

LIREC

Lettre d'information sur les Risques et les Crises

N°65 - FÉVRIER 2022

DOSSIER THÉMATIQUE

DÉFIS ACTUELS ET ÉMERGENTS DES GESTIONNAIRES ET SPÉCIALISTES DE CRISE

POINT DE VUE

LES DÉFIS ET LES STRATÉGIES
DE LEADERSHIP
EN GESTION DE CRISE

RECHERCHE

PROJET APRIL
PROGRAMME AGENCE NATIONALE
DE LA RECHERCHE

LIREC

n°65 FÉVRIER 2022



DÉPARTEMENT ÉTUDES ET RECHERCHES

Le département Études et recherches de la direction de la recherche et de la prospective (DIREP), de l'Institut des hautes études du ministère de l'Intérieur (IHEMI) publie la Lettre d'information sur les Risques et les Crises – LIREC

Directeur de la publication :

Éric FREYSSELINARD

Directeur de la rédaction :

Nacer LALAM

Rédactrice en chef :

Cheila DUARTE COLARDELLE

Pour vous abonner,
envoyez-nous un courriel à :
lirec@ihemi.fr

Vous pouvez nous envoyer des
informations concernant un événement,
une manifestation ou
une proposition d'article à :
lirec@ihemi.fr

Suivez nous :



Les informations contenues dans ce document
sont issues de sources ouvertes et ne sauraient être
interprétées comme une position officielle
ou officieuse de ses rédacteurs ou des services
de l'Etat.

ISSN 2265 – 464X



Photo de couverture :
©alphaspirit - stock.adobe.com

ÉDITORIAL

ÉRIC FREYSSELINARD

Préfet, directeur de l'Institut des hautes études
du ministère de l'Intérieur



Depuis sa création en 2009, la LIREC s'appuie sur une veille continue des événements nationaux et internationaux. Son ambition est d'apporter un éclairage pluridisciplinaire, tout en proposant des préconisations destinées à éclairer les parties prenantes, publiques et privés.

Ce 65^e numéro de la LIREC se concentre sur les défis émergents auxquels les gestionnaires et spécialistes des crises devront faire face dans les années à venir.

Le premier article pose la question du renforcement de la crédibilité et de la légitimité de l'autorité publique en temps de crise. Avec la médiatisation quasi immédiate des crises, la communication s'est imposée comme une des composantes essentielles de la gestion de la crise. Lorsque la légitimité du décideur est contestée, la capacité à incarner un message impacte fortement l'efficacité de la gestion de crise. Une fonctionnaire de Défense et de Sécurité, du ministère de la Culture, possédant une riche expérience de terrain, apporte son éclairage à cette problématique.

Le deuxième article, issu du monde de la recherche en milieu industriel, s'interroge sur les modalités d'évaluation d'une gestion de crise. Quatre approches sont proposées afin d'identifier des indicateurs d'évaluation de la performance de la gestion de crise.

Le troisième article porte un regard sur les stratégies de résilience face au scénario d'un dysfonctionnement ou d'une cyber attaque provoquant l'indisponibilité des systèmes d'information en cellule de crise. Il présente des stratégies d'action proposées par un décideur en cybersécurité émanant du secteur privé.

Enfin, le quatrième article permettra d'exposer certains défis auxquels des décideurs sont exposés et des stratégies de leadership possibles en gestion de crise.

Je vous souhaite une excellente lecture et profite de ce message pour rappeler l'importance du partage des connaissances notamment à travers la formation et la recherche afin de faire face aux défis futurs.

Bonne lecture !

4

BRÈVES

14

POINT DE VUE

Les défis et stratégies
de leadership en gestion
de crise

Colonel Pierre DE VILLENEUVE

16

RECHERCHE

Projet ANR APRIL

5

DOSSIER THÉMATIQUE

DÉFIS ACTUELS ET ÉMERGENTS
DES GESTIONNAIRES ET SPÉCIALISTES DE CRISE



- ⑥ Comment renforcer la crédibilité de l'autorité en temps de crise ?
Dominique BUFFIN
- ⑧ La résilience des dispositifs de crise au niveau stratégique face
à la perte des Systèmes d'Information
Marie-Odile CRINON
- ⑪ Évaluer une gestion de crise, l'appel pour une vision cognitiviste
et alter-prospectiviste
Raphaël DE VITTORIS

17

FORMATION

18

AGENDA



LES 10 RISQUES MONDIAUX, ÉMÉRGENTS

(source : *Future Risks Report AXA 2021*)

Cette étude mondiale a analysé l'évolution de la perception des risques émergents selon une double perspective : un panel d'experts en gestion des risques et le grand public, avec plus de 23 000 personnes interrogées.

