Cyberattaques : Impact des perceptions individuelles du risque dans l'activité de gestion de crise

Marin François, Pierre-Emmanuel Arduin, Myriam Merad

Cyberattaques : Impact des perceptions individuelles du risque dans l'activité de gestion de crise

Une proposition d'analyse systémique, cognitive et ergonomique

Marin François [1,2], **Pierre-Emmanuel Arduin** [2], **Myriam Merad** [1]

1. *Université Paris-Dauphine, PSL, LAMSADE UMR CNRS 7243*
   Place du Maréchal de Lattre de Tassigny, 75775 Paris Cedex 16, France
   marin.francois@dauphine.psl.eu,myriam.merad@dauphine.psl.eu*
2. *Université Paris-Dauphine, PSL, DRM UMR CNRS 7088*
   Place du Maréchal de Lattre de Tassigny, 75775 Paris Cedex 16, France
   pierre-emmanuel.arduin@dauphine.psl.eu

RÉSUMÉ. *Dans cet article, nous proposons un méta-modèle des relations entre perceptions individuelles du risque et processus décisionnels collectifs dans le cadre de la gestion de crise cyber. Nous évaluons notre modèle à travers deux études de cas d'exercices de gestion de crise cyber au sein d'une organisation. Enfin, nous proposons un ensemble de cinq mesures complémentaires aux référentiels de gestion de crise cyber, permettant d'intégrer plus efficacement la prévention des effets d'entraînement liés à ces perceptions individuelles.*

ABSTRACT. *In this paper, we propose a meta-model of the relationships between individual risk perceptions and collective decision-making processes in the context of cyber crisis management. We evaluate our model through the case study of two cyber crisis management exercises within an organisation. Finally, we propose a set of five complementary measures for cyber crisis management frameworks to integrate more effectively the prevention of spillover effects linked to these individual perceptions during crisis management exercises.*

MOTS-CLÉS : *Gestion de crise, Cybersécurité, Risques, Gouvernance*

KEYWORDS: *Crisis Management, Cybersecurity, Risks, Governance*

1. Introduction

Prévoir les crises, que ce soit dans le domaine de la cybersécurité ou non, est un défi, si ce n'est une impossibilité (Ros, 2020, Renn, 2021), car les risques de crise sont *de-facto* complexes. La prévention des crises cyber se heurte ainsi à la difficulté de créer des modèles opérationnels didactiques (Boin, McConnell, 2007). Cependant, s'il n'est pas possible de prévoir le déroulement des évènements menant à une crise, il est néanmoins possible de formuler une suite de recommandations pour la neutralisation des effets d'entraînement liés à la prise de décision en situation de crise, *i.e.*, en évitant l'exacerbation de risques déjà présents (Fysarakis *et al*., 2022). Ainsi, le positionnement de l'équipe de gestion de crise est double : d'une part il lui revient de traiter techniquement les incidents symptomatiques de la crise, et d'autre part de veiller à ne pas empirer l'effet d'entraînement durant la prise de décision collective. À travers cette dualité, nous retrouvons le paradigme socio-technique propre aux systèmes d'information (Boaden, Lockett, 1991, Florent *et al*., 2019). Il faut donc distinguer les risques associés aux événements survenants en amont de la crise (« gestion de risques »), et les risques liés à l'activité de gestion de crise (« gestion de crise ») (Merad *et al*., 2011, Merad, Trump, 2020).

En matière de crise cyber, les référentiels généralistes tels que l'ISO-27001(-27002) et le NIST-CSF traitent principalement du contrôle des risques en amont, dans une approche interdisciplinaire et fonctionnelle. L'ISO-27001(-27002) ne mentionnent pas explicitement les bonnes pratiques pour contenir une crise, mais la mise en œuvre d'une méthode formelle d'analyse des risques pour la formalisation d'une procédure de gestion de crise. Dans le NIST Cybersecurity Framework (NIST-CSF), la gestion de crise est mentionnée sous les piliers « réponse » et « récupération » et se concentre principalement sur la gestion des incidents. À l'inverse, les référentiels spécialisés fournissent des informations détaillées sur les bonnes pratiques en matière de contrôle de la crise. L'ISO-22361, qui remplace la norme européenne CEN-TS 17091 pour la gestion de crise et la résilience depuis 2022 définit une crise selon trois caractéristiques: complexité, instabilité, incertitude. Les principes clés de la gestion de crise selon cette norme résident dans l'efficacité de la gouvernance, de la stratégie, de la gestion des risques, de la prise de décision et de la communication. Cette approche se retrouve dans la série des publications spécialisées NIST-SP-800, dont SP-800-30 (évaluation des risques), SP-800-61 (gestion des incidents) et SP-800-184 (gestion de la récupération). Le recours aux exercices de gestion de crise est une base commune de ces référentiels. Ces exercices permettent de tester les procédures opérationnelles et habituent les participants à la prise de décision collective en situation de crise, quand ces derniers subissent une forte pression psychologique individuelle (De la Garza, Weill-Fassina, 1995, Glendon, 1999, Merad *et al*., 2011).

En outre, les référentiels mentionnés (à l'exception de NIST SP-800-61) se limitent au périmètre de l'organisation, mais qu'en est-il de la gestion de crise au sein d'un réseau d'organisations ? (Boeke, 2018, Provan, Kenis, 2008). En effet, le système d'information et de connaissance (Arduin *et al*., 2015) globalisé est incompatible avec résilience « passive », centrée sur l'organisation, à travers une réponse dans l'urgence

à la dégradation des systèmes (Evrard Samuel, Ruel, 2013). Au contraire, la résilience « active », qui est un ajustement par l'apprentissage inter-organisationnel doit se faire par une gestion de crise centrée sur le réseau d'organisations. Nous n'avons cependant identifié aucun modèle des relations entre la perception individuelle des risques et l'activité de gestion de crise cyber, que ce soit au niveau de l'organisation ou au niveau du réseau. Nous proposons donc de répondre à la problématique suivante : quel est l'impact des perceptions individuelles du risque sur les processus de décision collective dans l'activité de gestion de crise cyber au sein d'un réseau d'organisations ?

