Formation immersive dans la gestion des crises d'origine cyber : Le cas du projet RESISTECC

José Manuel Castillo, Nicolas Louveton, Parenthoen Marc

Immersive Training in Cyber Crisis Management: The Case of the RESISTECC Project

Formation immersive dans la gestion des crises d'origine cyber : Le cas du projet RESISTECC

JOSÉ MANUEL CASTILLO*
NICOLAS LOUVETON*
*CeRCA CNRS UMR 7295, Université de Poitiers, Université François-Rabelais de Tours, Poitiers, France
MARC PARENTHOEN, Université de Poitiers, Université de Limoges, CNRS, XLIM, Poitiers, France

The "Resilience through Immersive Strategic and Technical Simulation of Cyber Crises" project aims to train staff from small communities and small socio-economic entities in the proper management of cyber crises. To carry this out, a Cyber-Range will be used as an experiential learning setting, which will simulate the learners' working environment as well as their databases and digital work tools. The main objective of this work is to position cognitive ergonomics within the RESISTECC project. This positioning will be based on the evaluation of three variables: immersion, situation awareness and cognitive load. The evaluation of these three variables will be a lever to achieve the instructional objectives of the project, both in the creation of simulation scenarios and in understanding how learners make decisions during stressful situations.

CCS CONCEPTS • Human-centered computing• Human computer interaction (HCI) • Interactive systems and tools

Keywords: Situational Awareness, Cyber-Range, Cognitive Load, Immersion

Le projet « Résilience par la Simulation Immersive Stratégique et Technique de Crises Cyber » vise à former le personnel des petites collectivités et des petites entités socio-économiques à la bonne gestion des crises d'origine cyber. Pour ce faire, un Cyber-Range sera utilisé comme dispositif d'apprentissage expérientiel. Il simulera l'environnement de travail des apprenants ainsi que leurs bases de données et outils numériques de travail. L'objectif principal de ce travail est de positionner l'ergonomie cognitive au sein du projet RESISTECC. Ce positionnement se fera sur la base de l'évaluation de trois variables : l'immersion, la conscience de la situation et la charge cognitive. L'évaluation de ces trois variables constituera un levier pour atteindre les objectifs pédagogiques du projet, tant dans la création de scénarios de simulation que dans la compréhension de la façon dont les apprenants prennent des décisions lors de situations stressantes.

Mots-clés : Conscience de la situation, Cyber Range, Charge Cognitive, Immersion

Reference:
José Manuel Castillo, Nicolas Louveton, and Marc Parenthoen. 2024. Immersive Training in Cyber Crisis Management: The Case of the RESISTECC Project. *IHM'24 : Actes étendus de la 35ème conférence Francophone sur l'Interaction Humain-Machine, March 25–29, 2024, Paris, France.*

1 INTRODUCTION

La crise d'origine cyber se définit par la déstabilisation immédiate et majeure du fonctionnement courant d'une organisation en raison d'une ou de plusieurs actions malveillantes sur ses services et outils numériques [10]. Elles peuvent avoir différents déclencheurs tels que des erreurs humaines ou des actes malveillants par les employés [30,37] ou l'attaque directe menée par des agents externes à l'organisation, qui utilisent souvent l'ingénierie sociale comme stratégie d'intrusion [6,14,17]. À l'heure actuelle, le risque de subir une cyberattaque est élevé. Cela est dû au degré de dépendance des organisations aux technologies numériques, à leur faible niveau de maîtrise des systèmes d'information ou à une pénurie de compétences en cybersécurité face à des acteurs malveillants qui sont de mieux en mieux organisés.

En se concentrant sur les institutions publiques, le rapport sur la menace cyber publié par l'ANSSI [38] montre que les attaques contre les autorités locales se multiplient. Il y a eu 187 incidents cyber affectant les collectivités territoriales entre janvier 2022 et juin 2023. Ces attaques ont eu différents objectifs, allant de la simple déstabilisation au gain économique, en passant par le sabotage ou l'espionnage. Cette augmentation progressive des incidents engendre un besoin de former les travailleurs (informaticiens et autres métiers) des collectivités et des petites entités socio-économiques à la gestion de ce type de crise. Ces formations doivent être pratiques, c'est-à-dire qu'elles doivent mobiliser les compétences des apprenants et permettre l'apprentissage par essai et erreur. Elles doivent également prendre en compte le contexte, les caractéristiques et l'activité de la structure ainsi que les compétences et la manière dont le personnel de la structure répond aux situations stressantes.

Le projet « Résilience par la Simulation Immersive Stratégique et Technique de Crises Cyber (RESISTECC) » répond à ce besoin, par une immersion totale des apprenants dans un environnement qui reproduit le système d'information et qui englobe habituellement leurs différentes fonctions, qu'ils soient des spécialistes de systèmes d'information ou non. Cet article présente les objectifs pédagogiques du projet RESISTECC et décrit les recherches en ergonomie cognitive qui seront menées pour permettre au Cyber-Range d'atteindre ses objectifs.

