness review before a crisis materializes. The decision scope also changes with some new actors: politically, financially and psychologically motivated groups targeting cyber assets. Serious games often treat security in red (offensive) and blue (defensive) terms. This chapter is mapping the potential differences that arise when the threat actor profile is presented in addition to the scenario, allowing the response plans of hospitals to be tailored to the specific threat. As the result, two contrasting scenarios are introduced, generating a response plan for a geopolitically-motivated hacker group and ideologically-motivated hacktivist. This approach could be further applied to cyber preparedness in hospitals, utilizing the process described in this study.

MOTS-CLÉS. Jeu sérieux, jeu utilitaire, cybersécurité, cyberterrorisme, cyberattaque, hôpital, terrorisme, prise de décision.

KEYWORDS. Serious game, cybersecurity, cyberterrorism, cyberattack, hospital, terrorism, decision-making

Introduction

En avril 2024, un hôpital français a subi une cyberattaque, paralysant ses systèmes numériques : les dossiers des patients, les plannings de rendez-vous et les registres pharmaceutiques étaient

inaccessibles. La décision a été prise de couper tout accès informatique et de revenir au stylo et au papier, même dans des départements critiques, tels que les soins d'urgence, la médecine interne, la chirurgie, la psychiatrie et la pédiatrie [PAG 20]. On a estimé que la récupération serait un processus long, et tous les cas non urgents ont été transférés à d'autres hôpitaux de la région pour une durée indéterminée. La décision de fermer un hôpital est probablement l'une des décisions les plus difficiles que peut prendre une direction : c'est un dernier recours pour protéger les patients et le personnel. Il existe de nombreuses méthodes pour se préparer à prendre ce type de décisions hautement conséquentielles : de la formation individuelle, en passant par des audits à l'échelle de l'organisation, jusqu'aux jeux sérieux reproduisant le défi.

Cet article propose un microjeu pouvant être utilisé pour préparer des plans de réponse aux scénarios de cyberattaque à haut risque, en tenant compte des divergences entre les groupes terroristes exécutant l'attaque, afin de préparer les décideurs à différents types de menaces (par exemple, un pirate informatique criminel demandant une rançon pourrait procéder d'une manière complètement distincte qu'une attaque exécutée par un employé mécontent visant à paralyser un département spécifique). Le cyberterrorisme représente une menace significative lorsque l'hôpital est la cible principale, mais aussi lorsqu'il est ciblé pour empêcher les soins d'urgence nécessaires en raison d'autres attaques [ULM 22].

Le cyberterrorisme est généralement perçu comme moins menaçant que les attaques terroristes conventionnelles, provoquant plutôt de la colère en raison des inconvénients que de la peur due à la violence [JAL 19]. Cette perception peut être trompeuse, car elle crée une illusion de séparation entre les actifs numériques et physiques. En fait, il existe toute une classe d'attaques cybernétiques ciblant les infrastructures physiques (souvent appelées technologie opérationnelle), qualifiées de cybercinétiques [APP 13]. Ce paradoxe entre l'impact élevé et la faible perception de la menace peut entraîner un manque de plans spécifiques pour les cyberattaques dans les hôpitaux.

Les cyberattaques peuvent se limiter à une perturbation à court terme ou se transformer en menace persistante. Si les ressources nécessaires pour y faire face sont plus importantes que disponibles, la direction pourrait devoir décider de cesser complètement ses opérations. Cela est arrivé à un hôpital local qui n'a pas pu se remettre de la crise et a dû être fermé [SEI 24].

En plus des hôpitaux individuelement attaqués, il existe une menace croissante de fournisseurs tiers qui desservent plusieurs sites, qui sont ciblés. Par exemple, *Change Healthcare*, le plus grand gestionnaire d'ordonnances aux États-Unis, a été hors service pendant plus de trois jours, provoquant une interruption des services pour 129 millions de clients [RUN 24]. Non seulement l'attaque a entravé les services normaux, mais elle a également posé une menace supplémentaire en propageant le logiciel malveillant à travers les plateformes connectées. Les attaques contre les grands hôpitaux sont ainsi les plus susceptibles de provoquer une crise régionale, même si les plus petits hôpitaux sont les moins capables de répondre à ces attaques.

Non seulement la perception limitée des menaces, mais aussi la (non)disponibilité des ressources pour y répondre peuvent contribuer au manque de plans de réponse aux cyberattaques. Il y a près de 20 ans, Green [GRE 05] a énuméré les mesures que la direction des hôpitaux devait prendre en compte lors de la planification : la diminution des subventions, le besoin croissant de soins gériatriques et l'augmentation de l'utilisation de la technologie dans les traitements contribuant à des coûts plus élevés. L'Association américaine des hôpitaux a rapporté en 2023 que les coûts des soins aveient augmenté de 17,5%, tandis que les ressources disponibles n'avaient augmenté que de 7,5% [AME 24]. Le même rapport a souligné que des services tels que l'informatique sont devenus 19,7% plus chers, car les traitements numériques nécessitent une infrastructure plus avancée. La forte

dépendance aux équipements électroniques et à l'accès à l'information fait que les risques augmentent avec l'innovation dans les soins à distance.

La combinaison d'une menace croissante, du paradoxe de perception et d'une numérisation rapide des hôpitaux conduit à la nécessité de nouveaux plans de réponse au cybercontreterrorisme. Par conséquent, cette étude vise à réaliser ce qui suit :

- Présenter les défis actuels de la cybersécurité pour les hôpitaux et les menaces terroristes associées.
- Identifier les éléments des jeux sérieux qui reproduisent les défis susmentionnés.
- Proposer un microjeu pouvant être adapté pour générer des plans de contre-terrorisme spécifiques à la menace.

La principale contribution de l'étude est la présentation du processus innovant d'adaptation du jeu sérieux, qui peut être utilisé par les hôpitaux confrontés aux menaces terroristes en matière de cybersécurité.

1. Introduction aux défis de la cybersécurité pour la gestion hospitalière

La prise de décision dans la constellation du personnel hospitalier, du personnel de soutien informatique, des fournisseurs tiers et des intervenants gouvernementaux présente de nombreux défis : de la compétence juridictionnelle et technique aux ressources disponibles. Il existe un certain nombre de défis spécifiques à la gestion hospitalière, notamment la priorisation des menaces, l'allocation des ressources, la pression temporelle et la pénurie de compétences [WOR 23a]. La direction hospitalière doit opérer dans un environnement d'incertitude constante concernant la charge de travail du personnel médical et les bénéfices qui seront générés [GHA 15]. La recherche dédiée à la prise de décision en matière de cybersécurité a diagnostiqué un certain nombre de difficultés pour apporter une réponse efficace à ce type d’événements :

- Tendance à rester dans un mode réactif plutôt que proactif,
- Retards dans le renforcement des capacités de réponse,
- Surconfiance dans les compétences en gestion alors que l'adaptabilité et la décision font défaut [JAL 19].

Dans le même temps, ces difficultés ont été quelque peu réduites par l'application réussie de simulations et de jeux sérieux. Des preuves montrent que les cyberattaques augmentent la collaboration entre les décideurs [KIA 19], ce qui souligne l'idée de maximiser l'échange d'informations et d'expérience.

Pour améliorer la cybersécurité et réduire le risque qu'une attaque réussisse, les facteurs les plus importants à prendre en compte sont l'alignement des parties prenantes internes et la complexité relativement élevée des points d'extrémité au sein des hôpitaux. En d'autres termes, il s’agit d’avoir une compréhension suffisante des systèmes informatiques connectés et parvenir à un alignement entre les différentes parties prenantes des mesures de sécurité internes. Pour tenir compte de cette complexité, le rôle de l'informatique dans le secteur de la santé est décrite dans la section suivante.