Pour répondre à cette problématique, nous revenons d'abord sur les définitions de la gestion de crise et des risques systémiques (Hancock, 2002, Golandsky, 2016, Shrivastava, 1993), puis nous étudions les modèles de relations de perceptions individuelles et collectives et d'analyse ergonomique du risque proposés dans la littérature (Glendon, 1999, Glendon *et al*., 2016, Wilde, 1998, De la Garza, Weill-Fassina, 1995). Nous étudions par ailleurs l'impact de la gouvernance du réseau d'organisations sur la gestion des crises cyber (Boeke, 2018, Provan, Kenis, 2008), à travers les méthodes d'analyse micro-structurelle des réseaux de gouvernance (Provan, Kenis, 2008). Dans la troisième section de cet article, nous proposons un méta-modèle des relations entre perceptions individuelles du risque et processus de décision collective, mettant en évidence l'amplitude du facteur d'impact individuel α (Zuccaro *et al*., 2018) et le potentiel d'entraînement qu'il induit dans l'activité de gestion de crise cyber (Merad, Trump, 2020, Merad *et al*., 2011), à l'échelle du réseau d'organisation. Dans la quatrième section, nous évaluons le méta-modèle proposé à travers deux études de cas réalisées en 2022 et 2023. En nous appuyant sur les méthodes d'analyse ergonomique (De la Garza, Weill-Fassina, 1995), nous procédons à l'extraction de schémas types d'aggravation des risques. Dans la dernière partie de cet article, nous proposons cinq bonnes pratiques complémentaires aux référentiels de gestion de crise cyber pour mieux prendre en compte l'impact des perceptions individuelles sur l'aggravation des effets d'entraînement.

2. Revue de littérature

2.1. Crises Cyber

Une crise cyber est un événement résultant d'incidents en cascade (Sherman *et al*., 2018) menaçant la sécurité de l'information et pouvant entraîner des dommages financiers, réputationnels et opérationnels graves (Hancock, 2002). Les référentiels de gestion de crise (pas nécessairement cyber) reposent sur des éléments techniques, organisationnels et scientifiques (Bénaben, 2016, Kulikova *et al*., 2012), mais se veulent généralistes et haut-niveau, adressant plus globalement la gestion de risque que la gestion de crise (Miller, Griffy-Brown, 2018). Dans l'ensemble, les concepts fondamentaux de la gestion de crise s'appliquent à la gestion des crises cyber, avec pour élément central la préparation (Hancock, 2002, Johansson, Härenstam, 2013, Kovoor-Misra *et al*., 2001).

La gestion des crises cyber implique d'abord l'anticipation des procédures – en portant attention particulière aux problèmes de sécurité théoriques (Mikolaj, 2005), puis pratiques, à travers la réponse et la récupération (Golandsky, 2016). La conformité réglementaire et la gestion de la réputation sont également à prendre en compte (Kulikova *et al*., 2012). La gestion efficace des crises cyber suppose une gestion efficace des connaissances et une communication adaptée (Johansson, Härenstam, 2013, Kulikova *et al*., 2012), la participation de multiples parties-prenantes (Lauras *et al*., 2015) pour une réponse rapide et coordonnée (Trimintzios *et al*., 2015).

L'évaluation et l'apprentissage sont cruciaux (Dawes *et al*., 2004) pour l'amélioration de la gestion de crise (Golandsky, 2016), au même titre que la construction de structures organisationnelles durables par les ressources internes, la formation des équipes et les investissements (Shrivastava, 1993). Les organisations peuvent apprendre des crises passées et aspirer au développement de leurs capacités de réponse (Bederna *et al*., 2017), pour passer d'une posture réactive à une posture anticipative (Shrivastava, 1993).

2.2. Nature des risques

Les risques systémiques sont caractérisés par quatre composantes (Renn, 2011). *(1) Complexité*, résultant en des difficultés à établir des relations causales entre plusieurs événements et effets indésirables; *(2) Incertitude*, caractérisée par une forte variation statistique des observations, un environnement prône aux erreurs de mesure, par un manque de connaissance ou une forte indétermination (Renn, 2011, 2021, Renn *et al*., 2019, Van Asselt, 2000); *(3) Ambiguïté*, sous-jacente à la variabilité dans l'interprétation logique des événements observés et l'incertitude (Renn *et al*., 2011), et *(4) Effet d'entraînement* au-delà de l'environnement des sources de risques (Kasperson *et al*., 2003).

Selon cette définition, les risques de crise cyber sont *de facto* des risques systémiques (Davis, 2005, Forscey *et al*., 2022, Sommer, Brown, 2011). Schweizer (2021), German Advisory (2018) proposent de qualifier les risques systémiques selon un modèle d'aide à la décision multicritère prennant en compte les facteurs d'évaluation suivants : étendue et persistence des dommages, ubiquité, réversibilité, latence, violation de l'équité et potentiel de mobilisation.

Ainsi, c'est parce qu'ils possèdent ces attributs très spécifiques qu'ils diffèrent des risques « classiques », connus sous le nom de risques « idiosyncratiques ». Ces derniers sont potentiellement quantifiables et prévisibles, ce qui n'est pas le cas pour les risques systémiques. Le tableau 1 résume les différences entre ces deux types de risques.

2.3. Perceptions du risque

L'un des modèles consensuels d'analyse des perceptions individuelles du risque est proposé par Glendon (1999), Hale, Glendon (1987). Cependant, dans sa première

TABLEAU 1. *Risques Systémiques vs. Idiosyncratiques*

Risques Systémiques	Risques Idiosyncratiques
Grande Complexité	Effet Causal Direct
Réponse Non Linéaire	Réponse Linéaire
Forte Stochasticité	Stochasticité Limitée
Distribution loi de puissance	Distribution Normale
Indétermination	Déterminé
Effet d'entraînement extrême	Faible effet d'entraînement

version, le modèle ne prend pas en considération la perception individuelle du risque lorsque l'individu fait partie d'un groupe. Le deuxième modèle d'interprétation des risques ultérieurement proposé par Glendon *et al*. (2016) introduit des risques spéculatifs (relatifs aux domaines de l'égo et du social), conciliant la Théorie de l'Homéostasie des Risques (RHT) de Wilde (1998) avec la théorie de la prise de décision organisationnelle – replaçant l'individu au sein du groupe (voir Tableau 2).

