RéSISTeCC : Résilience par Simulation Immersive Stratégique et Technique de Crise Cyber

Marc PARENTHOËN, *Université de Poitiers, XLim, UMR CNRS 7252*

***Abstract*—Le projet de Résilience par la Simulation Immersive Stratégique et Technique de Crises Cyber (RéSISTeCC) adresse la formation continue de tous les métiers aux bons réflexes dans la gestion des crises d'origine cyber par une immersion des apprenants dans un environnement reproduisant par simulation le système d'information qui supporte habituellement leurs différents métiers, qu'ils soient non-informaticiens ou informaticiens. Les principaux verrous sont la complexité des interactions au sein d'une cellule de crise tout comme entre plusieurs cellules de crise, et l'automatisation de la spécification des exercices de formation aux bons réflexes pour différents métiers afin de proposer des exercices stimulant la motivation des équipes et améliorant le transfert d'apprentissage du monde virtuel au monde réel.**

Cet article se contente d'exposer l'intention de ce projet interdisciplinaire qui démarre à peine.

***Index Terms*—premiers secours cyber, cyber range, gestion de crise, pédagogie immersive, cyber résilience.**

I. Introduction

Le projet RéSISTeCC a comme objectifs pédagogiques de préparer les organisations à mettre en œuvre une réponse rapide et efficace lorsqu'une cyberattaque surviendra, et de les engager à construire des plans de continuité d'activité efficients qui auront été testés avec tous les maillons de la chaîne : pilotage stratégique, activation de procédures en mode dégradé, réponse informatique à l'incident et criminalistique numérique, gestion de l'impact médiatique.

L'ambition scientifique est l'étude des interactions dans une cellule de crise entre les aspects stratégiques et les aspects informatiques de la gestion de la crise, avec une montée en complexité dans les interactions entre les différentes entités impliquées dans la gestion de la crise : d'un acteur isolé victime d'une cyberattaque à tout un bassin d'activité, qu'il soit sectoriel ou géographique. Parallèlement à ce double verrou de la complexité intra et inter cellules de crise, sera étudiée la paramétrisation des exercices pour les adapter facilement et à moindre coût à différents contextes métiers, à des architectures informatiques particulières, et à des niveaux de maturité hétérogènes, en spécifiant des modèles génériques d'apprentissage aux bons réflexes cyber à toutes sortes de métiers par la collaboration de chercheurs en informatique, en cindynique et en psychologie.

Techniquement, nos entraînements collaboratifs en immersion vont utiliser une plateforme de type *cyber range* pour simuler l'environnement, qu'il va falloir augmenter des concepts, méthodes et outils associés à la production d'exercices de gestion de crise à destination des non informaticiens, avec des scénarios dépendant de la maturité cyber des organisations et des apprenants.

Plan d'Investissement dans les Compétences, Plan de transformation et de digitalisation de la formation, Dispositifs France Formation Innovante NUMérique (PIC DEFFINUM)

II. Etat de l'art pour la formation à la gestion des crises cyber

L'état de l'art sur les dispositifs immersifs ou numériques de formation à la gestion des crises cyber reflète la scission technique/stratégique et s'adressent principalement à des entités avec un minimum de maturité cyber. Côté technique, on trouve les cyber range immergeant les apprenants au sein d'un système d'information réaliste, et côté stratégique on trouve des exercices grandeur nature ou des jeux sérieux avec des aides technologiques pour l'observation des apprenants par les animateurs de l'exercice afin d'alimenter la phase de débrief. Il existe également un ensemble de bonnes pratiques sous la formes de normes, de revues annuelles ou de guides dont certains adressent les petites entités socio-économiques. Nous terminerons cette section par l'initiative ROOM#42 du Cybersecurity Competence Center (C3) au Luxembourg qui place l'humain au centre de la crise.

A. Formations techniques en cyber range

Les cyber range [1], [2] sont des plateformes de simulations dans lesquelles les équipes opérationnelles peuvent s'entraîner et améliorer leur capacité de réaction en cas de crise cyber, par le biais d'une réplication des systèmes informatifs d'une organisation. Cet outil permet de tester et de développer des compétences telles que : les capacités d'intrusion, de protection des réseaux et de durcissement des SI, mais également de reconnaître les TTPs (Terrorist tactics, Techniques, and Procedures).