2 LE PROJET RESISTECC

Les objectifs principaux du projet RESISTECC sont l'établissement d'une plateforme immersive permettant la collaboration des participants, la création d'un ensemble d'exercices adaptés aux collectivités et petites entités socio-économiques et la consolidation d'un catalogue de formation continue en gestion de crises d'origine cyber [28].

Les processus cognitifs mis en jeu par les acteurs de la gestion de crise sont un facteur critique dans la résolution de ces crises. La plateforme de formation immersive proposée a pour but à la fois de réaliser les apprentissages nécessaires mais aussi d'être une plateforme de recherche à part entière portée sur l'étude de l'ergonomie cognitive du Cyber-Range (voir figure 1) en tant qu'outil d'apprentissage. Cette plateforme nous permettra à terme d'étudier différentes composantes de l'immersion et de la prise de décision, les processus de collaboration et d'échange d'information ainsi que l'ergonomie des outils numériques mis à disposition des acteurs de la gestion de crise.

Le Cyber-Range est un outil permettant de répliquer un réseau complet et complexe d'un système d'information qui est généralement utilisé pour la cyberformation [16]. Classiquement, il permet de tester et de développer des compétences en cyber attaque et en cyberdéfense telles que : les capacités d'intrusion, de protection des réseaux et de durcissement des Systèmes d'information, mais également de reconnaître les tactiques, techniques et procédures des attaquants [28]. Ce Cyber-Range sera appuyé par des scénarios détaillant le contexte et la genèse d'une crise d'origine cyber. Pour une formation réussie à l'aide de ce type de dispositif, différents aspects doivent être pris en compte tels que l'établissement des objectifs, la sélection d'une approche (d'attaque ou de défense), l'établissement d'une topologie (les

matériels et logiciels qui seront utilisés), la constitution d'un scénario, l'établissement des règles et la définition de métriques nécessaires pour mesurer l'efficacité de l'exercice [7,33].

Traditionnellement, la formation ayant recours à ce dispositif implique la constitution de deux équipes composées de personnels techniques en cybersécurité : l'équipe rouge qui attaque et simule l'activité des hackers, et l'équipe bleue qui défend et simule le personnel protégeant le système d'information [33]. Néanmoins, dans le cas du Cyber-Range RESISTECC, une équipe supplémentaire sera constituée et composée de personnels non experts en cybersécurité en charge de la prise de décisions, la cellule stratégique. Les opérateurs de cette troisième équipe travailleront simultanément sur des questions telles que la continuité des activités essentielles de la structure, la communication avec les parties prenantes et les médias, pendant que la cellule technique (l'équipe bleue) résoudra les problèmes informatiques liés à l'attaque des pirates.

Ces trois équipes seront finalement accompagnées par une équipe d'orchestrateurs ou d'animateurs. Ces personnes seront externes à la simulation orchestrent le déroulement du scénario notamment en injectant des stimuli (des événements qui font avancer la simulation). Un scénario est donc le déroulement chronologique d'évènements (stimuli) qui se produisent au cours de l'exercice [19]. Ces stimuli peuvent représenter des phénomènes, des défis, des perturbations auxquels les participants doivent faire face lors de la gestion d'une crise. Ils peuvent également être utilisés pour guider les participants vers l'exécution de tâches précises. Les stimuli doivent reproduire une dynamique réelle de crise et correspondre aux objectifs de la formation [19,35]. Les animateurs seront également chargés de réaliser une séance d'évaluation de l'expérience des participants après l'achèvement du scénario. Cette évaluation aura deux objectifs : le premier, de recueillir la perception des participants concernant la qualité du scénario et du Cyber-Range et le deuxième, de donner un feedback aux participants concernant l'atteinte des objectifs d'apprentissage.

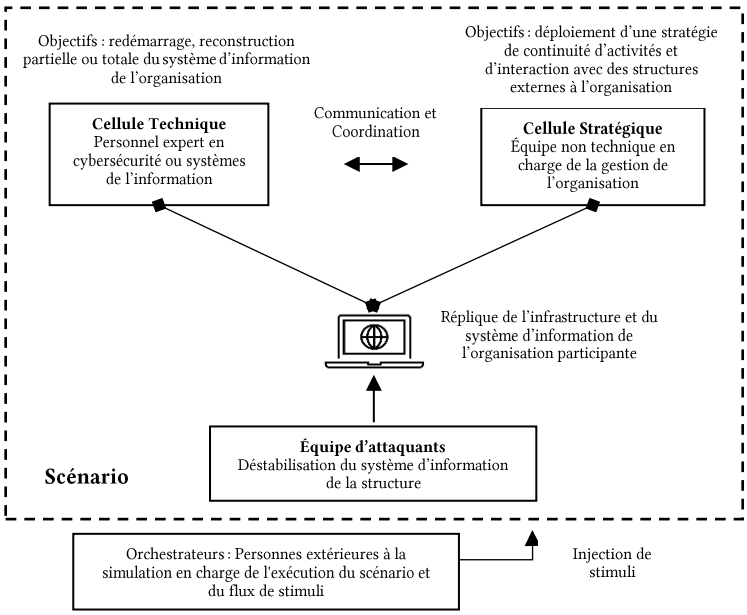

Figure 1 : Représentation du Cyber-Range du Projet RESISTECC.