1.1. Introduction au secteur de la santé et au rôle des technologies de l'information

La demande mondiale de soins de santé augmente rapidement et, par conséquent, de nombreuses organisations, y compris les hôpitaux, sont soumises à une énorme pression [CRU 19][WOR 22]. Une approche pour gérer efficacement cette charge de travail croissante consiste en l'adoption d'une grande variété de solutions technologiques de traitement de l'information [KRA 21].

Plusieurs tendances qui affectent l'utilisation de la technologie façonnent actuellement le secteur de la santé. En raison de l'augmentation rapide de l'espérance de vie moyenne mondiale, les maladies liées à l'âge et au mode de vie, y compris les maladies chroniques non transmissibles, entraînent un fardeau croissant de la maladie dans le monde entier. Le traitement de ces maladies est relativement difficile et coûteux, ajoutant une pression supplémentaire aux systèmes de santé, y compris les hôpitaux, qui sont déjà confrontés aux effets à long terme de la pandémie du COVID-19 [WOR 23c].

Une autre tendance qui modifie les soins de santé est l'avancement du traitement et de la médecine personnalisés [HAM 10]. Grâce à l'adoption de nouvelles technologies numériques, telles que le séquençage de l'ADN, la protéomique, les dossiers de santé numériques, l'imagerie médicale assistée par l'IA et les dispositifs de surveillance de la santé personnelle, la variation (inter-)individuelle dans les processus de maladie est prise en compte et les informations sur les patients sont disponibles quand et où elles sont nécessaires.

En outre, un autre développement majeur est l'importance croissante de la prestation de soins en dehors de l'hôpital. Les patients reçoivent davantage de soins à domicile grâce à l'utilisation de dispositifs de diagnostic et de surveillance portables et à des systèmes de distribution de médicaments administrés à domicile [WOR 23b].

Les tendances susmentionnées reposent toutes fortement sur les progrès technologiques et l'amélioration de l'acquisition, de l'analyse et de l'application des données. Plus spécifiquement, l'augmentation de la pression sur les organisations et les praticiens de santé nécessite des solutions numériques pour automatiser les activités et accroître leur efficacité. L'avènement de la médecine personnalisée et l'utilisation généralisée des dossiers de santé électroniques nécessitent des technologies d'analyse et de stockage de données novatrices. L'augmentation des soins à domicile nécessite des dispositifs médicaux télémétriques avancés et des applications de surveillance. Cette dépendance à l'informatique entraîne une grande variété de risques en matière de cybersécurité [ARG 20][KRA 21][WAS 22].

1.2. L'environnement technologique et informationnel des hôpitaux

Pour mieux comprendre l'environnement hospitalier et les risques de cybersécurité inhérents, il est nécessaire de comprendre l'environnement technologique et informationnel des hôpitaux. Les hôpitaux existent sous de nombreuses formes et tailles et peuvent être classés selon divers critères. Une classification en fonction de la taille est basée sur le nombre de lits. Un hôpital de taille moyenne typique compte généralement entre 100 et 500 lits. Une autre classification est basée sur le type d'hôpital. Des distinctions sont faites, par exemple, entre les hôpitaux à usage général, les hôpitaux académiques (de recherche), les hôpitaux pour enfants et plusieurs types de cliniques. En fonction de la taille et du type de l'hôpital, son environnement informatique et technologique est structuré différemment.

L'un des traits qui caractérise du système technologique et informationnel des hôpitaux est la nature décentralisée et complexe de leur environnement [PAR 02][JAL 18]. Différents services ont

souvent leur propre système informatique et leurs équipements spécialisés. Cet ensemble d'équipements comprend parfois des systèmes ou dispositifs hérités et obsolètes, mais aussi des équipements acquis de manière ad hoc, sans prendre en compte les exigences de cybersécurité. De plus, différents services sont souvent très spécialisés et opèrent relativement indépendamment les uns des autres d'un point de vue organisationnel, mais sont très connectés d'un point de vue technique.

En plus de la nature complexe et décentralisée de leur environnement technologique et informationnel, les hôpitaux utilisent généralement une grande variété de systèmes d'information différents avec différents cas d'utilisation, ce qui crée une large surface d'attaque [OWE 20]. Ces systèmes comprennent des systèmes fonctionnant comme des systèmes d'information de santé (y compris des dossiers de santé électroniques et des systèmes d'archivage et d'information en radiologie), des applications de télémédecine pour la prestation de soins de santé à distance, des systèmes de support clinique, y compris des systèmes de diagnostic et de surveillance, et des systèmes d'information et administratifs pour la planification, la facturation, la gestion des ressources et de la chaîne d'approvisionnement [WAS 22].

2. Introduction aux risques de cybersécurité spécifiques aux hôpitaux

Comme décrit précédemment, une grande variété de risques ont émergé en raison de l'utilisation croissante des technologies de l'information dans les opérations quotidiennes des hôpitaux. Les risques de cybersécurité sont souvent regroupés en fonction de leur impact sur trois propriétés de la sécurité de l'information, à savoir : la confidentialité, l'intégrité et la disponibilité, également connues sous le nom de triade CIA (pour *Confidentiality*, *Integrity and Availability*) [SAM 14].

Une menace majeure mise en évidence par des rapports sectoriels est celle des rançongiciels (*ransomwares*) et de la divulgation de données associée [ENI 23b][NAT 23]. Alors que les rançongiciels entraînaient, traditionnellement, principalement l'indisponibilité des systèmes et des données, les cybercriminels ont changé leur modus operandi en volant également de grandes quantités de données sensibles (données patients) et en demandant une rançon pour empêcher la publication de ces données [HAC 22]. On estime que les données confiées aux hôpitaux sont 10 à 20 fois plus précieuses à voler que dans tout autre secteur, en raison de leur sensibilité et de leur potentiel de réutilisation (par exemple pour le vol d'identité ou la fraude à l'assurance) [ARG 20]. L'analyse des attaques de rançongiciels en 2023 a montré une baisse de 20% des revenus au cours de la première semaine de l'attaque et une augmentation de la mortalité (passant de 3 décès pour 100 hospitalisés à 4), malgré une baisse des patients acceptés [NEP 23].

Il existe également des cas de divulgation d'informations médicales sensibles en raison d'attaques ciblées, autres que les rançongiciels, soit par ingénierie sociale (*social engineering*), y compris le hameçonnage, soit par l'exploitation de vulnérabilités logicielles. Le vol d'informations médicales sensibles peut entraîner diverses conséquences financières et juridiques, notamment le paiement d'importantes sommes d'argent aux cybercriminels et un examen plus approfondi de la part des régulateurs.

De plus, la suppression ou le blocage de l'accès aux systèmes et données (médicales), ou une violation de leur disponibilité, peut également entraîner une grande variété de conséquences négatives. L'examen susmentionné des incidents de type rançongiciels dans les organisations de soins de santé aux États-Unis signale des perturbations opérationnelles, telles que le détournement d'ambulances, l'annulation de rendez-vous et d'opérations, l'indisponibilité d'équipements tels que les scanners X et les scanners tomographiques par ordinateur, et des systèmes perturbés, y compris

les systèmes de dossiers de santé électroniques [NEP 22]. Un autre type d'attaque qui affecte directement la disponibilité des données est une attaque par déni de service distribué (*Distributed Denial of Service* ou DDoS). Bien que moins courantes que les attaques de rançongiciels, les récentes tensions géopolitiques pourraient avoir entraîné une augmentation de ce type d'attaque [TEI 23].

