J3eA, Journal sur l'enseignement des sciences et technologies de l'information et des systèmes
J3eA 24 (2025) 25
https://doi.org/10.1051/j3ea/20250025
https://www.j3ea.org

Expérimentation d'utilisation du jeu pour la sensibilisation à la cybersécurité : Mille bornes de sécurité

Alexandre Philippot[1]*

[1] Université de Reims Champagne-Ardenne, CReSTIC, Reims, France

*Auteur de correspondance : alexandre.philippot@univ-reims.fr

Résumé : *Dans le contexte de la digitalisation croissante de l'industrie, la cybersécurité est devenue un enjeu majeur pour la protection des infrastructures et des systèmes d'information. Pour répondre à ce défi, il est crucial de former et de sensibiliser les étudiants dès leur parcours académique. Les futurs ingénieurs et techniciens doivent « être équipés » des connaissances et des compétences nécessaires pour gérer les risques cybernétiques. Le papier présente une expérimentation de sensibilisation à la cybersécurité par une stratégie de gamification. L'expérimentation utilise un jeu inspiré de "Mille Bornes" pour sensibiliser les étudiants à la terminologie et aux bonnes pratiques de sécurité. Les résultats de l'expérimentation montrent un intérêt des étudiants pour la gamification, mais soulignent également des points d'amélioration.*

Mots clés : cyberécurité, gamification, retour d'expérience.

Abstract: *In the context of the increasing digitalization of industry, cybersecurity has become a major issue for the protection of infrastructures and information systems. To meet this challenge, it is crucial to train and raise awareness among students from their academic careers. Future engineers and technicians must be equipped with the knowledge and skills necessary to manage cyber risks. This paper presents an experiment to raise awareness of cybersecurity through a gamification strategy. The experiment uses a game inspired by "Mille Bornes" to raise students' awareness of security terminology and best practices. The results of the experiment demonstrate students' interest in gamification but also highlight areas for improvement.*

Keywords: *cybersecurity, gamification, feedback.*

1. Introduction

Dans le contexte actuel de digitalisation croissante des processus industriels, la cybersécurité est devenue un enjeu majeur pour la protection des infrastructures et des systèmes d'information. L'industrie 4.0, caractérisée par l'interconnexion des machines, l'automatisation avancée et l'utilisation intensive des données, a ouvert de nouvelles perspectives pour l'efficacité opérationnelle et l'innovation. Cependant, cette transformation numérique a également exposé les entreprises à des menaces cybernétiques plus complexes et sophistiquées. La cybersécurité industrielle se distingue par la nature spécifique des actifs qu'elle vise à protéger : des systèmes de contrôle industriels (ICS), des réseaux de capteurs, des robots de production, et des chaînes logistiques. Ces systèmes, souvent intégrés dans des environnements critiques tels que l'énergie, les transports, et la santé, nécessitent des mesures de sécurité robustes et adaptées pour prévenir les incidents qui peuvent avoir des conséquences graves, allant de perturbations opérationnelles à des catastrophes environnementales et humaines [1, 2].

Face à ces défis, il est crucial de former et de sensibiliser les étudiants à la cybersécurité industrielle dès leur parcours académique. Les futurs ingénieurs, techniciens doivent être équipés des connaissances et des compétences nécessaires pour comprendre et gérer les risques cybernétiques dans les environnements industriels. Cette sensibilisation précoce permet de développer une culture de la sécurité dès le début de leur carrière, favorisant ainsi l'adoption de pratiques sécuritaires dans les organisations.

Les programmes académiques vont devoir inclure des modules spécifiques sur la cybersécurité industrielle, abordant des sujets tels que :

- Les vulnérabilités spécifiques aux systèmes industriels.
- Les menaces émergentes et les techniques d'attaques.
- Les meilleures pratiques pour la sécurisation des infrastructures critiques.
- L'utilisation de technologies avancées comme l'intelligence artificielle et l'apprentissage automatique pour la détection et la réponse aux attaques.
- Les cadres réglementaires et les normes internationales en matière de cybersécurité.

En outre, des projets pratiques peuvent offrir aux étudiants des expériences concrètes, les aidant à mieux comprendre les enjeux réels de la cybersécurité industrielle. Ces expériences sont essentielles pour développer une vision holistique de la sécurité et pour préparer les étudiants à des rôles de leadership dans la gestion des risques cybernétiques. Oui, mais… comment préparer au mieux ces étudiants à se défendre, sans créer des attaquants (hacker) ? Comment développer des compétences « très » spécifiques sans équipe dédiée ? Et enfin, comment ne pas les « ennuyer » dans un discours de sensibilisation soi-disant connu ?