Ce modèle implique les processus de « *hot-cognition* » et « *cold-cognition* » à travers quatre questions sources impactant la psychologie de l'individu. Le concept de « *hot-cognition* » et « *cold-cognition* », détaillé dans Glendon (1999), revient notamment à jauger l'impact des émotions sur le processus cognitif. De Smidt, Botzen (2018) ont étudié, pour le cas précis de l'évaluation de risques cyber, comment les biais de jugement des individus occupant différents rôles de gestion de risque cyber impactaient leurs perceptions, montrant que les décideurs techniques surestiment les probabilités d'attaque et sous-estiment les impacts financiers. En outre, la vulnérabilité perçue, les croyances en compétences propres (Debb, McClellan, 2021), les aptitudes personnelles (Kostyuk, Wayne, 2021), interpersonnelles et l'heuristique d'affect (Skagerlund *et al*., 2020, Van Schaik *et al*., 2020) influencent également la perception du risque et donc la gestion de crise.

Pour extraire des schémas types de situation d'aggravation à travers l'interprétation collective du risque, De la Garza, Weill-Fassina (1995) s'appuient sur les méthodes d'analyse systémique et cognitive. Historiquement, la première approche se concentre sur les caractéristiques environnementales du risque, tandis que la seconde considère les schémas d'interprétation de l'individu. Les auteurs s'appuient sur la première version du schéma d'interprétation et de réaction aux risques (Glendon, 1999, Hale, Glendon, 1987), combiné à l'approche systémique. Dans cet article, nous nous appuyons sur le « cadre combiné d'analyse ergonomique » ainsi proposé par les auteurs, cependant, nous utiliserons le modèle de Glendon *et al*. (2016), puisque celui-ci prend en compte la dimension collective.

2.4. Réseaux de Gouvernance

Pour Provan, Kenis (2008), les réseaux sont des ensembles regroupant trois organisations indépendantes ou plus avec des objectifs individuels et collectifs, présentant des dynamiques spontanées, mandatées ou contractuelles. Les auteurs proposent des

TABLEAU 2. *Perception individuelle vs. collective du risque*

Individuelle	Collective
« *Cold cognition* »	« *Cold & Hot cognition* »
Risques purs	Risques purs & spéculatifs
Adaptations choisies	Culture, règles, politiques
Boucle unique fermée	Boucles multiples

éléments pour l'analyse des modes de gouvernance dans les réseaux d'organisations, où deux approches prévalent : l'approche micro-structurelle et l'approche du réseau en tant que forme de gouvernance (Provan, Kenis, 2008). Dans la permière, le réseau est analysé à travers les relations et les caractéristiques des individus qui le composent, dans la seconde, le réseau est analysé « à l'échelle », ce qui signifie que l'unité de référence est celle du réseau, et non plus des organisations qui le composent.

Provan, Kenis (2008) proposent un cadre tenant compte de différentes configurations micro-structurelles et incluant également la dynamique du réseau à l'échelle. Trois modes distincts de gouvernance des réseaux sont indentifiés : (1) Réseau gouverné par les participants (« *Shared Governance* »), (2) Réseau gouverné par une organisation meneuse (« *Lead Agency* ») et (3) Réseau gouverné par une organisation administrative annexe (« NAO »). Pour Provan, Kenis (2008) toujours, l'adaptation entre le mode de gouvernance et les caractéristiques micro-structurelles du réseau définit la performance ou l'échec de la gouvernance. Les organisations doivent choisir un mode de gouvernance adapté aux caractéristiques du réseau : niveau de confiance au sein du réseau, nombre de participants, force du consensus sur les objectifs, besoin en compétences techniques, *etc.*... Puis, arbitrer parmi plusieurs avantages et inconvénients liés au mode de gouvernance choisi, comme l'inclusivité de la prise de décison et la réactivité, la légitimité interne des choix stratégiques et la légitimité externe, la stabilité des processus et la flexibilité.

Tous ces éléments influencent directement la résilience du réseau et des organisations qui le composent, comme le montre Boeke (2018), en appliquant la méthode d'analyse de Provan, Kenis (2008) pour étudier les différences structurelles dans les modes de gouvernance des états au sein du consortium européen de collaboration pour la cybersécurité (EU-CyCLONe).

3. Méta-modèle et méthode d'analyse

Maintenant que nous avons une vue d'ensemble des relations liant la perception individuelle du risque, la perception collective et les conditions de performance de la gouvernance en réseau, nous sommes en mesure de proposer un méta-modèle reliant ces éléments. Le modèle proposé est présenté dans la Figure 1.

(A) Dans notre méta-modèle, les biais de jugement, par exemple liés à l'expertise, ont un impact direct sur les perceptions individuelles du risque (Skagerlund *et al.*,

2020, Van Schaik *et al*., 2020), au même titre que l'absence de connaissances (Arduin *et al*., 2015).

(B) Nous stipulons ensuite que les perceptions individuelles du risque, à travers les « *hot-cognition* » et « *cold-cognition* », (Glendon, 1999, Glendon *et al*., 2016, Hale, Glendon, 1987) modifient l'appétence au risque et l'interprétation des signaux en situation de crise (Wilde, 1998). L'évaluation du risque au niveau collectif, tenant compte des facteurs cognitifs spécifiques aux perceptions individuelles au sein du groupe (Glendon, 1999) est donc différente de celle des individus.