Les risques liés au changement climatique dominent les préoccupations et constituent les menaces les plus importantes en termes de probabilité et d'impact. L'étude

révèle également une forte inquiétude en ce qui concerne le risque cyber dans un contexte encore marqué par l'accélération de la transformation numérique et une augmentation des cyber attaques. En troisième place se situe le risque de pandémie (premier risque en 2020).

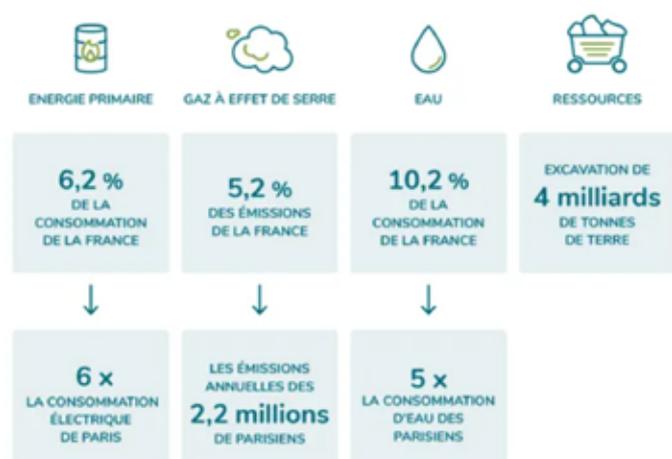
Pour télécharger le rapport : [AXA Future Risks Report 2021 | AXA](#)

LES IMPACTS ENVIRONNEMENTAUX DU NUMÉRIQUE EN FRANCE, EN 2020

(Source : *Rapport « iNum », GreenIT.fr*)

Entre janvier et juin 2020, un groupe d'experts a réalisé l'étude « iNum », publiée en janvier 2021. Cette étude vise à quantifier les impacts environnementaux du numérique en France et à identifier des pistes d'actions adaptées aux spécificités françaises. Pour accéder à ce rapport : <https://www.greenit.fr/wp-content/uploads/2021/02/2021-01-iNum-etude-impacts-numerique-France-rapport-0.8.pdf>

Réduire l'empreinte environnementale du numérique est également l'objet des deux études commandées par une mission d'information du Sénat (2020 et 2021). Pour en savoir plus : [Réduire l'empreinte environnementale du numérique: un état des lieux inédit et une feuille de route pour la France - Sénat \(senat.fr\)](#)





DOSSIER THÉMATIQUE

DÉFIS ACTUELS ET ÉMERGENTS DES GESTIONNAIRES ET SPÉCIALISTES DE CRISE



Comment renforcer la crédibilité de l'autorité en temps de crise ?

par Dominique BUFFIN



À PROPOS DE L'AUTEUR

Dominique BUFFIN

Elle est entrée dans l'administration publique d'État en tant qu'officier de police en 2001.

Après un passage par les services de renseignements, elle rejoint en 2007 la direction centrale de la Police judiciaire, où elle exerce d'abord dans un groupe d'enquête de l'office central de Lutte contre le crime organisé, puis à l'office central de Lutte contre le trafic de biens culturels (OCBC). En 2013, elle est mise à disposition du ministère de la Culture, où elle sera conseillère pour la sûreté des musées de France pendant quatre ans, auprès de la direction générale des Patrimoines.

En juin 2017, elle est nommée haute fonctionnaire de défense et de sécurité adjointe au ministère de la Culture, où elle travaille notamment à la formalisation et à l'amélioration du dispositif de gestion de crise du ministère, et à la formation des fonctionnaires concernés.



CHERCHER LE RENSEIGNEMENT UTILE À LA DÉCISION

La décision peut s'appuyer sur des informations qui ne sont pas forcément partagées par tous, surtout dans le cas d'une crise à cinétique rapide, où le temps de la pédagogie vers les populations cibles est forcément contraint.

Ainsi, plus la décision est étayée par des preuves de renseignements fiables, plus la crédibilité du décideur est augmentée.

Le choix des membres qui composent la cellule de crise, ainsi que des experts qui l'alimentent en renseignements, vont jouer un rôle non négligeable.