Ce papier vient présenter une expérimentation de sensibilisation à la cybersécurité à travers l'utilisation de la gamification. L'idée principale étant de débuter un futur module sur le thème de la cybersécurité industrielle en informant les étudiants avant tout sur de la terminologie, du vocabulaire et des bonnes pratiques à mettre en place, tout d'abord au niveau de l'IT (Information Technology) afin d'évoquer le niveau OT (Operational Technology) ultérieurement.

La proposition évoque succinctement le problème de cybersécurité industrielle et de son apprentissage en section 2. La section 3 introduit l'intérêt croissant de la gamification dans l'apprentissage. En section 4, nous présentons l'expérimentation mis en place autour du jeu de « Mille bornes de sécurité ». Une analyse de celle-ci est retournée en section 5 avant de conclure sur la poursuite de cette étude.

2. Etat des lieux de la cybersécurité

2.1. Introduction à la cybersécurité

Dans notre monde de plus en plus connecté, la cybersécurité joue un rôle crucial dans de nombreux secteurs, y compris l'industrie, le gouvernement, la santé, mais aussi l'éducation. Elle regroupe l'ensemble des mesures prises pour protéger les systèmes informatiques, les réseaux, et les données contre les accès non autorisés, les attaques malveillantes, et les dommages physiques. Elle englobe une variété de domaines, tels que la protection des données personnelles, la prévention des intrusions, la gestion des risques, et la réponse aux incidents [1, 2]. La cybersécurité vise à garantir la confidentialité, l'intégrité, et la disponibilité des informations numériques.

Les coûts associés aux cyberattaques, y compris les pertes financières directes, les frais de réparation, et les coûts de récupération, peuvent être considérables. Selon divers rapports, les pertes mondiales liées aux cybercrimes s'élèvent à des milliards de dollars chaque année [3]. En France, selon la CNIL[1], 385 000 cyberattaques ont été recensées en 2022 et le pays est aujourd'hui le 4ème le plus touché au niveau mondial, après les États-Unis, la Chine et l'Allemagne. La protection des utilisateurs et des citoyens contre les menaces cybernétiques est une responsabilité morale. Les organisations doivent veiller à ce que leurs pratiques soient éthiques et respectueuses de la vie privée.

La cybersécurité ne concerne pas seulement les grandes entreprises et les gouvernements. Les individus sont également exposés à des risques, notamment par le biais de la fraude en ligne, du vol d'identité, et des attaques ciblant les appareils personnels. La sensibilisation et la formation sont essentielles pour aider les utilisateurs à adopter des pratiques de sécurité appropriées.

2.2. Histoire de …

Le premier virus informatique identifié, appelé "Creeper", a été créé en 1971 par Bob Thomas. Il se propageait sur le réseau ARPANET, affichant le message "I'm the creeper, catch me if you can!". Plus tard, Ray Tomlinson a développé "Reaper", le premier antivirus, conçu pour supprimer Creeper. Au cours des années 1990, l'usage d'Internet a explosé, entraînant une prolifération des virus informatiques et des Malwares. Des logiciels antivirus comme Norton AntiVirus et McAfee ont commencé à se développer pour répondre à ces menaces.

Mais c'est en juin 2010 avec Stuxnet que le monde industriel a connu un tournant dans l'Histoire de la cybersécurité. Stuxnet était spécifiquement conçu pour cibler les systèmes de contrôle programmable (PLC – Programmable Logic Controller) fabriqués par Siemens, utilisés dans les installations nucléaires iraniennes. Son but était de perturber les centrifugeuses utilisées

[1] https://www.cnil.fr

pour l'enrichissement de l'uranium. Stuxnet a marqué un tournant dans l'histoire de la cybersécurité en montrant comment les cyberarmes pouvaient être utilisées pour causer des dommages physiques à grande échelle.

En 2017, WannaCry, attaque de type Ransomware, a touché des centaines de milliers d'ordinateurs dans plus de 150 pays. Elle a exploité une vulnérabilité dans le système d'exploitation Windows, mettant en évidence l'importance des mises à jour de sécurité.

Chaque année, le nombre d'infractions liées au cyber semble augmenter comme l'illustre la figure 1, issue du « Rapport annuel sur la cybercriminalité 2024 »[2] publié par le Ministère de l'Intérieur et des Outre-Mer. C'est donc primordial de former et d'informer nos étudiants sur ce que sera demain.