Comme le présente la Figure 1, la simulation proposée par le Cyber-Range RESISTECC est un système qui tente de reproduire l'interaction des différents éléments dans un contexte complexe. Compte tenu du fait que nous sommes dans

un contexte d'apprentissage immersif, il est nécessaire de procéder à une évaluation globale des éléments qui composent ce dispositif afin d'atteindre une efficacité de l'apprentissage des participants.

Il est considéré que l'application de l'ergonomie cognitive dans la construction des scénarios est un levier pour atteindre les objectifs du projet RESISTECC pour deux raisons : Premièrement, parce que le contenu de la formation se concentre sur la gestion d'une crise, qui d'un point de vue cognitif, se traduit essentiellement par une étape de prise de décision au cours d'une situation complexe. Deuxièmement, parce que l'étude de la manière avec laquelle les participants prennent des décisions sera faite dans des situations artificielles (scénario et injections de stimuli), qu'il faudra contrôler afin d'éviter des éléments non pertinents pouvant interrompre le processus d'immersion des participants.

Différentes variables peuvent être utilisées pour comprendre la prise de décision lors de la gestion d'une crise d'origine cyber, y compris pour la constitution de scénarios de formation pertinents. Ce travail se concentre principalement sur la conscience de la situation de l'opérateur comme déterminante de l'apprentissage. Nous postulons que la conscience de situation est modulée par l'immersion et la charge cognitive. Dans la section suivante, chacune de ces variables sera expliquée et leur choix sera justifié.

3 CADRE THEORIQUE

1.1. L'immersion

La simulation est une technique de pratique et d'apprentissage qui peut être appliquée à de nombreuses disciplines et types d'apprenants différents [18]. Il s'agit d'un enseignement immersif qui consiste en une représentation d'un système ou d'un processus en fonctionnement. Elle désigne une représentation artificielle de processus du monde réel destinée à atteindre des objectifs éducatifs grâce à l'apprentissage expérientiel [15]. D'une part, elle aboutit généralement à une amélioration des connaissances et des compétences ; et d'autre part, les étudiants et les instructeurs expriment des niveaux élevés de satisfaction à l'égard de la simulation en tant que méthode pédagogique [25].

La simulation permet la matérialisation de concepts abstraits et la manipulation de l'objet d'apprentissage qui devient observable et analysable [35]. Elle offre aussi la possibilité d'étudier la relation entre l'affect et l'apprentissage, car les émotions des participants sont inévitablement mobilisées [13].

L'intérêt d'utiliser la simulation pour la formation dans la gestion de crises réside dans le fait que celle-ci permet : une reproduction des dangers potentiels pour l'homme, de l'environnement ou le matériel du système réel, l'opportunité de simplifier ou d'altérer une réalité afin de mieux l'étudier, l'acquisition de compétences liées à la prise de décision et à la résolution de problèmes ou encore la possibilité de simuler des situations graves pour entraîner l'utilisateur à y faire face [35]. Comme évoqué plus haut, le Cyber-Range RESISTECC comprendra une réplique du système d'information de la structure. Cela passera également par la reproduction de ses bases de données et outils numériques, ce qui permettra d'observer comment les salariés réagissent et mobilisent leurs compétences vis-à-vis d'une crise d'origine cyber.

Pour parvenir à cette mobilisation des compétences, il est nécessaire que la simulation génère un état immersif chez les participants. L'immersion est un état psychologique caractérisé par la perception d'être impliqué et en interaction avec son environnement qui fournit un flux continu de stimuli et d'expériences [36]. Une définition plus récente indique que l'immersion serait un état d'implication mentale profonde lors duquel les processus cognitifs de l'individu provoqueraient un changement de son état d'attention, afin qu'il puisse expérimenter une dissociation de la conscience du monde physique[1].

Cet état psychologique peut être le produit, premièrement, d'une réponse perceptive aux stimuli multisensoriels qui entourent la personne ; deuxièmement, d'une réponse au récit ou à la fiction (c'est-à-dire à l'histoire ou aux personnages

qui la composent) ; troisièmement, d'une réponse à un défi qui sollicite les capacités de la personne et enfin, d'une réponse aux propriétés d'un système qui représente un monde virtuel [1,3,26].

Une part importante de l'efficacité de l'apprentissage par simulation est son aspect immersif. Les apprenants doivent se sentir engagé dans l'environnement, la narration et les mécaniques de jeu proposés par le scénario. Le Cyber-Range a la particularité d'être un dispositif immersif hybride, avec des composantes virtuelles (événements orchestrés sur le système d'information, réseaux sociaux, etc.) et des éléments réels comme les locaux, les outils utilisés (téléphone, logiciel) et les relations avec les autres acteurs. Il convient d'analyser comment la nature de ces différentes composantes de la simulation impacte l'immersion et finalement améliorent l'apprentissage.

De cette façon, le scénario et la simulation doivent donc être suffisamment proches de la réalité pour activer l'immersion chez les participants et les injections de stimuli doivent être appropriées pour maintenir cet état tout au long de l'exercice. Cette tâche incombe principalement aux animateurs qui, dans un premier temps, doivent capturer les caractéristiques nécessaires de la structure pour réaliser une scénarisation correcte de la crise et, dans un deuxième temps, doivent injecter des stimuli pour maintenir les participants immergés dans l'exercice.