Les cyber range existent depuis 2002 et ont fait leurs preuves pour former les soldats de la cyberdéfense ; aujourd'hui, tous les gros centres de réponse aux incidents de sécurité (C-SIRT) ont leur propre cyber Range pour former continûment les analystes et ingénieurs à réagir efficacement aux incidents de sécurité. Les cyber range commencent à être utilisés dans le domaine civil depuis une dizaine d'années [8]. Aux Etats-Unis, ce sont plus de 300 universités qui sont dotées de cyber range, avec une recherche active sur des outils d'aide au déploiement des formations [4] et sur la génération de trafic internet crédible. Microsoft a lancé en mai 2021 son logiciel de simulation de cyberattaques Simuland[1]. En

[1]https://www.microsoft.com/en-us/security/blog/2021/05/20/simuland-understand-adversary-tradecraft-and-improve-detection-strategies/

Israël, Cyberbit, la ”roll-royce” des cyber ranges équipe les 6 centres de recherche cyber et s'exporte à prix d'or avec des licences annuelles supérieures à 100k€ pour un total d'heures d'entraînement annuellement vendues supérieur au million[2] ; il existe également une version dédiée à la gestion des crises stratégiques ”sur mesure” : le *cyber crisis simulator*. N'ayant pas trouvé de publications scientifiques concernant cet objet ”de luxe”, je n'en dirai malheureusement pas plus.

B. Formation à la gestion stratégique de crise d'origine cyber

Les exercices de crise permettent d'améliorer les Plans de Continuité des Activités (PCA) communs aux structures devant interagir pendant la gestion des crises. Aujourd'hui il existe quelques exemples d'exercices d'entraînement et depuis peu des guides pour les préparer. Ils concernent de grands acteurs socio-économiques identifiés comme OIV ou OSE par le gouvernement, présentant généralement une maturité cyber importante caractérisée par la présence de Systèmes de Management de la Sécurité des Systèmes d'Information et de Continuité des Activités (SMSI : ISO- IEC 27001, SMCA : ISO-IEC 22301) opérationnels. On trouve, par exemple, à l'Institut des Hautes Études du Ministère de l'Intérieur (IHEMI, incluant l'ancien INHESJ) les publications du département Risques et crises, notamment, une définition de la cyber résilience dans le Lirec N°59 (mai 2019) [6]. Mais aussi, dans le même numéro les apports du jeu sérieux dans la gestion des crises. L'INHESJ a notamment développé CRISIS (édité en octobre 2020) : un jeu sérieux permettant à un COMEX d'expérimenter un exercice de crise sous la forme d'un jeu de plateau, dont le scénario Kiaza est à destination d'un Organisme d'Importance Vitale (OIV).

L'Exercice Cyber Résilience Attaque Nationale (ECRAN-santé#2019) regroupe, lui, un ensemble d'une centaine de joueurs et 9 structures. Cet exercice a permis de tester la chaîne d'alerte et le dispositif de crise des différentes structures et tester la coordination entre la gestion SI de l'incident cyber et la gestion des impacts sanitaires, en cas d'incident cyber majeur. Il a mobilisé le DG du Ministère des Solidarités et de la Santé (DGS), le Service du Haut Fonctionnaire de Défense et de Sécurité (HFDS/FSSI), la Direction Générale de l'Offre de Soin (DGOS), l'Agence Nationale de Sécurité du Médicament et des produits de santé (ANSM), l'Etablissement Français du Sang (EFS), l'Établissement de Transfusion sanguine Île-de-France (ETS IdF), l'ASIP Santé, l'Agence Régionale de Santé Ile-de-France (ARS IdF), et deux CHU.

C. Bonnes pratiques, guides et normes

Les normes internationales sur les systèmes de management de la sécurité des systèmes d'information (SMSI), respectivement celui de la continuité des activité (SMSA) sont l'ISO-IEC 27001 et l'ISO-IEC 22301 respectivement. La norme ISO-DIS 22361 “Crisis management” est quant à elle en rédaction. Ces normes sont généralement conçues pour des grandes entreprises et devront être adaptées aux petites entités. Elles n'abordent pas, à ma connaissance, la complexité inter cellules.

Outre atlantique, le modèle de management de la résilience développé par l'université de Carnegie-Mellon est partagé publiquement et régulièrement mis à jour sous la forme d'une revue de cyber résilience[3] (CRR) : un guide pour mesurer la maturité d'une organisation dans son management de la cyber résilience avec des questionnaires d'auto-évaluation qui accompagnent les principes à mettre en oeuvre. Parmi ces principes essentiels se trouvent une proposition d'amélioration continue de la sensibilisation et l'entraînement à la cyber résilience. Cette méthode peut aider à définir les plans d'action pédagogique à mettre en œuvre en fonction de la maturité des organismes.