La manipulation de données et d'appareils médicaux, soit une violation de l'intégrité du système, peut également entraîner des situations dangereuses. Un exemple typique d'un tel scénario est la manipulation d'implants électroniques ayant une fonction thérapeutique, tels que les stimulateurs cardiaques, les défibrillateurs cardioverter implantables (DCI) et les pompes à insuline. En 2017, la *Food and Drug Administration* (FDA) des États-Unis a émis une alerte pour un rappel volontaire d'environ 500 000 stimulateurs cardiaques, citant une exploitation potentielle de vulnérabilités de cybersécurité [DOW 17]. De même, en 2018, des chercheurs en sécurité ont démontré l'exploitation de plusieurs vulnérabilités dans des stimulateurs cardiaques développés par *Medtronic* [SHI 18]. Les chercheurs ont pu manipuler le programmeur du stimulateur cardiaque qui contrôlait les impulsions électroniques envoyées au cœur, pouvant potentiellement entraîner une insuffisance cardiaque. En raison des récentes tensions géopolitiques, un autre exemple pertinent d'une violation de l'intégrité est la défiguration des sites Web d'hôpitaux par des hacktivistes [MAN 12][ROM 17].

2.1 Attaques terroristes contre les hôpitaux

Les attaques terroristes contre les hôpitaux peuvent avoir des conséquences directes sur la disponibilité et l'intégrité des services fournis aux patients, ainsi que des dommages sur leur réputation si la direction n'est pas en mesure de faire face à la crise. Des incidents déjà relevés comprennent le détournement des moyens de transport de l'hôpital pour échapper aux forces de l'ordre (par exemple une ambulance), la prise d'otages pour obtenir un levier auprès du gouvernement local, les attaques physiques contre les infrastructures et les attaques contre les actifs financiers de l'organisation.

Les attaques contre les hôpitaux reflètent les changements géopolitiques, tels que le ciblage des installations par des pirates pro-russes [EUR 24] cherchant à venger les intérêts nationaux (par exemple en travaillant contre les pays qui ont soutenu l'Ukraine ou qui ont voté à l'ONU pour lancer une enquête sur la destruction de biens culturels). Contrairement aux ordres internationaux qui conduisent à ce que des groupes spécifiques prennent pour cible un hôpital dans un pays donné, certaines affaires concernent les soins prodigués à des patients individuels.

Dans un cas relevé aux États-Unis, un hacktiviste a attaqué un hôpital en raison d'un conflit sur un différend entre des parents et le personnel médical. Cet hacktiviste a tenté de faire pression sur la direction pour qu'elle intervienne contre un médecin, qui a fait appel aux services de protection de l'enfance pour séparer un enfant de sa famille (sans un nombre conséquent de preuves de négligence des parents) [REE 18]. La multiplicité des motifs de ces attaques rend souvent la préparation du système plus difficile, car les incidents se multiplient plus rapidement que les plans de réponse disponibles. Il existe des preuves croissantes que les hôpitaux nécessitent un programme de formation pour faire face aux menaces terroristes, reconnaissant la valeur des simulations pour être prêt à affronter des scénarios spécifiques [CHE 23].

Les hôpitaux sont souvent qualifiés de « cibles faciles » en raison de leur sécurité relativement faible et de leur rôle essentiel dans la société. En raison de leurs équipements spécifiques, ils constituent également un site potentiel de menaces chimiques, biologiques, radiologiques et

nucléaires (CBRN), si l'attaque réussissait à libérer des substances nocives. La présence de matériaux dangereux accroît, de fait, l'attrait des hôpitaux en tant que cible.

L'analyse de la *Global Terrorism Database* a identifié 454 attaques terroristes contre des hôpitaux, commises jusqu'en 2022 (sur une période de 50 ans) [ULM 22]. Elle indique également que le nombre d'attaques terroristes augmente de manière disproportionnée contre les hôpitaux par rapport à d'autres cibles, telles que le militaire, les ONG ou les entreprises [MCN 22]. Les menaces terroristes contre les établissements de santé sont considérées comme un scénario à fort impact, avec des études décrivant les mesures existantes contre ce type d'incidents malveillants [DEN 24]. La responsabilité principale de la sélection des bonnes contre-mesures incombe aux administrateurs de l'hôpital concerné, à son conseil d'administration et aux équipes nationales d'intervention spécialisées. Leurs capacités de défense peuvent être améliorées grâce à des jeux sérieux portant sur les deux éléments clés : la menace d'une cyberattaque et le groupe terroriste qui l'exécute contre l'hôpital.

3. Jeux sérieux pour la cybersécurité

Les jeux sérieux sont régulièrement utilisés en cybersécurité pour obtenir des informations sur les choix d'investissement, les stratégies défensives et offensives, ainsi que la capacité organisationnelle à mettre en œuvre des mesures de défense informatique [JAL 19]. Dans la plupart des cas, le jeu sérieux est guidé par des objectifs d'apprentissage et équilibré entre des éléments d'engagement et de valeur éducative. Un jeu sérieux en cybersécurité est un exercice stratégique et proactif conçu pour reproduire un incident réel causé par des acteurs menaçants dans un environnement contrôlé [COE 20]. Il est associé à un scénario qui permet aux organisations d'évaluer et d'améliorer leurs capacités de cybersécurité, d'évaluer les procédures et d'identifier les ressources nécessaires. Leur objectif est de fournir un environnement d'apprentissage dynamique qui reproduit les défis du paysage des menaces cybernétiques en constante évolution.

Un jeu efficace à des fins de cybersécurité présente les qualités suivantes :

- Permettre des résultats imprévus et mettre les joueurs au défi ;
- Répondre aux objectifs de formation ;
- Fournir aux joueurs les informations nécessaires pour prendre des décisions ;
- Offrir un environnement réaliste ;
- Générer des données et des résultats transparents et partageables [HOP 21].

Les principales caractéristiques mentionnées dans la pratique de l'introduction des jeux sérieux en cybersécurité sont l'engagement des joueurs, la configuration à plusieurs niveaux permettant différents niveaux d'expertise et des groupes cibles spécifiques bénéficiant de l'utilisation du jeu sérieux. Dans cet article, la conception a été adaptée à trois éléments : la cybersécurité, les menaces terroristes et la gestion hospitalière comme public cible principal. La combinaison des trois éléments conduit à une conception utilisable spécifique pour la formation dans des scénarios d'attaques planifiées par des groupes terroristes motivés différemment. Pour assurer le réalisme, la configuration inclut à la fois des perspectives de défense et d'attaque.

La configuration classique de la plupart des exercices est divisée en une équipe rouge et une équipe bleue, agissant comme attaquante (équipe rouge / *red team*) et défenderesse (équipe bleue /

blue team) par rapport au scénario. Les définitions de ces deux équipes dans le contexte de la cybersécurité sont présentées dans le tableau ci-dessous :

Blue team	***Red team***
Le groupe chargé de défendre l'utilisation des systèmes d'information d'une entreprise en maintenant sa posture de sécurité contre un groupe de faux attaquants (c'est-à-dire la *Red team*). **Généralement, la *Blue team* et ses soutiens doivent se défendre contre des attaques réelles ou simulées** 1) sur une période significative, 2) dans un contexte opérationnel représentatif (par exemple, dans le cadre d'un exercice opérationnel), et 3) selon des règles établies et surveillées avec l'aide d'un groupe neutre arbitrant la simulation ou l'exercice (c'est-à-dire la *White team*). **Sur la base des conclusions et de l'expertise de la Blue team, ils fournissent des recommandations qui s'intègrent dans une solution de sécurité globale pour renforcer la posture de préparation à la sécurité du client.**	Un groupe de personnes autorisées et organisées **pour émuler les capacités d'attaque ou d'exploitation d'un éventuel adversaire** contre la posture de sécurité d'une entreprise. L'objectif de la *Red team* est d'améliorer la cybersécurité de l'entreprise en **démontrant les impacts des attaques réussies** et en montrant ce qui fonctionne pour les défenseurs (c'est-à-dire la *Blue team*) dans un environnement opérationnel. Aussi connu sous le nom de *Cyber Red team*.