1.2. La conscience de la situation de l'individu et de l'équipe

La gestion de crise comprend essentiellement la détection des risques, la reconnaissance et l'interprétation du risque pour le contexte immédiat, la communication du risque à plusieurs organisations ou entités, l'auto-organisation et la mobilisation d'un système de réponse collective pour réduire les risques et répondre au danger[8]. Une réponse réussie aux crises repose sur une compréhension approfondie du domaine de travail et de la manière dont les opérateurs perçoivent et traitent les obstacles à la réalisation des objectifs [24].

L'un des prédicteurs mesurables d'une bonne prise de décision dans des environnements complexes est la conscience de la situation de l'individu et de l'équipe [11,20]. La conscience de la situation ou conscience situationnelle (CS) est une variable largement étudiée dans les systèmes critiques tels que le domaine militaire ou nucléaire et actuellement, son étude revêt une importance vitale dans le domaine de la cybersécurité [4,21]. Pour Endsley [11] la CS de l'opérateur est un processus hiérarchisé divisé en trois niveaux : la perception, la compréhension et la projection. Ce modèle se base sur une théorie cognitive utilisant une approche de traitement de l'information. Endsley décrit la CS comme une composante du traitement de l'information qui suit la perception et conduit à la prise de décision et à l'exécution d'actions [31].

Le premier niveau constitue la perception des éléments du contexte, c'est-à-dire l'identification du statut, des attributs et de la dynamique des éléments pertinents du milieu dans lequel se situe l'opérateur. Le deuxième niveau est la compréhension (ou l'interprétation) de la situation. Celle-ci est basée sur une synthèse et/ou un regroupement d'éléments perçus lors de la première étape. En d'autres termes, il s'agit de comprendre la signification de ces informations soit sous une forme « intégrée », soit sous la forme d'une image (holistique) ou de modèles permettant d'extraire une description de l'état actuel de la situation ou du système. Bien entendu, ce sous-processus serait conditionné par les objectifs et par le niveau d'expérience de l'opérateur.

Le troisième niveau correspond à la projection (ou à la prévision) de l'état futur du système. Il s'agit de de la dernière étape de la conscience de la situation et du niveau le plus élevé, atteint à partir de la connaissance des éléments et du statut du système. Ce troisième niveau déterminera le cours des actions que l'opérateur doit suivre pour atteindre ses objectifs.

Endsley [11] indique que l'attention et la mémoire de travail de l'opérateur sont des facteurs critiques qui limitent l'acquisition et l'interprétation des informations de son environnement, ce qui crée des difficultés pour établir une conscience de la situation. Compte tenu de ce point, le stress, la charge de travail, la complexité, la conception des

systèmes et des interfaces sont des éléments de contexte qui peuvent avoir un effet délétère sur la conscience de la situation des opérateurs, dans la mesure où ils influenceraient l'attention et la mémoire de travail. Ce dernier point est particulièrement important étant donné que dans les situations de crise, le processus de décision est complexe ; en effet, les décideurs sont exposés à des niveaux de stress élevés (décisions très difficiles, pression hiérarchique ou médiatique, etc.), ainsi qu'à différents préjugés qui peuvent avoir un impact sur les individus, leurs représentations et leurs décisions, entre autres [32].

Concernant la Conscience de la situation de l'Équipe (CSE), elle est définie comme le degré de conscience de la situation de chaque membre de l'équipe au regard de ses responsabilités individuelles [11,12]. La CSE comprend la conscience de la situation de chaque membre de l'équipe ainsi que la conscience de la situation partagée, appelée « l'image commune » [31]. Selon cette vision, les membres d'une équipe prennent conscience de différents aspects de la situation et rassemblent les pièces du puzzle par la communication ou d'autres interactions pour prendre les mesures appropriées [2].

1.3. La Théorie de la charge cognitive

La théorie de la charge cognitive (TCC) est un cadre permettant d'optimiser l'apprentissage complexe. Elle s'appuie sur des modèles d'architecture cognitive humaine et de traitement de l'information [23]. La littérature nous apprend que ce modèle théorique est utile pour l'évaluation de scénarios de simulation dans des situations complexes comme celles du secteur médical. L'application de cette théorie favorise la conception de scénarios permettant l'acquisition de connaissances, de compétences ou d'aptitudes complexes, sans surcharger la capacité de l'apprenant à intégrer de nouveaux matériaux, c'est-à-dire en respectant les limitations de la mémoire de travail [22].

L'idée indiquée par Meguerdichian [22] est parfaitement transposable à la prise de décision en situation de crise, dans la mesure où l'attention et la mémoire de travail sont des facteurs critiques pouvant impacter le développement de la conscience de la situation par l'opérateur [11]. Cela est prévisible étant donné que tous les opérateurs humains ont une capacité limitée de réception et de traitement de l'information [39].