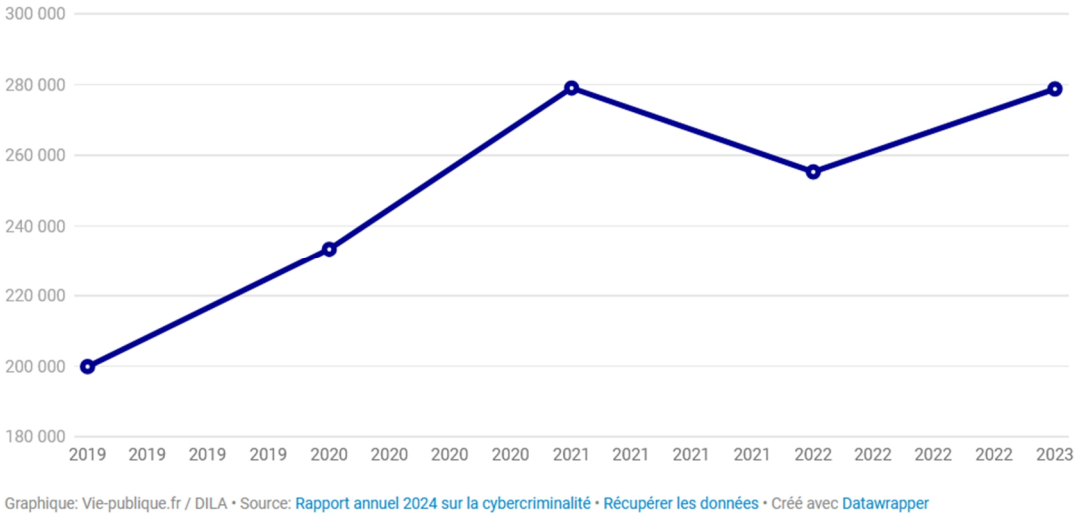

Figure 1. Nombre d'infractions liées au cyber entre 2019 et 2023

2.3. Types de Menaces Cybernétiques

Il est possible de distinguer les menaces selon leur stratégie et leur perturbation [4, 5] provoquée comme suit :

- Malwares (Logiciels Malveillants)
  - Virus : Programmes qui se reproduisent en s'attachant à d'autres programmes ou fichiers. ILOVEYOU en 2000 a infecté des millions de machines via des e-mails.
  - Trojans : Logiciels qui prétendent être légitimes mais contiennent des fonctions malveillantes (vole d'informations financières).
  - Ransomware : Logiciels qui cryptent les données de la victime et demandent une rançon pour les déchiffrer (WannaCry en 2017).
  - Adwares : Programmes qui affichent des publicités indésirables.
  - Spywares : Logiciels qui espionnent les activités de l'utilisateur et collectent des infor-mations.

[2] https://www.interieur.gouv.fr/sites/minint/files/medias/documents/2024-07/30-07-24-Rapport_sur_la_cybercriminalit_2024_-Num%C3%A9rique.pdf

- Phishing et Ingénierie Sociale
    - Phishing : Technique consistant à envoyer des e-mails ou des messages trompeurs pour inciter les utilisateurs à divulguer des informations sensibles.
    - Spear Phishing : Forme ciblée de phishing visant des individus spécifiques au sein d'une organisation (dirigeants d'entreprises).
    - Whaling : Phishing ciblant les hauts dirigeants d'une organisation (PDG pour obtenir des informations financières ou des accès à des systèmes critiques).
- Attaques par Déni de Service (DoS/DDoS)
    - DoS (Denial of Service) : Attaques visant à rendre un service indisponible en submergeant le serveur de requêtes (utilisant des bots).
    - DDoS (Distributed Denial of Service) : Attaques DoS coordonnées à partir de multiples sources, souvent des ordinateurs zombies.
- Attaques par Injection SQL
    - Technique consistant à injecter des commandes SQL malveillantes dans une requête pour accéder ou modifier des bases de données.
- Attaques Zero-Day
    - Attaques exploitant des vulnérabilités inconnues des développeurs et des utilisateurs. Stuxnet (2010) a exploité plusieurs vulnérabilités zéro-jour dans Windows.
- Attaques par Exploits
    - Utilisation de vulnérabilités connues dans des logiciels pour exécuter des codes malveillants.
- Attaques Man-in-the-Middle (MitM)
    - Attaques où l'attaquant intercepte et peut modifier les communications entre deux parties.
- Attaques par Ingénierie Inverse
    - Technique consistant à décompiler ou à analyser un logiciel pour comprendre son fonctionnement et identifier des vulnérabilités (failles de sécurité).
- Attaques par Brute Force
    - Tentatives répétées pour deviner des mots de passe ou des clés de chiffrement.
- Attaques par Cross-Site Scripting (XSS)
    - Injection de scripts malveillants dans des pages Web affichées à d'autres utilisateurs.