Pour un évènement comme un incendie, la responsabilité de la gestion de l'évènement dans les tout premiers temps de la crise incombe logiquement aux pompiers. La police ou la gendarmerie nationales doivent également éventuellement assurer la protection du site afin de réguler la circulation, d'éviter un suraccident... Les services du ministère de l'Intérieur sont donc les services qui dirigent.

Toutefois, si l'incendie touche un monument historique bien suivi et documenté, dans ce premier temps de la crise, les experts comme l'architecte des Bâtiments de France, l'architecte en chef des Monuments historiques, le conservateur des Monuments historiques peuvent apporter un concours non négligeable, notamment sur la façon dont le feu peut être attaqué au regard de l'architecture du bâtiment, ou encore sur la mise en application du plan de sauvegarde des biens culturels (destiné à préparer le sauvetage du patrimoine mobilier le cas échéant).

Au cours des six dernières années, le milieu culturel a été confronté à des crises exceptionnelles en France. Certaines de ces crises étaient sectorielles, multifactorielles, ou souvent transversales : les attentats de *Charlie Hebdo* et ceux du Bataclan en 2015, la crue de la Seine en 2016, la dégradation de sites en 2018 lors de manifestations (l'Arc de Triomphe, le jardin des Tuileries), l'incendie de la cathédrale de Paris et celle de Nantes en 2019, et, depuis 2020, la crise sanitaire, au cours de laquelle il a été interdit aux organismes patrimoniaux et de spectacle vivant d'ouvrir au public, tandis que l'ouverture des archives, des bibliothèques et des lieux d'enseignement culturel était subordonnée à des règles sanitaires rigoureuses.

La crise relative à la pandémie de COVID-19 a démontré une grande capacité d'adaptation et une forte plasticité des professionnels de la culture, en ce qu'ils ont accepté les nouvelles règles et les ont mises en application. Ainsi, ils ont su inventer des substituts aux offres culturelles qu'ils proposaient auparavant, et adapter des solutions existantes.

Une mesure comprise est une mesure qui fera moins l'objet de critiques et

dont l'application sera plus aisée car mieux acceptée, et donc plus efficace à court, moyen et long terme.

La crédibilité de l'autorité chargée de la gestion de crise est donc essentielle dans ces périodes où les décisions doivent se prendre rapidement, avec des temps de consultation réduits.

La crédibilité, le crédit ou encore la confiance accordée par la population à l'autorité qui gère la crise ne se décrète pas.

De plus, dans la mesure où la crise est un déséquilibre, et qu'elle est considérée comme une anomalie par la population, le crédit disponible d'une autorité auprès d'une population va nécessairement se dégrader.

Comment renforcer cette crédibilité pour faciliter et rendre plus efficace la gestion de crise ?

Il nous semble que cette crédibilité peut être travaillée et remise en question au cours des trois étapes suivantes : la recherche du renseignement utile à la décision, la communication sur la décision et la mise en application de la décision.

Ce sont également les professionnels du patrimoine qui seront capables de déterminer le temps nécessaire aux travaux de restauration, les problématiques du chantier à venir et ses éventuels chausse-trapes. Ce sont ces experts que le gestionnaire devra savoir écouter pour sortir du cycle de la crise qui ne se clôt pas simplement à l'extinction des dernières braises. La mise en œuvre de leurs conseils permettra éventuellement d'éviter un rebond de la crise.

Le nerf de la guerre de la prise de décision réside dans la fiabilité des renseignements portés à la connaissance du décideur et dans l'écoute que le décideur est capable d'accorder aux responsables qui l'entourent.

Écouter les propositions ne signifie pas qu'elles doivent systématiquement être acceptées. Mais le devoir des participants à la gestion de crise consiste à exposer l'ensemble des solutions et des problématiques pour permettre aux décideurs de prendre une décision de la manière la plus éclairée possible.

JUSTIFIER LES DÉCISIONS ET COMMUNIQUER

Il peut être nécessaire d'exposer les différentes solutions qui se présentent, et d'expliquer pourquoi une décision a été prise plutôt qu'une autre. Par la suite, et pendant tout le temps d'application de la mesure, la communication peut être axée d'une part sur les modalités d'application de la mesure et d'autre part sur les marqueurs d'efficacité de cette dernière.

Si l'exercice peut paraître chronophage, il est nécessaire pour obtenir l'adhésion, même rétroactivement.