L'origine de la TCC s'inscrit dans le cadre de la psychologie cognitive et de l'apprentissage[34]. Selon cette théorie, la charge cognitive est décomposable en trois sous-types : la charge cognitive intrinsèque, laquelle est liée au contenu et à la difficulté des matériaux à apprendre ; la charge cognitive extrinsèque, liée au mode de présentation de l'information, et la charge cognitive essentielle qui représente les ressources mobilisées pour la construction des schémas. Le principe derrière ce modèle est que dans les situations d'apprentissage, les éducateurs devraient viser à : (a) gérer la charge cognitive intrinsèque, c'est-à-dire que ce type de charge doit être adapté au niveau de l'apprenant ; (b) minimiser la charge externe, c'est-à-dire qu'il s'agit d'éviter les aspects non essentiels de la tâche d'apprentissage, et (c) stimuler la charge mentale essentielle ou pertinente pour la génération de l'apprentissage [13,23].

En d'autres termes, la TCC en situation de simulation permet de catégoriser ce qui est pertinent et ce qui ne l'est pas pour l'apprentissage et, par un processus itératif, d'améliorer la qualité des simulations en mesurant les performances des participants. Cependant, pour atteindre cet objectif, il s'agit de prendre en considération deux conditions : La première est que le scénario à simuler sera une situation stressante pour les participants, c'est-à-dire que le stress fera partie du scénario sous la forme de stimuli afin de reproduire un état émotionnel d'alerte chez les participants. Cependant, le stress contribue à une charge cognitive externe, dont l'excès altère la fonction de la mémoire de travail, augmentant le risque de surcharge cognitive et de résultats d'apprentissage moins bons. En d'autres termes, un excès d'émotion produit par le stress peut provoquer une saturation chez l'apprenant qui aura un effet néfaste sur son

apprentissage [5,13,22]. Ainsi, nous postulons qu'une charge émotionnelle élevée aura un impact négatif sur l'apprentissage lors de l'exécution des exercices de cybersécurité.

La seconde est que la scénarisation doit être bien conçue, c'est-à-dire qu'un examen minutieux de la manière dont elle est structurée, présentée et conçue doit être effectué. Ceci afin d'éviter que les apprenants allouent des ressources attentionnelles à des éléments étrangers ou externes à la simulation, ce qui pourrait réduire leur immersion dans l'exercice. Des exemples en sont la mauvaise qualité des matériaux, des objectifs non définis ou irréalistes, etc. Ainsi, nous pensons qu'une mauvaise conception de l'exercice de simulation d'un exercice de gestion de crise cyber aura un impact négatif sur le processus d'immersion des participants, ce qui compromettra leur apprentissage.

4 METHOLOGIE ENVISAGEE

Les hypothèses de recherche sont les suivantes : l'injection de stimuli (événements réalistes, mais fictifs liés à la simulation) augmente l'immersion des participants et par conséquent le traitement cognitif de la situation, ce qui engendre une meilleure conscience de la situation ainsi qu'un meilleur apprentissage. Toutefois, l'injection de stimuli augmente également la charge cognitive externe, ce qui va limiter la capacité de traitement de la situation et générer une dégradation de la conscience de la situation et de l'apprentissage. De cette manière, il y a un optimum à trouver entre le nombre et le type de stimuli injectés et la performance du simulateur en termes d'apprentissage.

Pour évaluer l'immersion des participants, il est envisagé d'utiliser des méthodes subjectives telles que l'application de questionnaires psychométriques et le développement d'entretiens structurés avec les participants une fois l'exercice de simulation terminé. L'application de ces deux méthodes sera réalisée lors de l'étape du retour d'expérience.

Une méthodologie d'évaluation subjective est également envisagée pour explorer la charge cognitive des participants ; cependant, il est prévu de lier cette évaluation subjective à celle de la performance des participants. Pour ce faire, il est envisagé d'observer le comportement de ceux-ci lors de l'injection des stimuli à l'aide d'une grille d'observation, laquelle portera sur l'évaluation du temps de réaction des participants aux stimuli, des comportements adoptés, des décisions prises en fonction de la complexité des stimuli, de l'accomplissement des objectifs et de la frustration, entre autres.

Concernant la méthode pour évaluer la conscience de la situation, il est prévu d'utiliser l'analyse cognitive des tâches (ACT). Des travaux antérieurs montrent qu'il s'agit d'une technique pertinente pour étudier cette variable dans le contexte de la cybersécurité [9,21,29]. L'ACT constitue une méthode d'analyse de nature qualitative permettant, d'une part, de caractériser l'activité cognitive qui sous-tend la performance d'un individu ou d'un groupe d'individus face à une tâche donnée, et d'autre part, de caractériser la tâche elle-même [27]. Pour réaliser l'analyse cognitive des tâches, nous observerons comment et sur quelle base les participants prendront leurs décisions. Il sera également prévu d'évaluer les verbalisations émises lors du déroulement de l'exercice. Compte tenu du fait que l'exercice de crise sera enregistré en vidéo, un entretien d'auto-confrontation sera également proposé aux participants pour explorer la conscience de la situation, c'est-à-dire que nous montrerons les parties de la vidéo où ils ont pris des décisions et nous leur demanderons de verbaliser leur ressenti, ainsi que de préciser la « raison » qui les a motivés à entreprendre cette action précise.