Tableau 1. *Description spécifique à la cybersécurité de la Blue team et de la Red team, basée sur le glossaire de l'Institut national des normes et de la technologie (2024).*

Le jeu sérieux dont il est question icic a été développé pour faciliter l'enseignement d'un cours sur la lutte contre le terrorisme dans une université et accompagner l'expérimentation de plans d'intervention axés sur le profil de la menace. Pour faciliter l'engagement, ainsi que la lecture en temps voulu, le format choisi est celui d'un microjeu.

4. Méthodologie des microjeux

Les microjeux sont des jeux très petits et courts qui offrent un engagement et une expérience significative aux joueurs. Ils soutiennent l'apprentissage et l'instruction vers des objectifs spécifiques et s'intègrent avec les ressources existantes [RAH 21]. Les expérimentations initiales ont prouvé un fort potentiel pour l'utilisation des microjeux grâce à des règles de jeu instantanées, des difficultés désignées et une adaptation au milieu de travail [ZHA 21]. Par essence, les microjeux promettent de fournir un format interactif pour mobiliser les professionnels sans entraver leur flux de travail quotidien. C'est un avantage significatif dans l'utilisation des microjeux dans un contexte hospitalier, étant donné que le personnel et les ressources sont trop précieux pour être réaffectés à un exercice plus long.

Le microjeu proposé dans cette étude présente les paramètres suivants :

• Il peut être joué en 30 minutes, explications comprises ;

• Il tient sur une feuille A4 recto-verso ;

• Il y a 3 tours, avec un événement qui change d'échelle au deuxième tour, offrant un défi supplémentaire aux joueurs ;

• Ses mécanismes sont basés sur l'allocation des ressources (et du personnel), représentant les décisions de gestion ;

• Il peut être joué individuellement ou en équipe faisant des mouvements ;

• La *Red team* est intégrée au jeu et peut être facilement remplacée par un autre groupe d'acteurs malveillants en changeant les tuiles de menace ;

• Les actifs hospitaliers nécessitant un accès informatique sont répertoriés dans des catégories où ils sont utilisés ;

• À la fin du microjeu, les participants ont la possibilité d'utiliser les questions de débriefing pour ajouter des éléments au plan de réponse.

Du point de vue du joueur, ils commencent le jeu en tant que gestionnaire chargé d'un hôpital. Dans chacun des scénarios, l'un des groupes terroristes menace l'hôpital. Cet élément est important pour faciliter les plans de réponse à cette motivation spécifique de l'adversaire (présentée dans la section sur les scénarios).

4.1. Microjeu Gestion Hospitalière

Les objectifs suivants ont guidé le développement du microjeu Gestion Hospitalière :

1. Les participants distinguent différentes catégories d'actifs nécessitant un accès informatique ;
2. Les participants comprennent les liens entre le personnel limité, les ressources et les conséquences des attaques sur la réputation de l'hôpital ;
3. Les participants élaborent un plan spécifique aux menaces pour répondre à une attaque en cybersécurité.

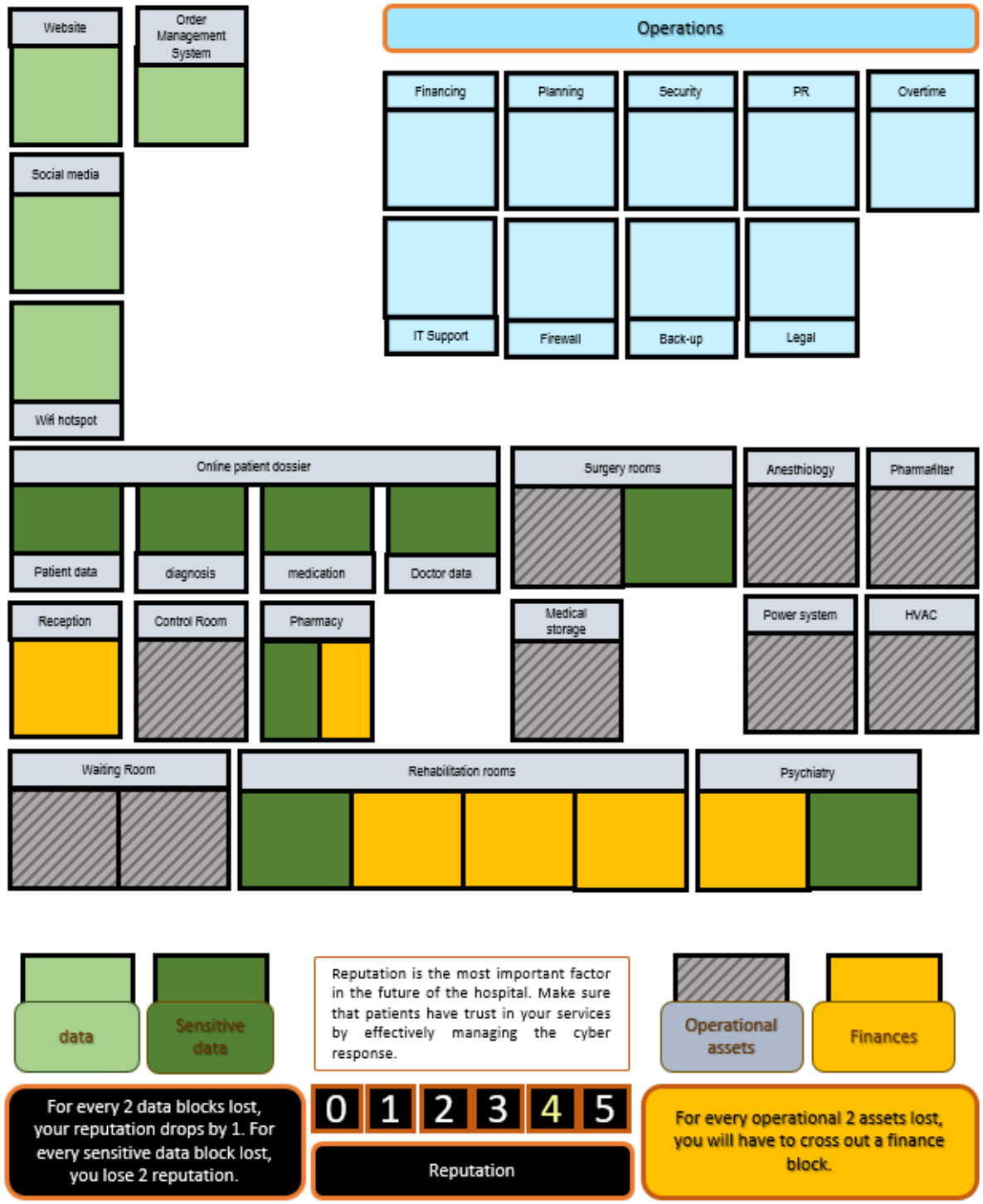

Figure 1. *Microjeu Gestion Hospitalière - page de couverture.*

Le format du jeu se compose d'une feuille A4, présentant la configuration avec les éléments respectifs suivants :

A. Personnel opérationnel (signalés par des cubes bleus) - représentant le personnel disponible pour répondre à une cyberattaque.