(C) Lorsque ces organisations forment des réseaux, ces derniers se caractérisent par l'alignement entre le mode de gouvernance choisi et les caractéristiques structurelles du réseau (Provan, Kenis, 2008). Selon Provan, Kenis (2008), cet alignement agit sur la perception du risque par les individus. Par exemple, un niveau de méfiance élevé au profit d'une gouvernance partagée aura un impact direct sur l'appétence au risque des individus, ce qui pourra se caractériser à terme, par l'adoption de règles, référentiels et normes communes et une incitation au contrôle entre les parties prenantes. C'est également cet alignement entre structure et mode de gouvernance qui impactera la performance du réseau en situation de gestion de crise, en impactant par exemple sa réactivité.

(D) À leur tour, les performances du réseau auront un impact sur les individus. *Ex-post*, les individus considéreront la structure de gouvernance du réseau à la lumière des décisions prises et de leur interprétation du déroulement des événements, les amenant à réévaluer leurs perceptions. Cela passe notamment par l'interprétation retrospective des décisions prises par les individus et le réseau par rapport aux conséquences de la crise et de sa gestion.

(E) Par ailleurs, les individus percevront les événements affectant d'autres participants de leur environnement (par exemple, une crise similaire chez un concurrent) et ajusteront leurs perceptions individuelles en tenant compte de ces éléments, ce sont les risques subjectifs.

(F) Enfin, nous stipulons que naturellement, le mode de gouvernance évoluera par la transformation du réseau vers un alignement optimal (Provan, Kenis, 2008) et que tous ces éléments sont soumis à l'incitation au changement fournit par la technologie (Provan, Kenis, 2008).

Notre méta-modèle permet donc de combiner les modèles existants pour un cadre d'analyse combiné incluant les perceptions individuelles, collectives, et entre plusieurs organisations dans le cadre d'une activité de gestion de crise. Par ailleurs, il permet d'analyser le caractère évolutif des pratiques de gestion de crise, en prenant en compte l'apprentissage organisationnel. Cette proposition n'existe – à notre connaissance – pas dans la littérature. Sans cette proposition, nous devrions analyser les données collectées au regard de trois grilles différentes, puis conjuger les résultats. Nous devrions par ailleurs faire ce travail pour les deux années, sans garantie de pouvoir lier les observations d'une année avec la suivante. Ainsi, en conjugant les éléments issus de la littérature dans un cadre combiné d'analyse, nous pouvons désormais utiliser les fac-

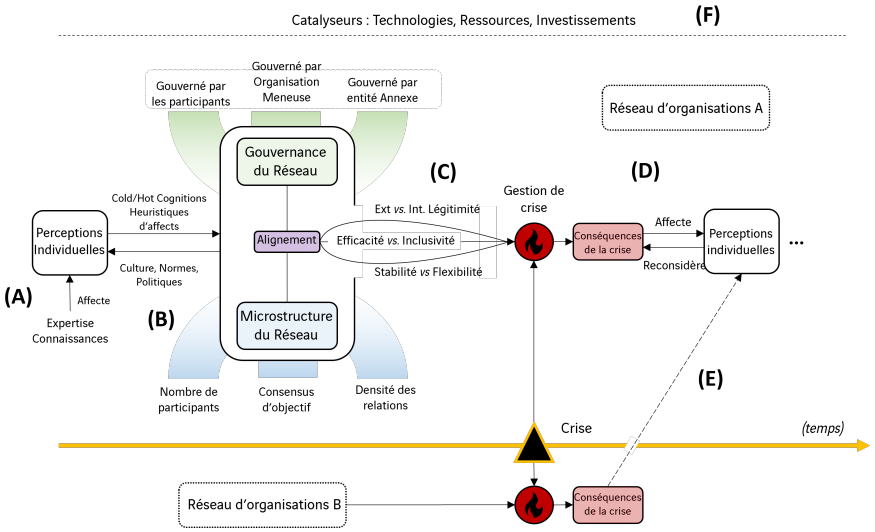

FIGURE 1. *Meta-modèle des relations entre le mode de gouvernance, les perceptions individuelles et l'activité de gestion de crise au sein du réseau d'organisations*

teurs listés et leurs interactions afin de valider ou non leur influence sur l'activité de gestion de crise et son évolution d'une année sur l'autre.

Nous allons maintenant évaluer ce méta-modèle (voir Figure 1) au regard de l'ensemble des données recueillies sur le terrain. Nous utilisons deux enregistrements d'une unité opérationnelle de gestion de crise cyber au sein d'un réseau d'organisations du secteur de l'énergie. Le premier enregistrement date du troisième trimestre de 2022, le second d'un an plus tard. Les protagonistes sont experts dans différents domaines (terminaux, réseaux, sécurité, applications, ERP, ...). Chaque enregistrement dure environ une demi-journée. Le tableau 3 résume les caractéristiques des enregistrements.

TABLEAU 3. *Caractéristiques des enregistrements*

Caractéristique	2022	2023
Scénario	Rançongiciel	Compromission prestataire
Profils	Experts Techniques	Experts Techniques
Chronologie	Q3 2022	Q3 2023
Lieu	Salle de crise	Salle de crise + À distance
Durée	Demi-journée	Demi-journée
# de participants	25	79
% de participants formés à la gestion de crise	100%	environ 30%
Nombre d'Organisations	1	45
Structure	Organisation Unique	Réseau d'Organisations

3.1. Méthode d'analyse ergonomique

Nous analysons les pratiques de gestion de crise telles qu'elles sont définies dans les référentiels par rapport aux facteurs de réussite ou d'échec tels que définis dans notre méta-modèle. Une représentation synthétique de ce mode d'analyse, tel que repris de De la Garza, Weill-Fassina (1995) est présentée dans la Figure 2.