2.1. Travail en cours

Des études préliminaires sur le terrain ont déjà commencé. Elles ont pour objectif d'identifier les éléments organisationnels des collectivités, ainsi que des petites et moyennes entreprises, dont la structure doit être répliquée lors de la simulation d'un exercice de cybersécurité. Ceci, afin d'assurer une proximité avec la réalité du terrain, ainsi qu'une

immersion des futurs participants. Pour ce faire, une grille d'entretien est utilisée pour recueillir les informations concernant les deux aspects suivants : (a) l'activité de la structure en question (organisation, activités essentielles ou critiques, adhérence des activités critiques à l'informatique, entre autres) et (b) l'expérience de celle-ci dans la gestion et l'élaboration d'une réponse collective aux situations de crises (expérience dans la gestion de crises, les moyens de communications privilégiés pendant cette étape, l'engagement de la gouvernance, etc.).

5 CONCLUSION ET PERSPECTIVES

Le projet RESISTECC a été créé en réponse au besoin de former le personnel des petites collectivités et des petites entités socio-économiques à la gestion des cyber-crises. Ce projet utilisera un Cyber-Range comme dispositif de simulation, qui servira à former les personnels techniques et non techniques de ces structures. L'apport de l'ergonomie cognitive se fera à travers l'étude de trois variables : l'immersion, la conscience de la situation et la charge cognitive. L'étude de ces variables permettra d'élaborer des scénarios de formation efficaces et améliorera la compréhension de la manière avec laquelle les participants prennent des décisions et apprennent lors d'une situation stressante.

Les aspects à considérer pour le bon déroulement des formations sont, d'une part, le matériel : le cyber-range doit répliquer efficacement le système d'information de la structure afin de reproduire l'environnement de travail réel des participants. Les scénarios doivent être plausibles et adaptés au contexte des structures et la gestion des stimuli doit être optimale pour ne pas surcharger les participants et ne pas influencer leur apprentissage. D 'autre part, il faut considérer la motivation et la disponibilité des participants. Sachant que la formation durera entre 2 et 4 heures, il est nécessaire que les participants maintiennent leur attention sur l'exercice et ne soient pas interrompus par des appels externes professionnels.

Les aspects méthodologiques à considérer sont : l'ordre d'évaluation des différentes variables évoquées et leur opérationnalisation correcte, ceci afin d'éviter des inconvénients ou interprétations erronées lors de leur mesure. Pour le premier point, il est nécessaire de créer un plan d'évaluation allant de pair avec le calendrier et les objectifs de la formation. Pour le deuxième point, il est nécessaire de disposer d'une base de comportements et d'indicateurs permettant de discriminer les variables psychologiques évoquées ci-dessus. Il est également nécessaire de disposer d'instruments de mesure standardisés et adaptés à la population française.

REFERENCES

[1] Sarvesh Agrawal, Adèle Simon, SØren Bech, Klaus BÆrentsen, and SØren Forchhammer. 2020. Defining immersion: Literature review and implications for research on audiovisual experiences. AES: J. Audio Eng. Soc. 68, (July 2020) 404–417. https://doi.org/10.17743/jaes.2020.0039

[2] Nancy Cooke, Michael Champion, Prashanth Rajivan, Shree Jariwala. 2013. Cyber situation awareness and teamwork. European union digital library (May 2013), 1-6. http://dx.doi.org/10.4108/trans.sesa.01-06.2013.e5

[3] Dominic Arsenault. 2005. Dark waters: spotlight on immersion. In Proceedings of the GAMEON-NA International Conference. Montreal, Quebec, 50-52. https://doi.org/1866/13052

[4] Paul Barford, Marc Dacier, Thomas Dietterich, Matt Fredrikson, Jon Giffin, Sushil Jajodia, Somesh Jha, Jason Li, Peng Liu, Peng Ning, Xinming Ou, Dawn Song, Laura Strater, Vipin Swarup, George Tadda, Cliff Wang, and John Yen. 2010. Cyber SA: Situational Awareness for Cyber Defense. 3-13. In Sushil Jajodia, Peng Liu, Vipin Swarup, Cliff Wang. (eds) Cyber Situational Awareness. Advances in Information Security, vol 46. Springer, Boston, MA. https://doi.org/10.1007/978-1-4419-0140-8_1

[5] Choon Looi Bong, Kristin Fraser, and Denis Oriot. 2016. Cognitive Load and Stress in Simulation. 3–17. In Vincent Grant, Adam Cheng (eds) Comprehensive Healthcare Simulation: Pediatrics. Comprehensive Healthcare Simulation. Springer, Cham, Switzerland. https://doi.org/10.1007/978-3-319-24187-6_1

[6] Brian M Bowen, Ramaswamy Devarajan, and Salvatore Stolfo. 2011. Measuring the Human Factor of Cyber Security. In Proceedings of the IEEE International Conference on Technologies for Homeland Security (HST). IEEE, Waltham, MA, 230-235. https://doi.org/10.1109/THS.2011.6107876

[7] Victor-Valeriu Patriciu and Adrian Constantin Furtuna. 2009. Guide for designing cyber security exercises. In Proceedings of the 8th WSEAS International Conference on E-Activities and information security and privacy (E-ACTIVITIES'09/ISP'09). World Scientific and Engineering

Academy and Society (WSEAS), Stevens Point, Wisconsin, USA, 172–177.