B. Actifs - englobant tous les éléments physiques et numériques que l'hôpital aurait à défendre.

C. Échelles de notation - réputation liée aux données, aux actifs et aux finances.

D. Scénario - un scénario est révélé pour chaque tour, lié aux choix effectués par les joueurs.

E. Profils de menace - discutés au début du jeu et intégrés dans le scénario.

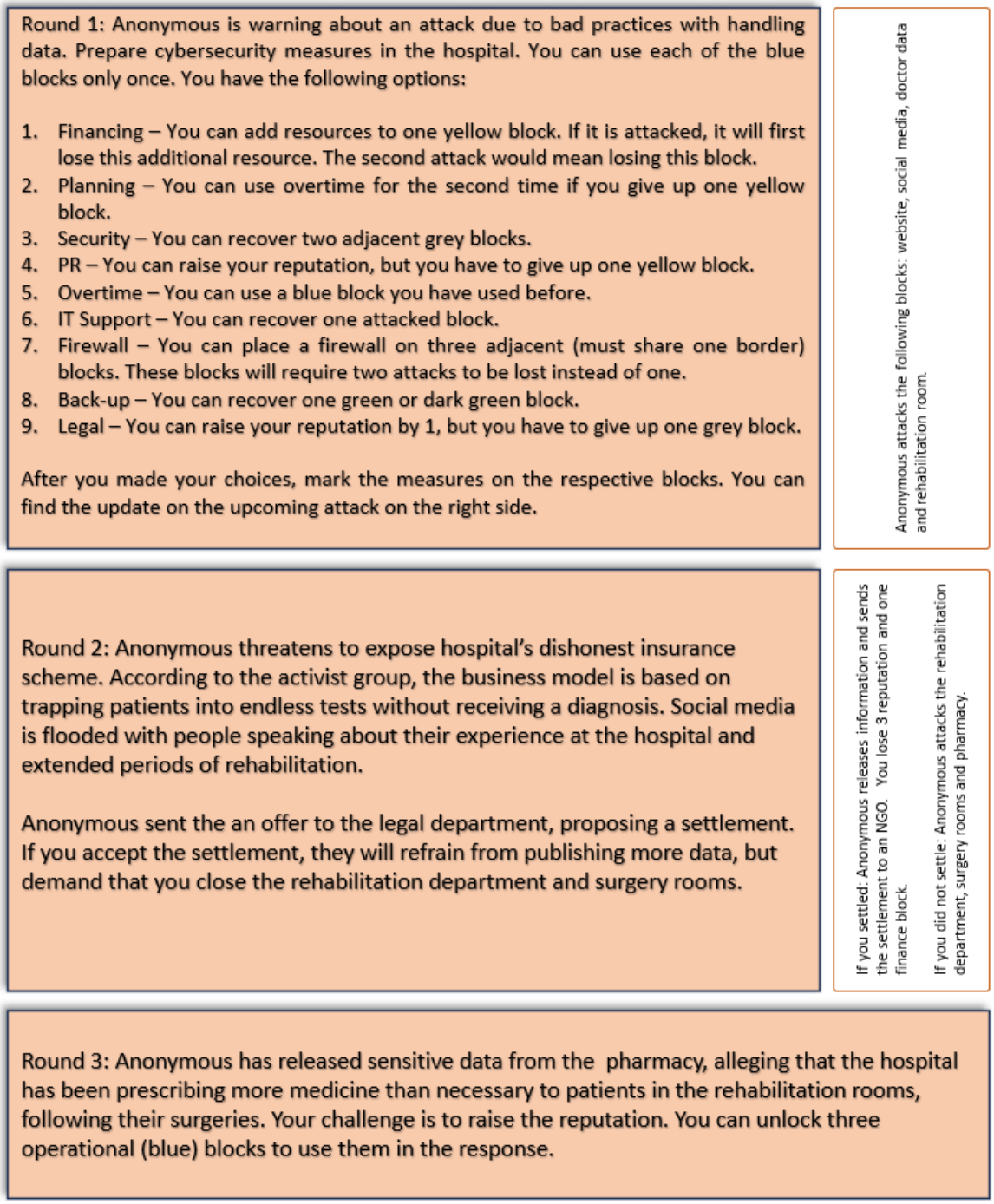

Figure 2. *Scénario et profil de la menace du jeu de gestion de l'hôpital Microjeu.*

4.2. Scénarios

Les scénarios sont basés sur les cinq types distincts de motivations qui peuvent être liées à différents acteurs de menaces en cybersécurité :

• Gain financier : toute action liée financièrement (menée principalement par des groupes de cybercriminalité) ;

• Espionnage : toute action visant à obtenir des informations sur la PI (Propriété Intellectuelle), des données sensibles, des données classifiées (principalement exécuté par des groupes parrainés par l'État) :

• Perturbation : toute action perturbatrice effectuée au nom de la géopolitique (principalement menée par des groupes parrainés par l'État) ;

• Destruction : toute action destructive pouvant avoir des conséquences irréversibles ;

• Idéologique : toute action soutenue par une idéologie (comme l'hacktivisme) [ENI 23a].

Dans le premier essai, deux scénarios ont été préparés afin de comparer les résultats du jeu sérieux. Le premier scénario représentait un groupe hacktiviste et le second un groupe motivé par la destruction.

Scénario 1 : Attaque motivée par l'idéologie sur un hôpital spécialisé dans la rééducation à long terme.

Le groupe motivé idéologiquement a publié un avertissement à un hôpital via les médias sociaux. Leurs premiers X messages mentionnent des problèmes financiers. Le groupe menace d'attaquer l'hôpital et de rendre le problème public, ainsi que la publication de données sensibles des patients et des médecins.

Tour 1 : Les joueurs sont invités à attribuer les départements disponibles pour protéger les actifs de l'hôpital contre les cyberattaques.

Tour 2 : Le groupe motivé idéologiquement attaque le site Web, les médias sociaux, les données des médecins et la salle de rééducation.

Le groupe motivé idéologiquement menace d'exposer le schéma d'assurance malhonnête de l'hôpital. Selon le groupe hacktiviste, le modèle économique est basé sur le fait de piéger les patients dans des tests sans fin sans recevoir de diagnostic. Les médias sociaux sont inondés de personnes parlant de leur expérience à l'hôpital et des périodes prolongées de rééducation.

Le groupe motivé idéologiquement propose un arrangement au département juridique. S'il accepte cet accord, ils s'abstiendront de publier plus de données, mais exigent que les joueurs ferment le service de rééducation et les salles d'opération.

Si les joueurs ont accepté : Le groupe motivé idéologiquement divulgue des informations et envoie le règlement à une ONG. Vous perdez 3 points de réputation et un bloc financier.

Si les joueurs n'ont pas accepté : Le groupe motivé idéologiquement attaque le service de rééducation, les salles d'opération et la pharmacie.

Tour 3 : Le groupe motivé idéologiquement a publié des données sensibles de la pharmacie, affirmant que l'hôpital prescrivait plus de médicaments que nécessaire aux patients dans les salles de rééducation, après leurs opérations. Le défi pour les joueurs est de restaurer la réputation de l'hôpital. Les joueurs pouvent débloquer trois blocs opérationnels (bleus) pour les utiliser dans leur réponse.

Scénario 2 : Attaque motivée par la destruction sur un hôpital dans un pays soutenant l'intervention militaire

Une activité malveillante a été détectée en relation avec une campagne d'ingénierie sociale contre les employés d'une société pharmaceutique. Un avertissement a été publié sur plusieurs comptes de médias sociaux, annonçant que le groupe souhaite venger les victimes de bombardements dans leur pays, qui ont utilisé des munitions fabriquées en Europe.