Les menaces sont donc nombreuses et diverses, avec une évolution constamment. Comprendre ces différents types de menaces est crucial pour mettre en place des mesures de sécurité efficaces. Les organisations et les individus doivent rester vigilants, appliquer des pratiques de sécurité robustes, et surtout être sensibilisés et informés des nouvelles techniques de protection pour minimiser les risques.

2.4. Apprendre à …

L'apprentissage en cybersécurité industrielle est crucial pour protéger les infrastructures critiques, les systèmes de production. Pour cela, il est nécessaire à nos étudiants d'avoir une connaissance du réseau d'entreprise et de son architecture (pyramide CIM - Computer Integrated Manufacturing), mais aussi une compréhension fine des protocoles industriels (Modbus, Profibus, Profinet …). Nos enseignements sont historiquement tournés vers des modules de programmation d'Automates Programmables Industriels (API), de Supervision industrielle, de Réseau industriel, de base de données, mais presque jamais de Sécurité des

Réseaux. Ce type de module demande d'aborder divers sujets comme la segmentation des réseaux, les protocoles de sécurité, la surveillance et la détection des intrusions, la gestion des risques et vulnérabilités, le contrôle d'accès, la législation et réglementation, les audits, les réponses aux incidents.

Mais avant de voir tout ceci, la sensibilisation et la connaissance d'un minimum de vocabulaire reste la première étape à acquérir. C'est dans ce cadre que la gamification est utilisé dans notre expérimentation.

3. Gamification en Enseignement

La gamification en enseignement consiste à intégrer des éléments de jeu, tels que les points, les badges, les niveaux, les défis, et les récompenses, dans des activités pédagogiques traditionnelles. L'objectif est de stimuler la motivation, l'engagement, et la participation des apprenants, tout en favorisant l'acquisition de connaissances et de compétences. Les travaux de [6] recensent un état de l'art intéressant de l'utilisation de la gamification dans des cursus industriels.

Il est possible de distinguer le type de jeu comme le type de joueur, favorisant ainsi différentes compétences. Ainsi, les jeux coopératifs favorisent la collaboration et le travail d'équipe lorsque les défis et les puzzles stimulent plus souvent la résolution de problèmes et la pensée critique. L'introduction de niveaux et de chemins de progression permettent d'adapter les compétences de chaque apprenant et créent ainsi une expérience personnalisée [7, 8].

Les jeux offrent un feedback immédiat, ce qui aide les apprenants à ajuster leurs stratégies et à progresser.

Des plateformes comme Khan Academy et Duolingo utilisent la gamification avec succès pour encourager l'apprentissage autonome. En classe, des outils comme Classcraft transforment la gestion de classe en un jeu de rôle, améliorant le comportement et la participation [9]. La gamification peut également être appliquée à la formation professionnelle, avec des simulateurs et des jeux de rôle pour développer des compétences pratiques. Pour être efficace, la gamification doit maintenir un équilibre entre le jeu et l'apprentissage, et veiller à l'inclusion et à l'équité. Les enseignants doivent être formés pour intégrer ces éléments de manière pertinente et évaluée. Des études ont montré que la gamification peut améliorer la performance académique et la satisfaction des apprenants [10].

4. Mille Bornes de Sécurité

A l'image du jeu historique « Mille Bornes », le jeu consiste à parcourir le premier 1000 kilomètres de cybersécurité en protégeant votre réseau tout en attaquant les réseaux adverses. Il se joue entre 4 et 6 joueurs et se compose donc d'un ensemble de 105 cartes papiers (Figure 2) à jouer de types :

- Distance (10 km, 25 km, 50 km, 100 km).
- Attaque (Virus, Malware, Phishing, Ransomware, DDoS).
- Défense (Antivirus, Pare-feu, Sauvegarde).
- Réparation (Mise à jour, Chiffrement).

Figure 2. Illustration de quelques cartes du jeu de Mille Bornes de cybersécurité

4.1. Règles du jeu

Après avoir mélangé les cartes, un joueur distribue à tour de rôle 6 cartes à chaque joueur et dispose le reste des cartes en pioche pour tous face cachée. C'est le joueur à droite du distributeur qui débute la partie.

A chaque tour de jeu, un joueur commence par piocher une carte et peut :

- Jouer une carte de distance pour avancer.
- Jouer une carte d'attaque contre un adversaire.
- Jouer une carte de défense pour se protéger.
- Utiliser une carte de réparation pour enlever un handicap.
- Se défausser d'une carte dans la pioche afin de disposer à nouveau de 6 cartes.