En France, l'ANSSI a récemment publié un guide avec le Club des Directeurs de Sécurité des Entreprises (CDSE) sur la gestion des crises cyber (Déc. 2021) et un guide avec le Club de Continuité des Activités (CCA) sur l'organisation d'un exercice de gestion de crise cyber (Oct. 2020). Ces guides sont principalement à destination des Opérateurs de Services Essentiels (OSE) et des Organismes d'Importance Vitale (OIV). Il conviendra d'adapter ces bonnes pratiques aux possibilités et capacités des plus petites entités socio-économiques.

Après ces présentations d'exercices soit techniques, soit stratégiques et les bonnes pratiques de gestion de crise, notons l'existence en Europe d'une proposition d'exercice cyber combinant les aspects techniques et stratégiques au sein d'une cellule.

D. ROOM#42 : un simulateur de gestion de crise cyber centré sur l'humain

Lancé en 2018 au sein du Cybersecurity Competence Center du Luxembourg, ROOM#42[4] immerge une cellule de crise d'une petite dizaine de personnes au sein d'un simulateur de cyberattaque pour tester les capacités de la cellule à réagir simultanément selon tous les métiers impliqués dans cette crise : direction, RH, IT, commerce, finance, juridique. D'après les centaines d'expériences réalisées en 4 ans, selon Pascal Steinchen, ce qui demanderait de l'entraînement semble surtout être les compétences de compréhension de la situation, de décision rapide sous pression et d'analyse des conséquences de la décision prise [9]. Je n'ai pas trouvé d'information scientifique publique sur les expérimentations réalisées avec ce dispositif qui est actuellement en phase de diffusion commerciale.

Ainsi, nous avons vu un panorama de l'existant pour la formation aux gestions des crises cyber, voyons maintenant quelques approches françaises pour la gestion des crises non cyber utilisant des environnements virtuels de formation pour y immerger les cellules de crise.

[2]Cyberbit : https://www.cyberbit.com/

[3]Cyber Resilience Review (CRR) : https://www.cisa.gov/uscert/resources/assessments

[4]ROOM#42 https://room42.lu/

III. Etat de l'art national des dispositifs immersifs pour la gestion des crises

Plusieurs équipes de recherche en France abordent les exercices de gestion des crises, mais pas spécifiquement cyber, par la médiation d'une technologie numérique immersive :

a) La plateforme de simulation et de recherche de l'Institut des Sciences des Risques: (IMT Mines Alès), avec l'équipe de J.Texier et F.Tena-Chollet propose d'immerger les apprenants en les isolant dans une salle reconstituant une cellule de crise, avec différents dispositifs d'interaction et de contrôle entre les apprenants et les formateurs (mur d'écrans, tableau blanc interactif, téléphones, immersion multimodale...) [12]. Chaque scénario est développé *sur mesure* en fonction des objectifs pédagogiques pour chaque groupe d'apprenants. Les recherches portent sur les simulations multi-agent, l'optimisation de la scénarisation, l'impact pédagogique du jeu sérieux.

b) L'Institut de Recherche en Informatique de Toulouse: (IRIT) autour de J-P. Jessel travaille sur les aspects collaboratifs dans des équipes interdisciplinaires à travers l'immersion dans un environnement virtuel avec un jeu sérieux pour la formation des équipes médicales aux aspects non techniques de la gestion des risques [11].

c) Le laboratoire GeoRessources: (IMT Mines Nancy) avec l'équipe de T.Verdel travaille avec la plateforme iCrisis [10] pour interconnecter différentes cellules d'un exercice complexe par immersion dans une messagerie collaborative et pour y développer des situations d'apprentissage qui vont permettre le partage d'expérience entre les différents apprenants.

d) L'équipe IHSEV au LabSTICC de Brest: a développé autour de R. Querrec un environnement virtuel pour la prise de décision des cellules de crise au sein des SDIS, avec un tuteur intelligent qui contrôle le scénario en fonction des actions des joueurs et des objectifs pédagogiques, selon le modèle MASCARET dédié à l'apprentissage de procédures [13], [14].

e) Au sein du laboratoire Heudyasic de l'UTC: (Sorbonne Universités), une équipe constituée autour de D. Lourdeaux sur les comportements cognitifs en situation dégradée propose la suite logicielle HUMANS intégrant une génération dynamique de scénarios dans un environnement virtuel de formation pour la gestion des crises [7]. Leur approche couple les environnements virtuels avec les travaux issus de la cognition située.

f) L'équipe interdisciplinaire InSyTE de l'UTT: propose la plateforme PRESAGES[5] avec P. Laclémence pour former les acteurs publics et privés à la gestion de crises en immersion au sein d'une plateforme de crise virtuelle, notamment liée à des problématiques de transition écologique. Leurs cibles sont notamment la formation des élus de proximité à la gestion des catastrophes naturelles.