Dans les lignes d'un tableau nous positionnons les éléments définis dans les référentiels spécialisés, et les colonnes suivantes sont divisées en groupes de séquences (T1, T2, ...) correspondant aux phases de l'exercice. Les séquences identifiées ont été tirées des travaux de préparation des exercices de crise, de manière à *(i)* s'assurer que les *stimuli* sont cohérents (communications envoyées, évènements majeurs décrits), et *(ii)* que les réponses possibles à ces *stimuli* constituent des apprentissages souhaitables. Une colonne est définie pour chaque facteur de performance/risque tels qu'identifiés dans notre méta-modèle. Pour chaque séquence d'actions (par exemple, E1/T1 (Exercice 1, Séquence 1) - Incident de fraude au paiement signalé), nous indiquons *(a)* si la tâche de gestion de crise est effectuée telle que définit dans les référentiels, et *(b)* si l'un des facteurs de performance/risque a impacté la tâche.

Les perceptions individuelles sont ainsi analysées au travers du discours des participants en lien avec les facteurs définis en Tableau 2, dans une approche descriptive. Par exemple, durant la première séquence clé de l'exercice 2022 (E1-T1), la tâche « NIST CSF - DT / ISO22361: Les évenements sont analysés pour anticiper les actions adverses » est effectuée, mais les échanges qui s'en suivent débouchent sur deux analyses divergentes par deux parties de l'équipe de gestion de crise. L'analyse choisie est alors définit par l'opérateur avec le plus haut niveau hierarchique. La compréhension des activités adverses est donc notée dans notre tableau comme « influencée par le facteur *structure organisationnelle et hiérarchique* ».

Cette méthode d'analyse est calquée sur la méthode d'analyse ergonomique proposée par De la Garza, Weill-Fassina (1995), à la différence que nous n'utilisons pas les mêmes représentations opérationnelles (notre méta-modèle prend en compte les risques subjectifs) ni les mêmes unités pour les séquences de temps (dans l'article original, les heures sont utilisées, nous utilisons les séquences).

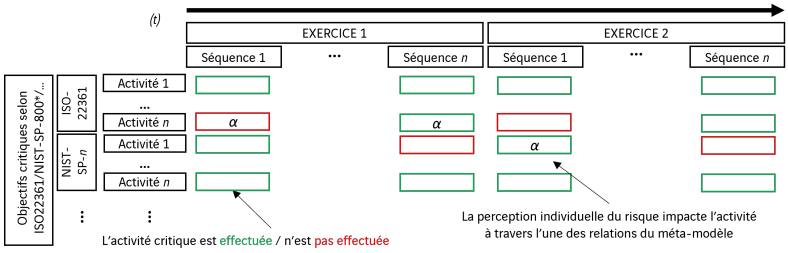

FIGURE 2. *Structure utilisée pour l'analyse ergnonomique, inspirée de De la Garza, Weill-Fassina (1995)*

4. Étude de cas

En analysant les données collectées, nous avons pu comparer à travers l'analyse descriptive du discours des participants et de leurs comportements, d'une année sur l'autre et comparer les mesures prises avec celles suggérées dans les référentiels. Nous avons pu valider la présence de facteurs influents tels que définis dans notre méta-modèle, notamment en identifiant des signes très concrets liés au processus de « *hot cognition* », à l'impact significatif du mode de gouvernance de la structure sur la gestion de crise, à l'importance de la confiance et de la prise de décision partagée dans les processus décisionnels sous pression, à l'impact des heuristiques d'affect et aux limites de l'efficacité des exercices de crise sur les participants. Les séquences analysées sont présentées dans le Tableau 4.

4.1. Impacts des perceptions individuelles du risque

La structure de l'équipe opérationnelle, avec un leadership fort guidant les autres équipes, correspond à un mode de gouvernance par Organisation Meneuse (« *Lead Agency* », Provan, Kenis (2008)). La prise de décision est en conséquence centrale, extrêmement rapide dans cette organisation. Cependant, cela a également conduit à ce que les suggestions d'autres membres, qui se seraient avérées efficaces, ne soient pas prises en compte. Au cours du premier exercice, l'équipe opérationnelle centrale a perdu beaucoup de temps en ne tenant pas compte d'une suggestion d'investigation formulée par un protagoniste. Il est ensuite apparu que cette recommandation aurait permit de contenir rapidement la crise. Bien qu'au début de l'exercice, la prise de décision soit soumise à la validation partagée, à mesure que l'exercice progresse, celle-ci dérive vers une prise de décision directe et centrale. Il est fait mention explicite que les décideurs seraient tenus responsables de certaines décisions si elles étaient remises en question en dehors de l'organisation, assurant ainsi la légitimité externe. Presque tous les techniciens impliqués ont fait preuve d'heuristiques d'affect lors de l'analyse des impacts potentiels et des délais de réponse associés aux systèmes dont ils ont la responsabilité. Nous avons par exemple constaté que les estimations de temps de chargement étaient jusqu'à quatre fois plus élevées que les temps avérés. Enfin, nous avons identifié des limites à la pratique des exercices de gestion de crise. Par exemple, lorsque plusieurs protagonistes ont identifié des soucis de cohérence dans les séquences, cela les a incité à réduire leur implication dans le jeu. Nous avons également noté que l'absence d'impact réel des décisions des joueurs sur le scénario les a progressivement démobilisé et les a amené à devenir de moins en moins impliqués. L'évolution globale de ce processus est présentée dans la Figure 3.