Lorsqu'un joueur joue une carte d'attaque, l'adversaire peut répondre avec une carte de défense ou réparation uniquement lorsque c'est son tour. Si l'adversaire n'a pas de défense, il doit subir la conséquence indiquée sur la carte d'attaque.

Lorsqu'un joueur joue une carte de défense ou de réparation, il ne peut pas rejouer aussitôt et doit attendre à nouveau son tour.

Le premier joueur à atteindre au moins 1 000 kilomètres de sécurité gagne.

4.2. Les cartes

Les cartes distances sont de 10 km (x15), 25 km (x15), 50 km (x15) et 100 km (x10). Elles permettent d'avancer classiquement dans le jeu.

Les cartes d'attaque (x5 par type) sont :

- Virus : Fait reculer l'adversaire de 20 km.
- Malware : Fait reculer l'adversaire de 30 km.
- Phishing : Fait perdre à l'adversaire une carte de défense de son choix.
- Ransomware : Fait reculer l'adversaire de 50 km et le rend incapable de jouer des cartes de défense pendant un tour.

- Attaque DDoS : Fait reculer l'adversaire de 40 km et l'empêche de jouer une carte de distance lors de son prochain tour.

Les cartes de défense (x5 par type) sont :

- Antivirus : Annule une attaque de Virus ou Malware.
- Pare-feu : Annule une attaque de Phishing ou DDoS.
- Sauvegarde : Permet de récupérer une carte de distance perdue suite à une attaque.

Enfin, les cartes de réparation (x5 par type) sont :

- Mise à jour : Annule une attaque de Malware ou Ransomware, protégeant ainsi votre réseau.
- Chiffrement : Annule une attaque de Phishing et protège une distance déjà parcourue.

Remarque : Pour un aspect ergonomique et visuel, le jeu de cartes a été à partir d'un site de génération d'images par IA[3].

5. Retour d'Expérimentation

L'expérimentation a été effectuée sur une promotion d'étudiants en 1ère année de Master EEEA Automatique et Robotique de Service de l'Université de Reims Champagne-Ardenne. C'est la première promotion de ce parcours de Master nouvellement accrédité. Cependant, la majorité de l'effectif provient de la licence EEEA de Reims. A noter, il n'y a aucun module officiellement nommé autour de la cybersécurité. C'est donc un créneau ajouter en sus à leur parcours.

Les étudiants ont été prévenus une semaine auparavant de la mise en place d'une expérimentation mais n'en avaient en aucun cas le sujet en information.

La séance s'est déroulée sur un créneau de 2 heures (10h15-12h15), le lundi 27 janvier 2025 dans une salle de TD classique. 14 étudiants (5 filles, 9 garçons) étaient présents sur un effectif officiel de 17. La séance s'est décomposée comme suit :

- Un premier Wooclap (15 minutes) sur la sensibilisation en cybersécurité à travers de 14 questions « basiques » reprises ou adaptées du site de sensibilisation du gouvernement français[4].
- Un diaporama de cours (30 minutes) présentant quelques mots de vocabulaire, un historique d'attaques, les risques, les organismes de certification et de défense, et quelques bonnes pratiques à mettre en place.
- Une phase de jeu (45 minutes).
- Un second Wooclap (15 minutes) de 14 questions davantage expertes.
- Un sondage de retour de séance avec discussion (15 minutes).

[3] https://www.canva.com/
[4] https://www.cybermalveillance.gouv.fr/medias/2020/01/Quizz.pdf

5.1. Observation durant la phase de jeu

Les étudiants se sont répartis d'eux même en 3 groupes éparpillés dans la salle. Les groupes sont composés de :

- GR1 : 1 fille et 4 garçons
- GR2 : 4 garçons
- GR3 : 4 filles et 1 garçon

A noter, pendant la phase de jeu, il n'y a eu aucune interaction entre les groupes. L'observation par l'enseignant se fait également sans intervention volontaire sauf si demandée par un groupe. Avant la distribution du kit de jeu, la question a été posée sur la connaissance des règles du jeu classique « Mille Bornes ». Aucun n'a répondu négativement.

GR1 prend rapidement une feuille de papier pour noter les évolutions kilométriques. En effet, comme il y a des attaques soustrayant des points kilométriques, il ne s'agit pas seulement de faire des additions (comme dans la version classique) mais aussi des soustractions. Bien que ce ne sont que des opérations primaires, cette activité semble leur faire perdre du temps et ne permet pas rapidement aux adversaires de voir l'avancée de chacun.