Le groupe a utilisé *LinkedIn* pour se faire passer pour des chercheurs en logiciels légitimes prétendant avoir trouvé un problème de sécurité dans le système pharmaceutique. Les pirates ont contacté l'hôpital et ont envoyé un lien actif à tous les employés, les invitant à participer à une étude de sensibilisation à la cybersécurité.

Tour 1 : Les joueurs sont invités à attribuer des ressources à leur personnel opérationnel.

Tour 2 : Le groupe a attaqué les blocs suivants : le service de psychiatrie, le pharmafiltre (filtre pour médicaments), la pharmacie et le *hotspot wifi*.

Le pharmafiltre a été éteint et menace maintenant de contaminer l'eau de l'hôpital. La pharmacie a été piratée, les prescriptions ont été mélangées et personne ne peut recevoir le médicament correct. Le *hotspot wifi* a été utilisé pour propager des logiciels malveillants à tous les appareils connectés. Les mesures de sécurité dans le service de psychiatrie ont été détournées et toutes les salles restent fermées.

L'équipe de direction a été contactée avec un ultimatum. Le personnel médical sera libéré si l'hôpital transfère trois de ses cubes financiers au groupe.

Si les joueurs acceptent : Le groupe ne libére pas les otages.

Si les joueurs n'acceptent pas : Le groupe ne libére pas les otages et vous perdez 1 point de réputation.

Tour 3 : Le groupe a publié des communications internes montrant que vous avez négocié avec les terroristes. Le défi des joueurs est de restaurer la réputation de l’établissement. Ils pouvent débloquer trois blocs opérationnels (bleus) pour les utiliser dans leur réponse.

Après que les joueurs ont conclu le dernier tour, ils peuvent consulter les questions de débriefing pour compléter leurs résultats.

4.3. Débriefing

Sur la base des résultats de chaque tour, les participants/joueurs devraient être en mesure de discuter de l'efficacité des contre-mesures choisies contre le groupe spécifique. Les questions supplémentaires suivantes peuvent être proposées pour stimuler une discussion plus approfondie sur les plans de réponse :

• Si ce scénario se produisait, quel serait le meilleur plan pour y répondre ?

• Le plan changerait-il si un groupe terroriste différent attaquait l'hôpital ?

• Quels sont les systèmes informatiques actuels de l'hôpital ? Existe-t-il une compréhension partagée de l'infrastructure numérique ?

• Existe-t-il un inventaire de tous les systèmes dépendant de l'accès à l'ordinateur ? Existe-t-il une vision partagée de la réponse lorsqu'un des systèmes est attaqué ?

• Quelles contre-mesures sont actuellement utilisées pour chacun des systèmes ? Existe-t-il une compréhension des vulnérabilités des fournisseurs tiers ?

• L'hôpital dispose-t-il d'un plan de communication interne concernant les plans de réponse en cybersécurité ?

Le débriefing vise à prendre en compte la complexité du point final et l'alignement des parties prenantes internes mentionnés précédemment comme les facteurs les plus importants pour l'amélioration de la cybersécurité dans les hôpitaux.

5. Résultats

Cette étude visait à présenter les défis en matière de cybersécurité pour les hôpitaux, à identifier les éléments des jeux sérieux reproduisant ces défis et à proposer un microjeu pouvant être adapté pour générer des plans de lutte contre le terrorisme spécifiques aux menaces pour les hôpitaux.

Les défis en matière de cybersécurité pour les hôpitaux comprennent une grande incertitude quant à la charge de travail du personnel médical, les développements technologiques et l'évolution rapide des organisations de soins de santé. Cela inclut le passage aux soins à distance, ainsi qu'une société vieillissante qui nécessite une quantité accrue de traitements. Pour répondre à ces changements technologiques et démographiques, de nombreuses technologies ont été développées : des tests à domicile, en passant par les consultations en ligne, jusqu'aux dispositifs individuels des patients. En raison de cette augmentation de la surface d'attaque, la confidentialité, l'intégrité et la disponibilité des informations (systèmes) sont de plus en plus menacées. Parallèlement, les terroristes ont ciblé les hôpitaux en raison de leur sécurité relativement faible et de leur grande valeur (en termes de données pouvant être vendues ou de rançons pouvant être exigées), ainsi que des enjeux de vie ou de mort liés au fonctionnement de ces établissements. Le risque d'attaques cybernétiques ne cesse d'augmenter en raison de l'augmentation des actifs numériques utilisés dans les traitements et des nouveaux logiciels pour les pharmacies, les dossiers des patients, les systèmes de gestion des commandes et les dispositifs médicaux. Paradoxalement, le cyberterrorisme est rarement considéré comme une menace importante, sur la base de la perception commune selon laquelle le numérique équivaut à une menace non physique. En réalité, les conséquences des cyberattaques incluent l'indisponibilité de l'accès aux informations des patients, le blocage des systèmes critiques et l'arrêt des opérations hospitalières.

La direction est donc confrontée à une situation avec des ressources limitées, une incertitude quant à la charge de travail pour le personnel médical et des risques croissants pour lesquels il est difficile de formuler des plans de réponse. Pour la plupart des établissements, une vue d'ensemble complète de toutes les dépendances n'est pas disponible (car les systèmes sont distribués et liés à des fournisseurs tiers). Dans ce cas, les jeux sérieux peuvent être utiles pour une prise de conscience en jouant les dilemmes de prise de décision pour des scénarios spécifiques de cyberterrorisme contre les hôpitaux.

Les éléments des jeux sérieux identifiés comme utiles en cas de scénarios sur mesure comprennent :

• Ressources et actifs limités,

• Scénario et profil de menace,

• Échelles de notation.

Les paramètres choisis pour soutenir la prise de décision dans le contexte de la gestion hospitalière ont été identifiés comme : le temps (30 minutes), l'espace (une feuille A4), les mécanismes (répartition des ressources par tour) et le débriefing (questions supplémentaires). Ces éléments constituent un microjeu, largement utilisé dans les environnements éducatifs et professionnels.

Le microjeu a été conçu pour générer des plans de réponse basés sur la description de la menace lors du premier tour. Dans la première partie, deux scénarios sont proposés pour différencier un groupe terroriste motivé par l'activisme et l'autre groupe agissant par vengeance géopolitique. En changeant de scénarios, les participants jouant au microjeu peuvent discuter de la manière dont les plans de réponse doivent changer en fonction de la menace spécifique.

Ce prototype a été testé dans le cadre du cours de gestion de la sécurité à la Haute École de La Haye (THUAS), en examinant en profondeur les risques pour les hôpitaux et les contre-mesures spécifiques qui seraient efficaces ou non contre une menace identifiée. Tous les participants ont confirmé une sensibilisation accrue aux problèmes, renforcée également par l'explication des cyberattaques cinétiques capables de cibler l'infrastructure physique.

6. Conclusion

Le microjeu a été un succès lors des tests de jeu, en atteignant les objectifs d'apprentissage initiaux pour les participants. Il y a eu une amélioration dans la distinction des différents actifs, la compréhension des limitations liées à la disponibilité du personnel et la préparation d'un plan de réponse pouvant éviter des dommages à la réputation. Même au sein d'un groupe d'étudiants à la THUAS, il a été possible de générer des plans de réponse qualitativement distincts.

Les hôpitaux ont élaboré des plans de réponse aux attaques terroristes par le passé, déclenchés par des événements à grande échelle. La liste initiale comprenait : panne du système d'air pour les patients, pénurie/défaillance de l'alimentation électrique, menace de bombe, déversement de produits chimiques, panne du téléphone, panne du système informatique, tremblement de terre, inondation, incendie, prise d'otages, défaillance du système d'oxygène, déversement de radiation, défaillance du système de vapeur, défaillance du système de vide, problème d'approvisionnement en eau, conditions météorologiques, évacuation, contamination de l'eau ou personne disparue [CHU 05]. Ces plans spécifiaient la menace générale du terrorisme en un événement indésirable potentiel ayant un protocole de réponse. Le microjeu peut offrir une opportunité similaire en termes de profils de menaces, qui peuvent être discutés selon les cibles spécifiques connues pour être choisies en fonction de la motivation des attaquants.