Ces savoir-faire de la recherche française dans la conception et l'usage des environnements virtuels de formation à la gestion des crises seront transférés vers la conception et l'usage d'un cyber range pour l'immersion des apprenants dans la simulation des crises cyber.

[5]Plateforme PRESAGES : https://recherche.utt.fr/presages

IV. Objectifs principaux de RéSISTeCC

RéSISTeCC présente trois objectifs principaux pour la formation à la gestion des crises cyber : une plateforme immersive et collaborative pour tous les métiers impliqués dans la gestion de la crise, un ensemble d'exercices de crise avec des scénarios couvrant plusieurs échelles des territoires dont les plus petites entités socio-économiques, un catalogue de formation continue en gestion des crises cyber répondant aux besoins identifiés par les retours d'expérience et l'anticipation des crises cyber.

A. Une plateforme immersive

Tout d'abord, le projet vise la conciliation de deux aspects qui régissent la réponse à une crise cyber, autour d'un outil de simulation unique, extension d'un cyber-range pour l'entraînement à la réponse à incident intégrant les méthodes, concepts et outils de simulation des impacts métiers et communicationnels de gestion d'une telle crise. Il s'agit d'industrialiser le processus permettant à un apprenant de s'immerger dans la simulation depuis son poste de travail habituel, avec l'importation du système d'information de l'organisation qu'il faudra simuler pour l'exercice et reproduire ses usages en mode dégradé selon les besoins en terme de simulation immersive des scénarios, avec trois niveaux de maturité cyber : informé, pratique et maîtrise. Nous reproduirons le fonctionnement du service informatique type de différents secteurs d'activité (Public, Secours, Santé, Agriculture, Numérique, Assurance). Une suite logicielle va augmenter le cyber range des aspects métiers autres que la cybersécurité et comprendra un outil de génération de scénarios d'attaques adaptés aux acteurs et à leur réaction pendant l'exercice, des outils dédiés à la préparation de la gestion de crise, à l'enseignement en classe, à l'aide à la planification ainsi qu'à l'analyse de la crise et au forensique numérique pour sortir de la crise.

B. Scénarios adaptés aux territoires

Le second objectif du projet concerne le développement des scénarios et des méthodes d'emploi permettant d'utiliser cet outil face à tout type d'interlocuteur : structure simple ou complexe, secteurs d'activités différents, niveau d'implication et de maturité cyber de chaque acteur... Ces exercices sont construits pour faire monter en compétences des interlocuteurs de tous horizons, intriquant dans les exercices l'organisme attaqué et les sociétés qui apportent les services numériques. Nous élaborerons et améliorerons une douzaine de scénarios de crise cyber pour des collectivités, des SDIS, des CH, des TPE et des PME, avec assemblages de certains scénarios pour réunir plusieurs cellules de crise en collaboration avec des administrations impliquées dans la gestion de la crise cyber comme la Police ou la Gendarmerie.

Nous allons expérimenter ces scénarios avec 4 agglomérations du nord de la nouvelle aquitaine (Gémozac, Châtellerault, Niort et Poitiers) ainsi que quelques communes plus modestes avec SOLURIS (solutions numériques pour les collectivités, Expert Cyber), les SDIS 16 et 86, le CHR de Niort, la GGD79, Pôle Emploi, en interaction avec la région Nouvelle-Aquitaine et le cyber campus régional.

C. Catalogue de formation

La plateforme de simulation immersive et interactive proposée par RéSISTeCC alimentera en exercices différents modules de formation à la gestion de crise d'une demie journée à une semaine, et jusqu'à un DU de deux ou trois mois pour la formation la plus complète, réalisés à partir des scénarios précédents qui en constituent des briques élémentaires. Cet ensemble de modules sera proposé aux acteurs socio-économiques des territoires par la médiation du Centre de ressources cyber. Les interactions particulières sous la forme de RETEX à court terme avec le centre de réponses à incidents (CERT-FR, CERT-NA) permettront d'adapter rapidement les exercices de crise aux nouvelles formes de cyberattaque et de maintenir des formations efficientes.

En s'appuyant sur les meilleures pratiques en termes de scénarisation et de jeu sérieux, nous espérons que RéSISTeCC assure l'accès à un large catalogue de scénarios de cyberattaques afin que chaque équipe organisationnelle et technique puisse reconnaître et répondre efficacement à toute technique, procédure ou encore mode opératoire de l'attaquant. Et ce, à des prix beaucoup plus abordables que les dispositifs surmesure actuels.