GR2 se focalise beaucoup sur les règles et cherchent davantage à les comprendre, voir à les affiner. Par exemple, il n'était pas précisé que la défense suite à une attaque était lors du tour du joueur et non pas aussitôt l'attaque subit.

Les cartes à jouer étant en anglais et sans explication détaillée, GR1 et GR3 ne comprennent pas directement l'effet d'une carte Sauvegarde nommée « Backup ».

Au bout de quelques minutes, l'enseignant observe que certains joueurs de GR1 ont plus de 6 cartes dans les mains. Il s'avère que la règle de la défausse n'est pas connu par certain. La pioche finira qu'avec 2 cartes.

Un joueur de GR3 semble perturbé par la diversité des cartes d'attaque et de défense. Dans ce même groupe, beaucoup de discussions ont lieu. Ils se challengent entre eux, se comparent et rient. Au cours du temps, aucun joueur n'a réellement avancé dans ses points kilométriques. Ils sont davantage dans un esprit d'attaque de l'autre que d'avancée de soi.

Les joueurs de GR1 et GR3 se posent mutuellement des questions (chacun dans leur groupe) sur la signification et l'effet du Phishing.

Au bout de 45 minutes, l'enseignant interrompt le jeu afin d'avoir le temps de débriefer. Aucun joueur n'a atteint les 1 000 bornes. Le joueur le plus proche est issu de GR2 avec 850 points kilométriques.

5.2. Retour de séance

Le premier constat de l'enseignant est d'abord sur la « Mise en place du jeu ». En effet, afin de se concentrer sur l'évolution des joueurs, la phase de calcul devrait être remplacée par un plateau d'avancement avec pions. Ainsi, chacun verrait où il en est et surtout où en sont les adversaires rapidement. Le pion évoluant positivement ou négativement selon les attaques. De même, il convient de rappeler et préciser directement sur les cartes les effets des attaques, défenses et réparations.

La question se pose maintenant de savoir si le jeu a été uniquement de l'ordre de l'amusement pour les étudiants ou si un apprentissage ou sensibilisation a été faite durant toute la séance. Le second Wooclap tente de répondre à cette interrogation. Durant ce questionnaire, 1 étudiant n'a pas réussi à se connecter. Sur certaines questions, il n'y a pas eu la totalité des répondants. Il en ressort les informations suivantes.

A la question « Q1 : Qu'est-ce que la cybersécurité ? », 92% des votant ont répondus correctement. Il en est de même pour la question « Q2 : Quel est le but principal d'un pare-feu (firewall) ? ». Aux questions « Q3 : Qu'est-ce qu'un Ransomware ? » et « Q4 : Quelle est la meilleure pratique pour créer un mot de passe fort ? », le score est de 100%.

En revanche, à la question « Q5 : Qu'est-ce qu'une attaque par ingénierie sociale ? », il n'y a que 46 % de bonnes réponses. Ce score parait très faible, notamment pour une génération utilisant massivement les réseaux sociaux. Cependant, il est à noter que ce volet n'était pas présent dans le jeu.

« Q6 : Quelle est la différence entre un antivirus et un antimalware ? » retourne un score de 10 bonnes réponses sur 13 répondants, soit 77%.

La question « Q7 : Qu'est-ce qu'une attaque par déni de service distribué (DDoS) ? » est à 62% de réponses correctes. Après discussion, il s'avère que c'était auparavant un terme inconnu pour la plupart.

58% de bonnes réponses pour la question « Q8 : Qu'est-ce qu'un certificat SSL/TLS ? ». Abordé dans le cours mais pas dans le jeu.

Le terme avait été discuté de nombreuses fois pendant la phase de jeu. A la question « Q9 : Qu'est-ce qu'un phishing ? », 9 réponses sont correctes sur 12 répondants (75%).

100% ont répondu correctement à « Q10 : Quelle est la meilleure pratique pour la mise à jour des systèmes et logiciels ? », et 85% pour la question « Q11 : Qu'est-ce que la segmentation de réseau et pourquoi est-elle importante ? » (dans le cours).

Le score tombe bas à la question « Q12 : Qu'est-ce qu'une attaque par force brute ? » avec uniquement 23% de réponses correctes.

A la question « Q13 : Qu'est-ce que la continuité des activités (Business Continuity) en cybersécurité ? », 85% ont répondu correctement. A savoir, cette information n'était présente nulle part pendant la séance.

Et enfin, à la question « Q14 : Qu'est-ce qu'une attaque par man-in-the-middle (MitM) ? », 11 bonnes réponses sur 13 votants, soit 85%.