7. Limites

Malgré le format du jeu qui permet des discussions sur les plans de réponse spécifiques aux menaces, il est possible qu'un groupe terroriste ne suive pas son modus operandi connu et attaque par exemple le point de sécurité le plus faible au lieu de l'objectif initial. Dans ce cas, il serait préférable de collecter les données par paires d'attaques et de contre-mesures qui améliorent leur sécurité. Une autre solution à cette observation pourrait être d'avoir un "plan de réponse générique

contre le terrorisme cybernétique" et un ensemble "spécifique à la motivation", abordant des solutions pour des incidents exemplaires.

La première itération du jeu ne comprenait que deux des cinq principales motivations qui distinguent les groupes terroristes. Une étude plus complète pourrait classer toutes les cinq motivations, leurs points de divergence les plus forts et les croisements potentiels (par exemple, une cible très recherchée par tous les profils de menace).

Les chercheurs notent également l'échantillon localisé des premières utilisations, qui ne peut représenter que le fonctionnement du prototype, mais pas une utilité à long terme pour les hôpitaux. Afin de recueillir davantage de données, il conviendrait de planifier des recherches plus approfondies en recueillant de manière critique les réactions des utilisateurs.

8. Discussion

La cybersécurité pose de plus en plus un défi aux décideurs hospitaliers en raison de la numérisation rapide des soins de santé, des traitements à distance, de la complexité croissante de l'environnement informatique et de l'incertitude dans l'allocation des ressources. La direction doit agir sous pression temporelle, avec un manque de connaissances techniques et d'expertise. Malgré les risques croissants d'attaques cybernétiques, la plupart des hôpitaux adoptent encore principalement des stratégies réactives en matière de cybersécurité. La question demeure de savoir comment l'importance de la préparation aux incidents cybernétiques pourrait être mise en évidence, conduisant à l'investissement des ressources nécessaires dans la préparation aux incidents de sécurité critiques, afin que les hôpitaux soient adéquatement préparés. Les serious games pourraient jouer un rôle indispensable dans ce processus, en fournissant une approche relativement abordable pour sensibiliser les principales parties prenantes et les décideurs. Des études supplémentaires pourraient se concentrer spécifiquement sur la recherche du transfert de compétences lors de micro-jeux et de ses effets sur les décisions futures. Une valeur supplémentaire pourrait être fournie avec une analyse comparative des profils de menace et des stratégies les plus efficaces pour les contrer.

Bibliographie

[AME 24] AMERICAN HOSPITAL ASSOCIATION. « America’s Hospitals and Health Systems Continue to Face Escalating Operational Costs and Economic Pressures as They Care for Patients and Communities », *AHA.org*, 2024. Available at: https://www.aha.org/costsofcaring

[APP 13] APPLEGATE S.D. « The dawn of Kinetic Cyber », *2013 5th International Conference on Cyber Conflict (CYCON 2013)*, Tallinn, Estonia, p. 1-15, 2013.

[ARG 20] ARGAW S. T., TRONCOSO-PASTORIZA J. R., LACEY D., FLORIN M.-V., CALCAVECCHIA F., ANDERSON D., BURLESON W., VOGEL J.-M., O’LEARY C., ESHAYA-CHAUVIN B., FLAHAULT A. « Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks », *BMC Medical Informatics and Decision Making*, n° 20(1), 2020. doi:10.1186/s12911-020-01161-7

[CHE 23] CHEN G, JIN G. « Insights from Evidence-Based Medicine Method for Building Security Systems Against Terrorist Attacks in Hospitals », *Journal of Multidisciplinary Healthcare*, n° 16, p.°4133-4137, 2023. doi:10.2147/JMDH.S426166

[CHU 05] CHUNG S, SHANNON M. « Hospital planning for acts of terrorism and other public health emergencies involving children », *Arch Dis Child.*, n° 90(12), p.°1300-1307, 2005. doi: 10.1136/adc.2004.069617.

[COE 20] COENRAAD M., PELLICONE A., KETELHUT D.J., CUKIER M., PLANE J.D., WEINTROP D. « Experiencing Cybersecurity One Game at a Time: A Systematic Review of Cybersecurity Digital Games », *Simulation & Gaming*, n° 51, p.°586 – 611, 2020.

[CRU 19] CRUZ-GOMES S., AMORIM-LOPES M., ALMADA-LOBO B. « The Demand for Healthcare Services and Resources: Patterns, Trends and Challenges in Healthcare Delivery », In: Alves, M., Almeida, J., Oliveira, J., Pinto, A. (eds) *Operational Research. IO 2018. Proceedings in Mathematics & Statistics*, (278), Springer, Cham, 2019. doi:10.1007/978-3-030-10731-4_7

[DEN 24] BARTEN D., JANSSEN M., DE CAUWER H., KEEREWEER D., TAN E., VAN OSCH F., MORTELMANS L. « Threat awareness and counter-terrorism preparedness of Dutch hospitals: A cross-sectional survey, *International Journal of Disaster Risk Reduction*, (102), 2024, doi:10.1016/j.ijdrr.2024.104311.

[DOW 17] DOWNS R. « FDA: Abbott's pacemakers vulnerable to cyberattack », *UPI.com*, August 31, 2017. Available at: https://www.upi.com/Top_News/US/2017/08/31/FDA-alerts-public-to-recall-of-pacemakers-vulnerable-to-cyberattack/4861504223465/

[ENI 23a] ENISA.EUROPA.EU. « Threat Landscape 2023 », *ENISA.europa.eu*, Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 [Accessed 20 October, 2023]

[ENI 23b] ENISA.EUROPA.EU. « Checking-up on Health: Ransomware Accounts for 54% of Cybersecurity Threats », *ENISA.europa.eu*, July 5, 2023. Available at: https://www.enisa.europa.eu/news/checking-up-on-health-ransomware-accounts-for-54-of-cybersecurity-threats

[EUR 24] EURONEWS.COM. « European hospitals targeted by "pro-Russian" hackers », *Euronews.com*, February 1, 2024. Available at: https://www.euronews.com/2023/02/01/european-hospitals-targeted-by-pro-russian-hackers

[GHA 15] GHANEM M, SCHNOOR J, HEYDE CE, KUWATSCH S, BOHN M, JOSTEN C. « Management strategies in hospitals: scenario planning », *GMS Interdiscip Plast Reconstr Surg DGPW*, Jun 22, n° 4, Doc06, 2015. doi: 10.3205/iprs000065

[GRE 05] GREEN L.V. « Capacity Planning and Management in Hospitals », In: Brandeau, M.L., Sainfort, F., Pierskalla, W.P. (eds) *Operations Research and Health Care. International Series in Operations Research & Management Science*, Vol. 70. Springer, Boston, MA, 2005. doi:10.1007/1-4020-8066-2_2

[HAC 22] HACQUEBORD F., HILT S., SANCHO D. « The Near and Far Future of Ransomware Business Models », *Key4biz.it*, December, 2022. Available at: https://www.key4biz.it/wp-content/uploads/2022/12/wp-the-near-and-far-future-of-ransomware.pdf

[HAM 10] HAMBURG M. A., COLLINS F. S. « The Path to Personalized Medicine », *New England Journal of Medicine*, n° 363(4), p.°301–304, 2010. doi:10.1056/nejmp1006304

[HOP 21] HOPPA M.A. « From Lessons Learned to Improvements Implemented: Some Roles for Gaming in Cybersecurity Risk Management », In: Daimi, K., Peoples, C. (eds) *Advances in Cybersecurity Management*. Springer, Cham, 2021. doi:10.1007/978-3-030-71381-2_14

[JAL 19] JALALI M. S., M., MADNICK S. « Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment », *The Journal of Strategic Information Systems*, n° 28(1), p.°66-82, 2019.