4.2. Apprentissage au sein du réseau d'organisation

Au cours du deuxième exercice, nous avons observé une évolution de la prise en compte de l'impact des décisions dans la gestion de crise. Nous avons pour cela comparé les processus décisionnels par rapport à l'année précédente au sein de l'orga-

TABLEAU 4. *Séquences des exercices*

Phase	Événements principaux
EX 1 - T1. Découverte de l'intrusion	– Activités suspectes provenant du serveur SRV1 vers SRV2 – Renseignements révèlent une campagne active d'exploitation 0-day sur SRV1 – Les enquêtes sur SRV1 révèlent une exploitation 0-day
EX 1 - T2. Rançongiciel	– Les journaux SRV2 indiquent des tentatives de connexion infructueuses d'un administrateur – Le SRV1 compromis est isolé – Le compte utilisé pour les tentatives SRV1 vers SRV2 est bloqué – Des problèmes de connexion sont apparus pour un petit groupe d'utilisateurs ERP – L'investigation révèle que les comptes associés n'ont plus suffisamment de droits pour se connecter à ERP – D'importantes modifications de l'annuaire ont été détectées sur SRV2 et le compte administrateur a été modifié – Plusieurs utilisateurs signalent des échecs de connexion ERP – Le département financier alerte sur des autorisations de paiement suspectes pour des montants élevés – Un rançongiciel a été détecté sur plusieurs terminaux – Une capture d'écran de la discussion de l'équipe de crise a été publiée sur Twitter avec le message « un coup d'avance » – Plusieurs applications sont chiffrées et inutilisables – Le compte utilisé pour propager le rançongiciel a été identifié – Un e-mail contenant une demande de rançon a été reçu
EX 1 - T3. Planification de la récupération	– Les systèmes ERP ont été arrêtés – Tout accès externe au système d'information a été fermé – La diffusion du rançongiciel est terminée, 50 % des terminaux ont été chiffrés – Une partie de l'ERP est chiffrée – Plusieurs fournisseurs contactent les services financiers pour se plaindre de retards de paiement
EX 1 - T4. Récupération	– Les services de SRV1,SRV2 et de réseau sont reconstruits – Antivirus est redéployé sur l'ensemble des terminaux – Applications et bases de données sont restaurées à l'aide de sauvegardes – Tous les ordinateurs impactés doivent être remis à neuf – La communication avec les clients et fournisseurs est effectuée
EX 2 - T1. Accès initial	– Plusieurs utilisateurs de la direction ont reçu un courriel frauduleux demandant le paiement de 800 000£ – Alertes multiples sur le poste de travail de l'utilisateur émetteur du courriel, le compte est compromis – Plusieurs entrées de données ERP ont été modifiées – Un deuxième compte compromis a été confirmé sur le poste de travail identifié
EX 2 - T2. Modification des données métier	– Modification confirmée des données pour au moins deux zones géographiques – L'investigation révèle que la compromission date d'une semaine – Confirmation que l'e-mail de frauduleux a été envoyé par un fournisseur externe – Alertes multiples sur plusieurs terminaux – Confirmation du gel de modifications des serveurs
EX 2 - T3. Mode de blocage	– Modification confirmée des données ERP et irréversibilité constatée – La direction financière demande le blocage des paiements – Rançongiciel détecté par l'EDR sur plusieurs terminaux – Plusieurs responsables financiers ont reçu le même courriel de demande de rançon – Les alertes de rançongiciel sont confirmées faux positifs
EX 2 - T4. Rançon demandée	– E-mail demandant une rançon reçu, fichier de 145 Go supposément récupéré et menacé d'être publié – Plusieurs protagonistes ont été contactés par des journalistes

nisation meneuse. Les protagonistes sont à deux joueurs près les mêmes que l'année précédente, avec les mêmes responsabilités respectives, ce qui facilite notre comparaison. La différence principale dans la structure du réseau est l'ajout de nouvelles organisations « suiveuses » de l'organisation meneuse présente depuis le premier exercice. Dans la mesure où les joueurs savent que les premiers signaux faibles observés conduiront à une situation de crise, ils ont résisté à l'incitation à activer directement le protocole de crise et se sont contentés de traiter l'incident source. Mention explicite est également faite des exercices passés, et en particulier de la nécessité de tenir un registre rigoureusement mis à jour des actions entreprises et d'alerter si des informations sont perdues lors de la prise d'une décision. Le responsable de l'organisation meneuse a également explicitement demandé aux joueurs de partager leurs commentaires et intuitions avec lui tout au long de l'exercice, mettant en exergue une volonté d'incorporer une prise de décision partagée. De manière générale, nous avons identifié deux domaines principaux de changement entre les deux exercices annuels : une communication améliorée et, surtout, une prise de décision partagée. Il semble que l'équipe opérationnelle ait réussi à travailler sur un mode de gouvernance qui lui permet de maintenir un certain degré d'efficacité tout en incluant de manière plus efficace les intuitions et l'expertise des autres membres. Nous avons par ailleurs noté une augmentation du biais de confiance au cours de cet exercice, avec une remise en question extrêmement importante de la véracité des informations, généralement suivie d'opérations de vérification. Cependant, cette approche rigoureuse de la vérification des informations a conduit à plusieurs reprises à un gaspillage inutile de temps. Aucune stratégie optimale pour ce point n'est mentionnée dans les directives de gestion de crise.

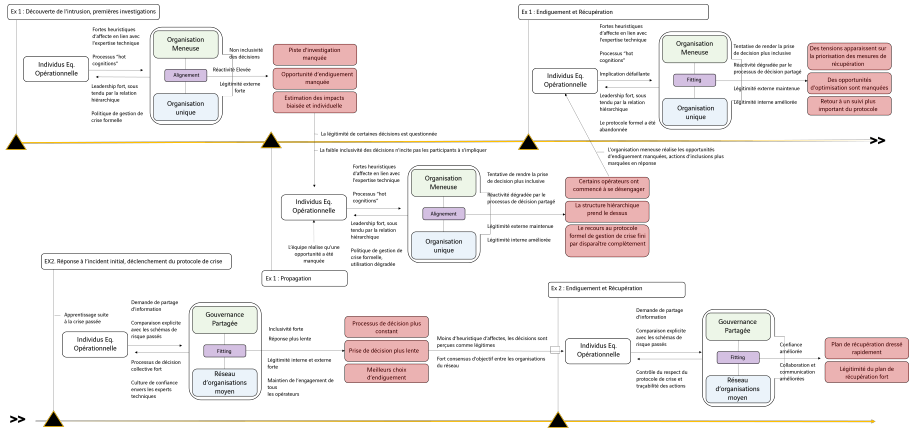

FIGURE 3. *Évolution de la gouvernance en lien avec les perceptions individuelles du risque*