[8] Louise K. Comfort. 2007. Crisis management in hindsight: Cognition, communication, coordination, and control. Public Adm Rev 67, SUPPL. 1 (December 2007), 189–197. https://doi.org/10.1111/j.1540-6210.2007.00827.x

[9] Anita D'Amico, Kirsten Whitley, Daniel Tesone, Brianne O'brien, and Emilie Roth. Achieving cyber defense situational awareness: a cognitive task analysis of information assurance analysts. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 49(3), 229-233. https://doi.org/10.1177/154193120504900304

[10] L'Agence nationale de la sécurité des systèmes d'information (ANSSI). 2021. Anticiper et gérer sa communication de crise cyber. Retrieved January 22, 2024 from https://cyber.gouv.fr/publications/anticiper-et-gerer-sa-communication-de-crise-cyber

[11] Mica Endsley 1995. Toward a theory of situation awareness in dynamic systems. Hum. Fact. 37, 32–64. https://doi.org/10.1518/001872095779049543

[12] Mica Endsley and William Jones. 2001. A model of inter- and intrateam situation awareness: implications for design, training and measurement. In Michael McNeese, Eduardo Salas, Mica Endsley (eds). New trends in cooperative activities: Understanding system dynamics in complex environments. 1-24. Santa Monica, CA

[13] Kristin L. Fraser, Paul Ayres, and John Sweller. 2015. Cognitive load theory for the design of medical simulations. Simulation in Healthcare 10, (October 2015) 295–307. https://doi.org/10.1097/SIH.0000000000000097

[14] Ibrahim Ghafir, Jibran Saleem, Mohammad Hammoudeh, Hanan Faour, Vaclav Prenosil, Sardar Jaf, Sohail Jabbar, and Thar Baker. 2018. Security threats to critical infrastructure: the human factor. J. Supercomp. 74, 10 (October 2018), 4986–5002. https://doi.org/10.1007/s11227-018-2337-2

[15] Jari Hautamaki, Mika Karjalainen, Paivi Hakkinen, and Timo Hamalainen. 2019. Cyber security exercise – literature review to pedagogical methodology. In Proceedings of 13th International Technology, Education and Development Conference (INTED). IATED, 3893–3898. https://doi.org/10.21125/inted.2019.0985

[16] Thibault Debatty, Wim Mess. 2019. Building a Cyber Range for training CyberDefense Situation Awareness. In proceedings of the IEEE International Conference on Military Communications and Information Systems (ICMCIS). IEEE, Budva, Montenegro, 1-6. https://doi.org/10.1109/ICMCIS.2019.8842802

[17] Esmeralda Kadena and Marsidi Gupi. 2021. Human Factors in Cybersecurity. Security. Sci. J. 2, 2 (December 2021), 51–64. https://doi.org/10.37458/ssj.2.2.3

[18] Fatimah Lateef. 2010. Simulation-based learning: Just like the real thing. J. Emerg. Tr. (October 2010). 348–352. https://doi.org/10.4103/0974-2700.70743

[19] Philippe Limousin. 2017. Contribution à la scénarisation pédagogique d'exercices de crise. PhD Thesis, l'Ecole des Mines de Saint-Etienne, Université de Lyon.

[20] Chanel Macabante, Sherry Wei, and David Schuster. 2019. Elements of Cyber-Cognitive Situation Awareness in Organizations. Proceedings of the Human Factors and Ergonomics Society Annual Meeting 63, 1 (November 2019), 1624–1628. https://doi.org/10.1177/1071181319631483

[21] Samuel Mahoney, Emilie Roth, Kristin Steinke, Jonathan Pfautz, Curt Wu, and Mike Farry. 2010. A Cognitive Task Analysis for Cyber Situational Awareness. Proceedings of the Human Factors and Ergonomics Society Annual Meeting 54, 4 (September 2010), 279–283. https://doi.org/10.1177/154193121005400403

[22] Michael Meguerdichian, Katie Walker, and Komal Bajaj. 2016. Working memory is limited: improving knowledge transfer by optimizing simulation through cognitive load theory. BMJ Simul. Tech. Enh Learn. 2 (July 2016), 131–138. https://doi.org/10.1136/bmjstel-2015-000098

[23] Laura M. Naismith, Jeffrey J.H. Cheung, Matthew Sibbald, Walter Tavares, Rodrigo B. Cavalcanti, Faizal A. Haji, and Kristin L. Fraser. 2019. Using cognitive load theory to optimize simulation design. In Chiniara Gilles (Ed.). 2019. Clinical Simulation (2nd ed.). 129–141. Academic Pres. https://doi.org/10.1016/B978-0-12-815657-5.00010-3