La mesure de généralisation du passe sanitaire au mois de juillet 2021 aux musées, aux spectacles enregistrés (cinémas), puis au mois d'août à d'autres entreprises comme les restaurants, a pu faire l'objet de critiques de la part du grand public. Elle a notamment provoqué des manifestations qui ont rassemblé entre 150 000 et 200 000 personnes au plus fort de l'été dans le courant du mois d'août.

La communication relative à la mise en application de cette mesure s'est faite en plusieurs temps et sur plusieurs aspects :

- Le président de la République annonce le 12 juillet que le champ d'application du passe sanitaire, réservé jusqu'alors aux événements culturels et sportifs de plus de 5 000 personnes, va être largement étendu à compter du 21 juillet pour les activités pour lesquelles cette possibilité est déjà prévue par la loi, puis début août pour d'autres (après intervention du législateur).

L'objectif assumé et communiqué était d'encourager fermement à la vaccination, comme seule solution contre une nouvelle augmentation des contaminations.

Si un peu plus de 60 millions de doses avait été administrées à cette époque, le rythme de vaccination risquait de ralentir en raison des vacances d'été. D'autre part, étant donné l'augmentation des chiffres de contamination, il fallait convaincre rapidement les personnes qui, sans être opposées à la vaccination, restaient indécises quant au fait d'effectuer cette démarche pour elles-mêmes.

- Dans les jours et les semaines qui ont suivi, les ARS ont travaillé à mettre en place des centres de vaccination dans des lieux de vacances des Français (y compris mobiles comme sur le Tour de France), afin de permettre à ces derniers de bénéficier d'une ou deux injections loin de leur domicile. Ces démarches ont, là encore, fait l'objet de publicité.

Au fil de l'été, de nombreux reportages sur les modalités d'application du passe dans les différents établissements qui y étaient soumis ont été diffusés.

- Fin septembre, le chiffre de 90 millions de doses de vaccins administrées en France était atteint, et le chiffre symbolique de 50 millions de personnes primo-vaccinées a été dépassé au milieu du mois.

Les contaminations sont en baisse depuis le mois d'août, ainsi que le nombre d'hospitalisations.

Ces chiffres ont été communiqués au grand public pendant l'été, les activités qui avaient été empêchées ou affectées par les trois premières vagues épidémiques ont pu se poursuivre, et les manifestations contre le passe sanitaire rassemblent un nombre toujours décroissant de personnes (moins de 70 000 dans l'ensemble du territoire le 25 septembre).

LA MISE EN APPLICATION DES DÉCISIONS

L'autorité chargée de la gestion de crise est « autorité » notamment parce que c'est à elle qu'incombe la prise de décisions, et c'est elle qui dispose des ressources (financières, matérielles, humaines) pour les faire appliquer.

Enfin, l'exécution d'un ordre, d'une commande d'une autorité, constitue une preuve en elle-même que cette dernière a autorité sur ses troupes.

Le temps de la crise est d'autant plus une période de test de l'autorité que la décision doit être appliquée dans l'urgence.

Lorsque la décision est étayée par des renseignements que l'on estime crédibles, l'annonce de la décision aux populations cibles doit se faire rapidement, **dès lors que la certitude qu'elle pourra être mise en application est acquise.**

La problématique à ce stade est moins l'adhésion à la mesure qu'il faut obtenir auprès du grand public que la conviction que les services qui doivent la mettre en œuvre ont compris la commande, sont capables de l'expliquer aux populations cibles et sont appuyés par d'autres services/administrations/structures qui contrôleront sa mise en œuvre.

La décision et son annonce doivent absolument être suivies d'effet si l'autorité souhaite conserver sa crédibilité.

En d'autres termes, l'annonce d'une mesure contraignante que le responsable de la gestion de crise assume peut être de nature à renforcer son autorité, si les moyens mis en œuvre permettent à cette mesure d'être bien appliquée ■

La résilience des dispositifs de crise au niveau stratégique face à la perte des systèmes d'information

par Marie-Odile CRINON



À PROPOS DE L'AUTEUR

Marie-Odile CRINON

Diplômée de l'EPF école d'Ingénieurs et du Churchill College-Cambridge University, Marie-Odile Crinon a eu pendant plus de vingt-cinq ans des responsabilités de management chez IBM, puis chez Devoteam.

En 2014, elle crée MRC2, cabinet de conseil spécialisé dans le Management des Risques et Crises Cyber. Elle conseille de grandes entreprises internationales privées et publiques dans le management de risques et de crises en lien avec leur transformation numérique. Elle effectue, pour des comités exécutifs, des directions métiers ou numériques, des missions de sensibilisation au cyberrisque et à la cyberrésilience, des analyses de risques, des exercices de (cyber)crise en France et à l'étranger.