[JAL 18] JALALI M. S., KAISER J. P. « Cybersecurity in Hospitals: A Systematic, Organizational Perspective », *Journal of Medical Internet Research*, n° 20(5), e10059, 2018. doi:10.2196/10059

[KIA 19] KIANPOUR M., ØVERBY H., KOWALSKI S.J., FRANTZ C. « Social Preferences in Decision Making Under Cybersecurity Risks and Uncertainties », In: Moallem, A. (eds) *HCI for Cybersecurity, Privacy and Trust. HCII 2019. Lecture Notes in Computer Science*, (11594). Springer, Cham, 2019. doi:10.1007/978-3-030-22351-9_10

[KRA 21] KRAUS S., SCHIAVONE F., PLUZHNIKOVA A., INVERNIZZI A. C. « Digital transformation in healthcare: Analyzing the current state-of-research », *Journal of Business Research*, n° 123, p.°557–567, 2021.

[SHI 18] SHIN S., LIPTON S. S. « Security researchers say they can hack », *CNBC.com*, August 17, 2018. https://www.cnbc.com/2018/08/17/security-researchers-say-they-can-hack-medtronic-pacemakers.html

[MAN 12] MANSFIELD-DEVINE S. « Estonia: what doesn't kill you makes you stronger », *Network Security*, (7), p.°12–20, 2012. doi:10.1016/s1353-4858(12)70065-x

[MCN 22] MCNEILLY B, JASANI G, CAVALIERE G, ALFALASI R, LAWNER B. « The Rising Threat of Terrorist Attacks Against Hospitals », *Prehosp Disaster Med*. April, n° 37(2), p.°223-229, 2022. doi: 10.1017/S1049023X22000413.

[NAT 23] NATIONAL CYBER SECURITY CENTRE (NCSC). « Ransomware, extortion and the cyber crime ecosystem », *NCSC.gov*. September 11, 2023. Available at: https://www.ncsc.gov.uk/whitepaper/ransomware-extortion-and-the-cyber-crime-ecosystem

[NEP 23] NEPRASH H., MCGLAVE C., NIKPAY S. We tried to quantify how harmful hospital ransomware attacks are for patients. Here's what we found. November 17, 2023. Available at: https://www.statnews.com/2023/11/17/hospital-ransomware-attack-patient-deaths-study/

[NEP 22] NEPRASH H. T., MCGLAVE C. C., CROSS D. A., VIRNIG B. A., PUSKARICH M. A., HULING J. D., ROZENSHTEIN A. Z., NIKPAY S. S. «Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021 », *JAMA Health Forum*, n° 3(12), e224873, 2022. doi:10.1001/jamahealthforum.2022.4873

[OWE 20] OWENS B. « How hospitals can protect themselves from cyber attack », *CMAJ*. January 27, n° 192(4), p.°E101-E102, 2020. doi: 10.1503/cmaj.1095841.

[PAG 20] PAGIANINI P. A. « French Hospital Was Forced To Reschedule Procedures After Cyberattack », *Securityaffairs.com*, April 20, 2020 available at: https://securityaffairs.com/162057/hacking/french-hospital-cyber-attack.html

[PAR 02] PARDALOS P. M. « Cost characteristics of hospitals », *Social Science & Medicine*, n° 55(6), p.°895–906, 2022. doi:10.1016/s0277-9536(01)00237-4

[RAH 21] RAHMADI F., LAVICZA Z., HOUGHTON T. « Defining Microgames in Education Context », *International Journal of Emerging Technologies in Learning (iJET)*, n° 16(22), p°4-16, 2021.

[REE 18] REED T. « Man convicted of "hacktivist" attacks on Boston Children's Hospital », *Fierce Healthcare*, August 3, 2018. Available at: https://www.fiercehealthcare.com/tech/man-convicted-hacktivist-attacks-boston-children-s-hospital

[ROM 17] ROMAGNA M., VAN DEN HOUT N. J. *Hacktivism and Website Defacement: Motivations* », *Capabilities and Potential Threats*, 2017.

[RUN 24] RUNDLE J., STUPP, C. « Hospitals and Pharmacies Reeling After Change Healthcare Cyberattack », *WSJ.com*, February 23, 2024. Available at: https://www.wsj.com/articles/hospitals-urged-to-disconnect-from-unitedhealths-hacked-pharmacy-unit-11c9691e

[SAM 14] SAMONAS S., COSS, D. « The Cia Strikes Back: Redefining Confidentiality, Integrity and Availability in Security », *Proso.com*, 2024. Available at: https://www.proso.com/dl/Samonas.pdf

[SEI 24] SEITZ A. Cyberattacks on hospitals are likely to increase, putting lives at risk, experts warn. Apnews.com, February 14, 2024. Available at: https://apnews.com/article/cyberattacks-hospital-lurie-childrens-ransom-eb6f9528198b4e3c2a5e82f74c4cb7e9

[TEI 23] TEICHMANN F., BOTICIU S., SERGI B. S. « The evolution of ransomware attacks in light of recent cyber threats. How can geopolitical conflicts influence the cyber climate? », *International Cybersecurity Law Review*, n° 4, 2023. doi:10.1365/s43439-023-00095-w

[ULM 22] ULMER N, BARTEN DG, DE CAUWER H, GAAKEER M., KLOKMAN V., VAN DER LUGT M., MORTELMANS L., VAN OSCH F., TAN E., BOIN A. « Terrorist Attacks against Hospitals: World-Wide Trends and Attack Types », *Prehospital and Disaster Medicine*, n° 37(1), p.°25-32, 2022. doi:10.1017/S1049023X22000012

[WAS 22] WASSERMAN L. « Hospital cybersecurity risks and gaps: Review (for the non-cyber professional) Frontiers of Digital », *Health*, 11 Security Health Technology Implementation, (4), 2022.

[WOR 23a] WORLD ECONOMIC FORUM. *Global Cybersecurity Outlook 2024*, World Economic Forum; State of Cybersecurity 2023, ISACA; A Closer Look at the Cyber Talent Gap, Trellix, 2023. Full report: https://initiatives.weforum.org/bridging-the-cyber-skills-gap/home

[WOR 23b] WORLD ECONOMIC FORUM, *Global Health and Healthcare Strategic Outlook: Shaping the Future of Health and Healthcare*. Insight Report, January, 2023. Available at: https://www.weforum.org/publications/global-health-and-healthcare-strategic-outlook-shaping-the-future-of-health-and-healthcare/

[WOR 23c] WORLD HEALTH ORGANIZATION. « Noncommunicable diseases », *Who.int*, September 16, 2023. Available at: https://www.who.int/news-room/fact-sheets/detail/noncommunicable-diseases

[WOR 22] WORLD HEALTH ORGANIZATION. REGIONAL OFFICE FOR EUROPE. *Health and care workforce in Europe: time to act*. World Health Organization. Regional Office for Europe, 2022. Available at: https://iris.who.int/bitstream/handle/10665/362379/9789289058339-eng.pdf?sequence=1

[ZHA 21] ZHANG Z., QIN L. « InterRings: Towards Understanding Design Micro-games to Fit Daily Work Routine », *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, p.°1-6, 2021. Doi:10.1145/3411763.3451733