5. Conclusions et perspectives

Nous avons proposé dans cet article un méta-modèle illustrant les relations complexes entre la perception individuelle du risque et la prise de décision collective dans le cadre de la gestion de crise cyber. Par deux études de cas, nous avons confirmé l'applicabilité de notre méta-modèle et démontré son efficacité pour identifier des schémas typiques d'aggravation du risque. L'impact des perceptions individuelles du risque émerge comme un élément significatif influençant l'efficacité des activités de gestion de crise, mais les normes actuelles de gestion de crise ne parviennent souvent pas à reconnaître et à aborder pleinement ce facteur. En intégrant explicitement l'interaction entre les perceptions individuelles du risque, la prise de décision collective et l'efficacité des modes de gouvernance du réseau lors de la gestion des crises cyber, ce méta-modèle offre une perspective nuancée qui peut être utilisée pour analyser la pratique de la gestion de crise au sein d'un réseau d'organisations. En réponse à la problématique de cet article, nous avons formulé ci-dessous cinq propositions didactiques pour la gestion de crise, au regard de notre analyse.

Leadership Si un leadership fort est crucial, il faut veiller à ce qu'il n'éclipse pas les suggestions des parties prenantes. Il faut ainsi encourager une communication ouverte et créer un environnement où tous les membres de l'équipe se sentent habilités à exprimer leurs perspectives.

Heuristiques d'affects Lors de la réalisation d'analyses d'impact, il convient de prendre en compte les heuristiques d'affects qui peuvent déformer les perceptions des analystes, en lien avec leurs spécialisations et les risques subjectifs perçus. Pour cela, il est possible de recourir à un outillage d'analyse d'impact partagé, connu et accepté des participants, faisant autorité en la matière et défini en amont de la crise.

Mode de gouvernance Adopter un modèle « Organisation Meneuse » pour une gouvernance efficace du réseau permet une réponse rapide aux incidents, l'idéal est de mettre en place des accords de décision partagée ou des points de validation réguliers. Cette inclusion permet non seulement une contribution collaborative, mais renforce également la légitimité interne et la confiance des participants sans compromettre l'efficacité globale.

Culture et expérience Il est pertinent de mentionner explicitement les crises passées lors des discussions pour aider à la visualisation et à la contextualisation. La référence à des instances spécifiques peut fournir un cadre tangible pour comprendre les défis potentiels et les solutions, en fournissant un référentiel partagé des schémas types de risques, améliorant la capacité de l'équipe à naviguer efficacement dans la crise.

Confiance et légitimité Les responsables d'équipes meneuses doivent donner la priorité à la légitimité interne et externe des décisions. En interne, il faut s'assurer que les décisions correspondent aux valeurs et aux objectifs de l'équipe, favorisant la confiance et la légitimité. En externe, il faut communiquer les décisions de manière transparente pour renforcer la légitimité des actions entreprises.

Dans nos futurs travaux, nous allons collecter les données d'un troisième exercice de crise afin de valider une nouvelle fois le méta-modèle proposé, en tentant d'anticiper les transformations du réseau que celui-ci pourrait induire. Par ailleurs, nous souhaiterions implémenter les recommandations formulées dans le plan de formation des opérateurs de l'organisation meneuse afin de vérifier leur efficacité. Aussi, nous souhaitons mettre en place un méthode d'analyse qualitative des perceptions individuelles plus complète que l'analyse descriptive proposée ici, notamment par la mise en place d'entretiens avec les participants. Enfin, nous souhaitons définir des marqueurs précis de l'influence technologique en tant que catalyseur des dynamiques des prise de décision, afin de vérifier que ces derniers ont un impact significatif, tels que nous l'avons stipulé dans notre méta-modèle.

Bibliographie

Arduin P.-E., Grundstein M., Rosenthal-Sabroux C. (2015). *Système d'information et de connaissance* (vol. 4). ISTE Group.

Bederna Z., Rajnai Z., Szadeczky T. (2017). Further strategy analysis of cybersecurity incidents. *Land Forces Academy Review*, vol. 26, n° 3, p. 251–260.

Bénaben F. (2016). A formal framework for crisis management describing information flows and functional structure. *Procedia Engineering*, vol. 159, p. 353–356.

Boaden R., Lockett G. (1991). Information technology, information systems and information management: definition and development. *European Journal of Information Systems*, vol. 1, n° 1, p. 23–32.

Boeke S. (2018). National cyber crisis management: Different european approaches. *Governance*, vol. 31, n° 3, p. 449–464.

Boin A., McConnell A. (2007). Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience. *Journal of contingencies and crisis management*, vol. 15, n° 1, p. 50–59.

Davis B. J. (2005). Prepare: seeking systemic solutions for technological crisis management. *Knowledge and Process Management*, vol. 12, n° 2, p. 123–131.

Dawes S. S., Cresswell A. M., Cahan B. B. (2004). Learning from crisis: Lessons in human and information infrastructure from the world trade center response. *Social Science Computer Review*, vol. 22, n° 1, p. 52–66.

De la Garza C., Weill-Fassina A. (1995). Méthode d'analyse des difficultés de gestion du risque dans une activité collective: l'entretien des voies ferrées". *Safety Science*, vol. 18, n° 3, p. 157–180.

Debb S. M., McClellan M. K. (2021). Perceived vulnerability as a determinant of increased risk for cybersecurity risk behavior. *Cyberpsychology, Behavior, and Social Networking*, vol. 24, n° 9, p. 605–611.

De Smidt G., Botzen W. (2018). Perceptions of corporate cyber risks and insurance decision-making. *The Geneva Papers on Risk and Insurance-Issues and Practice*, vol. 43, p. 239–274.

Evrard Samuel K., Ruel S. (2013). Systèmes d'information et résilience des chaînes logistiques globales. *Systèmes d'information et management*, vol. 18, n° 1, p. 57–85.