[24] Christopher Nemeth, Robert L. Wears, Sachin Patel, Greg Rosen, and Richard Cook. 2011. Resilience is not control: Healthcare, crisis management, and ICT. Cog. Tech. Work. 13, 3 (September 2011), 189–202. https://doi.org/10.1007/s10111-011-0174-7

[25] Debra Nestel, Jeffrey Groom, Sissel Eikeland-Husebø, and John M. O'Donnell. 2011. Simulation for learning and teaching procedural skills: The state of the science. Simulation in Healthcare 6, 7 SUPPL. (August 2011). https://doi.org/10.1097/SIH.0b013e318227ce96

[26] Niels Christian Nilsson, Rolf Nordahl, and Stefania Serafin. 2016. Immersion revisited: A review of existing definitions of immersion and their relation to different theories of presence. Hum. Tech. 12, 2 (November 2016), 108–134. https://doi.org/10.17011/ht/urn.201611174652

[27] Yenny Otálora. 2019. Cognitive task analysis as a methodological strategy for understanding and explaining human cognition. Univ. Psycho. 18, 3 (January 2019), 1–12. https://doi.org/10.11144/Javeriana.upsy18-3.acte

[28] Marc Parenthoen. 2023. RéSISTeCC : Résilience par Simulation Immersive Stratégique et Technique de Crise Cyber. In Proceedings of the conference "Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI 2023)". Neuvy-sur-Barangeon, France, 1-4.

[29] Celeste Lyn Paul and Kirsten Whitley. 2013. A Taxonomy of Cyber Awareness Questions for the User-Centered Design of Cyber Situation Awareness. In Louis Marinos and Ioannis Askoxylakis (eds) Human Aspects of Information Security, Privacy, and Trust (HAS 2013). Lecture Notes in Computer Science, vol 8030. Springer, Berlin, Heidelberg. 145–154. https://doi.org/10.1007/978-3-642-39345-7_16

[30] Alessandro Pollini, Tiziana C. Callari, Alessandra Tedeschi, Daniele Ruscio, Luca Save, Franco Chiarugi, and Davide Guerri. 2022. Leveraging human factors in cybersecurity: an integrated methodological approach. Cog. Tech. Work. 24, 2 (May 2022), 371–390. https://doi.org/10.1007/s10111-021-00683-y

[31] Paul M. Salmon, Neville A. Stanton, Guy H. Walker, Chris Baber, Daniel P. Jenkins, Richard McMaster, and Mark S. Young. 2008. What really is going on? Review of situation awareness models for individuals and teams. Theory. Issues Erg. Sci. 9, 4 (May 2008), 297–323. https://doi.org/10.1080/14639220701561775

[32] Sophie Sauvagnargues, Dimitri Lapierre, Philippe Limousin, Noémie Frealle, Florian Tena-Chollet, Pierre-Alain Ayral, Aurélia Bony-Dandrieux, and Jérôme Tixier. 2018. Tools and Methods for Crisis Management Training. In Sophie Sauvagnargues (eds). Decision making in Crisis Situations: Research and Innovation for Optimal Training. 1–33. https://doi.org/10.1002/9781119557869

[33] Ensar Seker, Hassan Ozbenli. 2018. The Concept of Cyber Defence Exercises (CDX): Planning, Execution, Evaluation. In Proceedings of the IEEE International Conference on Cyber Security and Protection of Digital Services (Cyber Security). IEEE, Glasgow, UK, 1-9. https://doi.org/10.1109/CyberSecPODS.2018.8560673

[34] John Sweller, Jeroen J.G. Van Merrienboer, and Fred G.W.C. Paas. 1998. Cognitive Architecture and Instructional Design. Educ. Psychol. Rev. 10, 3 (September 1998), 251–296. https://doi.org/10.1023/A:1022193728205

[35] Florian Tena-Chollet. 2012. Elaboration d'un environnement semi-virtuel de formation à la gestion stratégique de crise, basé sur la simulation multi-agents. PhD Thesis. Ecole Nationale Supérieure des Mines de Saint-Etienne

[36] Bob G Witmer and Michael J Singer. 1998. Measuring Presence in Virtual Environments: A Presence Questionnaire. Presence: Teleoperators and Virtual Environments 7, 5 (June 1998), 225-240. https://doi.org/10.1162/105474698565686

[37] Heather Young, Tony van Vliet, Josine van de Ven, Steven Jol, and Carlijn Broekman. 2018. Understanding human factors in cyber security as a dynamic system. In Proceedings of the International Conference on Applied Human Factors and Ergonomics (AHFE). Los Angeles, CA, 244–254. https://doi.org/10.1007/978-3-319-60585-2_23

[38] L'Agence nationale de la sécurité des systèmes d'information. 2023. Synthèse de la menace ciblant les collectivités territoriales. Retrieved January 22, 2024 from https://www.cert.ssi.gouv.fr/cti/CERTFR-2023-CTI-008/

[39] Colonel Robert O'Donnell, Thomas Eggemeier. 1986. Workload assessment methodology. In K. R. Boff, L. Kaufman and J. P. Thomas (Eds.), Handbook of perception and human performance, Vol. 2. Cognitive processes and performance. 1–49. John Wiley & Sons.