L'ensemble des réponses sont positives sauf pour les questions Q5, Q7 et surtout Q12. Q5 et Q7 sont de l'ordre d'un problème de méconnaissance du vocabulaire alors que Q12 davantage technique d'attaque.

Ces 14 questions ciblent l'ensemble du module mais ne permet pas en soit de distinguer l'apport de la gamification. C'est pourquoi, un second sondage a été nécessaire. Sur une graduation comme suit : (i) D'accord, (ii) Plutôt d'accord, (iii) Plutôt pas d'accord et enfin (iv) Pas d'accord, une affirmation d'ordre général « J'ai passé un moment agréable à jouer » a fourni

un score de 100% de « D'accord ». A la phrase « Le jeu m'a apporté un plus », 42% sont plutôt d'accord et 58% d'accord.

A la question « Que faudrait-il améliorer sur ce jeu ? », 17 réponses ont été relevées classées en 3 catégories (cartes, règles et divers) comme sur la figure 3. Sur les cartes, il apparaît important de décrire celle-ci davantage directement sur le support. Sur les règles, idem, elles doivent être plus explicites et deux propositions relèvent de l'objectif final des 1000 points kilométriques : soit diminuer le score final à atteindre, soit augmenter la valeur des cartes. Sur la première, cela impliquerait de changer simplement le nom du jeu. Sur la seconde, en effet, ayant la possibilité de perdre des points, l'avancement peut devenir plus long et fastidieux. Enfin, sur la catégorie divers, 2 n'ont rien à améliorer, 2 proposent d'ajouter une limite de temps au jeu ou d'autres types d'attaques. Nous verrons en conclusion/discussion la proposition d'extensions de cartes. Une réponse concerne le visuel des cartes, 2 propositions semblent hors sujet avec des notions de question/réponse qui n'appartiennent pas aux règles du jeu, et enfin une proposition est faite sur un apport des effets des cartes à chaque tour de jeu. Il faudrait alors avoir un « maître du jeu » au sein du groupe.

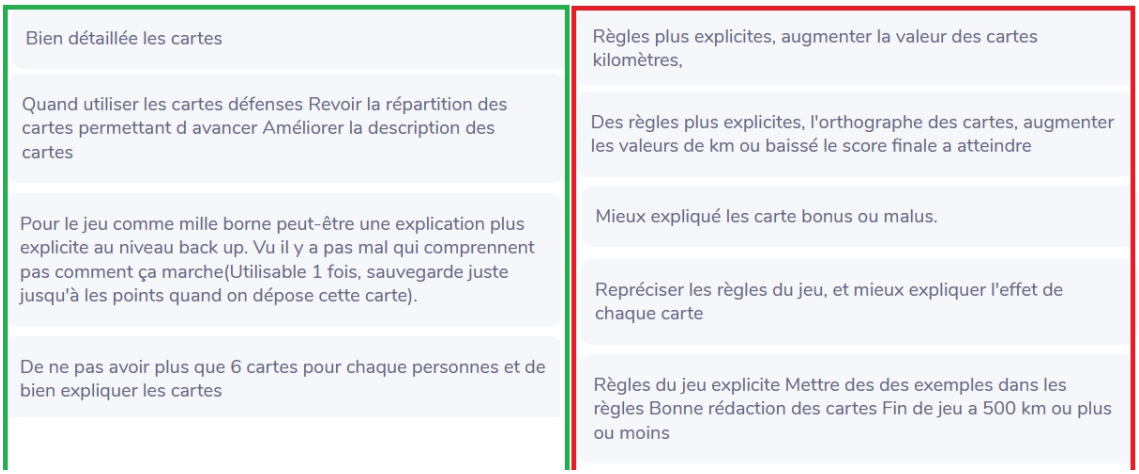

Figure 3. *Extrait des réponses au sondage par catégorie*

Enfin, sur la question « Quel autre jeu serait utile pour illustrer la cybersécurité ? », le nuage de mots en figure 4 (14 répondants) montre très peu de propositions. En effet, 6 semblent « sans idée », puis on y retrouve 2 propositions pour les jeux « Loups garou », « Escape game » et « Among Us », et enfin 1 proposition de « Uno » et « Magic maze ». A noter, « Among Us » semble être un jeu sur application smartphone et non cartes ou plateau. Cependant, tout comme « Loups garou », il y a cette notion « d'inconnu » parmi les joueurs. Ce qui pourrait être pertinent en cas de recherche de « Hacker ».