Florent B., Nicolas M., Marchand A. L., Colin B. (2019). Cyber attaques: Organiser la confiance. In *Epic*.

Forscey D., Bateman J., Beecroft N., Woods B. (2022). *Systemic cyber risk: A primer*. Carnegie Endowment for International Peace.

Fysarakis K., Mavroeidis V., Athanatos M., Spanoudakis G., Ioannidis S. (2022). A blueprint for collaborative cybersecurity operations centres with capacity for shared situational awareness, coordinated response, and joint preparedness. In *2022 ieee international conference on big data (big data)*, p. 2601–2609.

German Advisory C. for. (2018). Strategies for managing global environmental risks.

Glendon I. (1999). Management of risks by individuals and organisations. *Safety Science Monitor*, vol. 3, n° 4, p. 2–11.

Glendon I., Clarke S., McKenna E. (2016). *Human safety and risk management*. Crc Press.

Golandsky Y. (2016). Cyber crisis management, survival or extinction? In *2016 international conference on cyber situational awareness, data analytics and assessment (cybersa)*, p. 1–4.

Hale A. R., Glendon I. (1987). *Individual behaviour in the control of danger*. Elsevier Science.

Hancock B. (2002). Security crisis management—the basics. *Computers & Security*, vol. 21, n° 5, p. 397–401.

Johansson A., Härenstam M. (2013). Knowledge communication: a key to successful crisis management. *Biosecurity and bioterrorism: biodefense strategy, practice, and science*, vol. 11, n° S1, p. S260–S263.

Kasperson R. E., Pidgeon N. F., Slovic P. (2003). *The social amplification of risk*. Cambridge University Press.

Kostyuk N., Wayne C. (2021). The microfoundations of state cybersecurity: Cyber risk perceptions and the mass public. *Journal of Global Security Studies*, vol. 6, n° 2, p. ogz077.

Kovoor-Misra S., Clair J. A., Bettenhausen K. L. (2001). Clarifying the attributes of organizational crises. *Technological Forecasting and Social Change*, vol. 67, n° 1, p. 77–91.

Kulikova O., Heil R., Berg J. van den, Pieters W. (2012). Cyber crisis management: A decision-support framework for disclosing security incident information. In *2012 international conference on cyber security*, p. 103–112.

Lauras M., Truptil S., Benaben F. (2015). Towards a better management of complex emergencies through crisis management meta-modelling. *Disasters*, vol. 39, n° 4, p. 687–714.

Merad M., Ouerdane W., Dechy N. (2011). Expertise and decision-aiding in safety and environment domains: what are the risks? In *Esrel annual conference 2011*, p. 2317–2323.

Merad M., Trump B. D. (2020). *Expertise under scrutiny*. Springer.

Mikolaj J. (2005). Crisis management in security environment. *Komunikácie-vedecké listy Žilinskej univerzity v Žiline*, vol. 7, nº 3, p. 29–33.

Miller H., Griffy-Brown C. (2018). Developing a framework and methodology for assessing cyber risk for business leaders. *Journal of Applied Business & Economics*, vol. 20, nº 3.

Provan K. G., Kenis P. (2008). Modes of network governance: Structure, management, and effectiveness. *Journal of public administration research and theory*, vol. 18, nº 2, p. 229–252.

Renn O. (2011). The social amplification/attenuation of risk framework: application to climate change. *Wiley Interdisciplinary Reviews: Climate Change*, vol. 2, nº 2, p. 154–169.

Renn O. (2021). New challenges for risk analysis: systemic risks. *Journal of Risk Research*, vol. 24, nº 1, p. 127–133.

Renn O., Klinke A., Van Asselt M. (2011). Coping with complexity, uncertainty and ambiguity in risk governance: a synthesis. *Ambio*, vol. 40, p. 231–246.

Renn O., Lucas K., Haas A., Jaeger C. (2019). Things are different today: the challenge of global systemic risks. *Journal of Risk Research*, vol. 22, nº 4, p. 401–415.

Ros G. (2020). The making of a cyber crash: a conceptual model for systemic risk in the financial sector. *ESRB: Occasional Paper Series*, nº 2020/16.

Schweizer P.-J. (2021). Systemic risks–concepts and challenges for risk governance. *Journal of Risk Research*, vol. 24, nº 1, p. 78–93.

Sherman A. T., DeLatte D., Neary M., Oliva L., Phatak D., Scheponik T. *et al*. (2018). Cybersecurity: Exploring core concepts through six scenarios. *Cryptologia*, vol. 42, nº 4, p. 337–377.

Shrivastava P. (1993). Crisis theory/practice: Towards a sustainable future. *Industrial & Environmental Crisis Quarterly*, vol. 7, nº 1, p. 23–42.

Skagerlund K., Forsblad M., Slovic P., Västfjäll D. (2020). The affect heuristic and risk perception–stability across elicitation methods and individual cognitive abilities. *Frontiers in psychology*, vol. 11, p. 970.

Sommer P., Brown I. (2011). Reducing systemic cybersecurity risk. *Organisation for Economic Cooperation and Development Working Paper No. IFP/WKP/FGS (2011)*, vol. 3.

Trimintzios P., Holfeldt R., Koraeus M., Uckan B., Gavrila R., Makrodimitris G. (2015). *Report on cyber crisis cooperation and management: Comparative study on the cyber crisis management and the general crisis management*.

Van Asselt M. (2000). *Perspectives on uncertainty and risk: the prima approach to decision support*. Springer Science & Business Media.

Van Schaik P., Renaud K., Wilson C., Jansen J., Onibokun J. (2020). Risk as affect: The affect heuristic in cybersecurity. *Computers & Security*, vol. 90, p. 101651.

Wilde G. J. (1998). Risk homeostasis theory: an overview. *Injury prevention*, vol. 4, nº 2, p. 89–91.

Zuccaro G., De Gregorio D., Leone M. F. (2018). Theoretical model for cascading effects analyses. *International journal of disaster risk reduction*, vol. 30, p. 199–215.