ACKNOWLEDGMENTS

L'appel à projets DEFFINUM a été lancé dans le cadre du *Plan de transformation et de digitalisation de la formation* de France 2030 piloté par le ministère du Travail, du Plein emploi et de l'Insertion et opéré par la Banque des Territoires.

Le consortium de RéSISTeCC constitué des sociétés DIATEAM, Crisalyde et de l'université de Poitiers remercie le PIA4 DEFFINUM pour sa confiance dans ce projet, ainsi que les toutes les structures ayant manifesté leur intérêt : Région Nouvelle-Aquitaine, Campus Cyber néo-aquitain, CLUSIR, IN.CRT, Grand Châtellereault, Gémozac, Niort Agglo, Île d'Oléron, Angoulins, Technopole Grand Poitiers, SOLURIS, MEDEF79, SPN, YPSI, SMACL et Groupe AÉMA, aini que GGD79, CHR de Niort, SDIS 16, SDIS 86 et Pôle Emploi Nouvelle-Aquitaine.

REFERENCES

[1] *NIST 2020*. The cyber range : A Guide. National Initiative for Cybersecurity Education (NICE) Cyber Range Project Team, NIST 2020.

[2] Yamin M.M, Katt B and Gkioulos V. Cyber ranges and security testbeds: scenarios, functions, tools and architecture. (2019) *Computers & Sécurity* 88(2020):101636, 1–26. https://doi.org/10.1016/j.cose.2019.101636

[3] Russo et al. Building Next Generation Cyber Ranges With CRACK Computer Security(95)101837_2020

[4] Beuran R., Pham C., Tang D., Chinen K, Tan Y and Shinoda Y. (2018) Cybersecurity education an training support system : CyRIS, *IEICE TRANS. INF. & SYST.*, E101–D(3):740–749, 2018.

[5] Kabil A, Duval T, Cuppens N, Le Comte G, Halgand Y and Ponchel C. (2018) *From Cyber Security Activities to Collaborative Virtual Environments Practices through the 3D CyberCOP Platform.* International Conference on Information Systems Security, Dec 2018, Bengaluru, India. pp.272-287. hal-01892161

[6] *INHESJ 2019*. Les risques et l'environnement numérique. Lettre d'information sur les risques et les crises (LIREC). 59.

[7] Lacaze-Labadie R. (2019) *Planification et modèle graphique pour la génération dynamique de scénarios en environnements virtuels*. Intelligence artificielle [cs.AI]. Thèse de doctorat. Université de Technologie de Compiègne, 2019. Français. NNT : 2019COMP2481. tel-02304061

[8] Päijänen J, Saharinen K, Salonen J, Sipola T, Vykopal J, Kokkonen T. (2021). *Cyber Range: Preparing for Crisis or Something Just for Technical People?*. 10.34190/EWS.21.012.

[9] Steinchen P. (2022). L'anticipation de la crise cyber : la clé de la réussite. Dans L. Raimondo (Dir) *Les fondamentaux de la gestion de crise cyber*, 47-76. Editions Ellipse. ISBN 9782340-066922.

[10] Judek Dugrand C. (2019). *The contribution of virtual crisis simulations to the study of crisis management situations: the case of iCrisis crisis simulation approach*. PhD thesis. Université de Lorraine, laboratoire GéoRessources. Nancy. tel-03117818

[11] PONS LELARDEUX C. (2017). *Environnement virtuel multi-joueurs temps-réel pour la formation à la gestion des risques: Communication et prise de décision*. Thèse de doctorat. Université de Toulouse. Laboratoire IRIT.

[12] Sauvagnargues S, Lapierre D, Limousin P, Frealle N, Tena-Chollet F, Ayral P-A, Dandreiux A et Tixier J. (2019). Concepts, outils et méthodes pour la formation à la gestion de crise. Chapitre de Prise de décision en situation de crise : Recherche et innovations pour une formation optimale. ISTE Eds. 5–32. hal-03315469

[13] Buche C., Querrec, R., De Loor P. and Chevaillier P. (2004). MASCARET : A pedagogical multi-agent system for virtual environment for training. *International Journal of Distance Education Technologies (JDET)*, 2(4):41–61.

[14] Saunier, J. Barange, M. Blandin, B., and Querrec, R. (2016) A methodology for the design of pedagogically adaptable learning environments. *The International Journal of Virtual Reality*, 16 (01): 15–21.