Figure 4. *Nuage de mots à la question « Quel autre jeu serait utile pour illustrer la cybersécurité ? »*

6. Conclusions et perspectives

Ce papier vient illustrer une première approche de gamification dans l'apprentissage de la cybersécurité. Il cible davantage la sensibilisation et au vocabulaire dans le domaine que la technique et la mise en œuvre. L'expérimentation a montré un intérêt à cette utilisation mais aussi des voix d'amélioration à sa mise en place comme l'introduction d'un plateau de jeu, l'augmentation des cartes de points kilométriques, mais aussi la description plus explicite des effets de chaque carte.

Les retours étudiants, mais aussi de rapporteurs du Colloque de l'Enseignement des Technologies et des Sciences de l'Information et des Systèmes CETSIS 2025[5] où a été présenté le jeu, ont permis de fournir une nouvelle version non expérimentée pour le moment. Cette version ne parle plus de 1000 bornes kilométriques mais de 1000 Go de données à sauver. Un plateau a été réalisé avec un pas d'avancement par case de 25 Go. L'ensemble des cartes a été revu manuellement (sans IA) pour fournir des explicabilités à chacune.

Figure 5. *Evolution du jeu vers le « Mille-Go »*

[5] https://cetsis2025.sciencesconf.org/

Par la suite, il est envisagé d'étendre le jeu de cartes avec une extension de type "événement" qui pourraient introduire des éléments imprévisibles dans le jeu impactant tous les joueurs ou non. Par exemple, :

- Une carte « Panne Réseau » pourrait faire perdre de 10 Go tous les joueurs.
- Une carte « Fuite de Données » pourrait obliger chaque joueur à montrer une carte de leur main. Un joueur révélant une carte d'attaque devrait alors perdre de 20 Go.
- Une carte « Mise à Jour Système » permettrait à chaque joueur de piocher 2 cartes supplémentaires (permettant ainsi de renforcer une défense ou attaquer massivement).
- Une carte « Incident de Sécurité » où tous les joueurs doivent remettre une carte de distance dans la pioche, et les forçant à perdre de 30 Go.
- Une carte « Audit de Sécurité » permettrait au joueur de choisir un adversaire et de regarder sa main et de demander à cet adversaire de se défausser d'une carte d'attaque.

Enfin, le support de jeu « Mille Bornes » est discutable et d'autres types de jeu seraient peut-être plus judicieux afin de favoriser la mise en place de défense de réseaux et non pas à l'incitation d'attaque.

Références

[1] Kevin D. Mitnick. *The Art of Deception: Controlling the Human Element of Security*. Wiley, 2002.
[2] P.W. Singer & Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know.* Oxford University Press, 2014.
[3] S. K. Jha et al. *A Survey on Intrusion Detection Techniques*, Computers & Security, 2019.
[4] A. Gandomi et M. Haider. *Cybersecurity in the Age of Big Data: Challenges and Opportunities*, Journal of Big Data, 2015.
[5] S. Chen et al. *The Role of Artificial Intelligence in Cybersecurity*, IEEE Transactions on Information Forensics and Security, 2020.
[6] K. Tharot. *An Innovative Approach for Teaching Cy-bersecurity in Cyber-Physical Systems*. Thesis, Uni-versité Grenoble Alpes, 2024.
[7] Dicheva, D., Dichev, C., Agre, G., & Angelova, G. (2015). *Gamification in education: a systematic map-ping study*. Educational Technology & Society, 18(3), 75-88.
[8] Zichermann, G., & Cunningham, C. (2011). *Gamification by Design: Implementing Game Mechanics in Web and Mobile Apps*. O'Reilly Media.
[9] Huang, W. H., & Soman, D. (2013). *Gamifying education: what is known, what is not and what is next?* Educational Technology Research and Development, 61(6), 1063-1079.
[10] Hamari, J., Koivisto, J., & Sarsa, H. (2014). *Does gamification work? A literature review of empirical studies on gamification*. 47th Hawaii International Conference on System Sciences (HICSS), 3025-3034.

Biographie de l'auteur

Alexandre Philippot : Après un DEA en Optimisation et Sûreté des Systèmes à l'Université de Reims Champagne-Ardenne en France, Alexandre Philippot a obtenu son doctorat en Diagnostic des Systèmes à événements discrets à l'Université de Reims Champagne-Ardenne en France (URCA). Il a effectué un PostDoc à l'École Normale Supérieure de Cachan (ENS-Cachan) en France (2007) avant d'être en poste de Maître de conférences à l'URCA. Il a défendu son HDR en 2018 et est Professeur des Universités à l'URCA depuis 2023. Thèmes de recherche : Commande, Reconfiguration et Diagnostic des Systèmes à événements discrets.