Marie-Odile Crinon est conférencière à Sciences Po Paris (Executive Master), à l'Institut national des hautes études de la sécurité et de la justice (INHESJ/IHEMI), au Forum International de la Cybersécurité (FIC).

Elle est administratrice de l'EPF école d'Ingénieurs et de l'école de l'air et de l'espace. Marie-Odile Crinon est auditrice de l'IHEDN et de l'INHESJ/IHEMI et colonel de réserve citoyenne de la cyberdéfense et de l'armée de l'air.

www.mrc2.fr

<https://www.linkedin.com/in/marie-odile-crinon-349b1b1b/>



Ces cyberattaques peuvent avoir des conséquences redoutables pour les entreprises, les administrations, les hôpitaux... Comment gère-t-on une cybercrise ?

Sidération ! C'est le premier mot qui me vient à l'esprit quand on est confronté à une cyberattaque. C'est toujours un choc de voir ces écrans noirs partout, avec un message indiquant que vos données ont été chiffrées. Rappelez-vous le témoignage du directeur général de TV5 Monde !

Il faut néanmoins rapidement organiser le dispositif de crise avec ses composantes stratégique et opérationnelle pour avoir la capacité de traiter tous les aspects d'une crise d'origine cyber.

La difficulté principale est de prendre des premières décisions très rapidement, alors que l'incertitude est très grande sur la nature et l'étendue de l'attaque, ainsi que sur la motivation des attaquants. La fameuse « *golden hour* »... Il s'agit d'éviter – si possible – de propager la contamination à l'intégralité des systèmes d'information de l'entreprise (et de ses partenaires), et donc d'accepter de s'isoler numériquement en coupant les flux. Décision difficile !

Les investigations techniques, qui peuvent prendre plusieurs jours, sont placées sous la responsabilité de la composante opérationnelle du dispositif de crise. La cellule de crise stratégique doit, elle, qualifier les impacts de l'attaque non seulement sur

Votre cabinet est spécialisé dans le Management des Risques et Crises Cyber. Comment analysez-vous l'évolution de la menace cyber ?

Nous vivons dans un monde de plus en plus numérisé. Plus de 4 milliards d'utilisateurs sont actifs sur les réseaux sociaux ! La pandémie a imposé un recours massif au télétravail et a donc favorisé le développement des cyberattaques grâce à une ouverture plus importante des systèmes d'information. Le nombre d'interventions de l'ANSSI (Agence nationale de sécurité des systèmes d'information) a ainsi été multiplié par quatre en 2020. La cybercriminalité est

devenue plus lucrative que le trafic de drogue, grâce à la revente de données volées ou au paiement de rançons, sans oublier bien sûr l'espionnage ou la déstabilisation d'États.

Et la menace de demain sera le cyberterrorisme avec des attaques contre des moyens de transport ou des producteurs d'énergie, comme l'attaque d'une station d'eau potable en Floride en février 2021.

La question aujourd'hui pour une entreprise ou une administration n'est plus « serai-je attaqué », mais « quand serai-je attaqué » et « suis-je prêt à poursuivre mes activités critiques en cas de cyberattaque ? »

les activités de l'entreprise, mais aussi sur sa réputation, sur ses engagements, dont le respect de certaines législations comme la loi de programmation militaire (LPM) ou le règlement général sur la protection des données (RGPD), et prendre les décisions nécessaires à sa survie. Chaque année des PME disparaissent à cause d'une cyberattaque.

Le dispositif de crise doit se structurer pour partager dans la durée son temps et ses ressources entre continuité d'activité et restauration du système d'information (qui peut prendre plusieurs mois). La priorisation des activités essentielles est toujours un exercice délicat pour la cellule de crise stratégique.

La perte du système d'information liée à une cyberattaque provoque des difficultés particulières en gestion de crise. Pouvez-vous nous éclairer sur ce point ?

Effectivement! Qu'il s'agisse d'une cyberattaque ou d'une panne informatique, la perte du système d'information est un élément primordial de déstabilisation, complexe à illustrer dans les travaux préparatoires de gestion de crise et de continuité d'activité.

Le numérique est partie intégrante de nos vies professionnelle et personnelle. Plus de système d'information signifie plus de télétravail, plus d'Internet, mais aussi plus de téléphonie, point souvent omis dans la cartographie des risques. Gérer une crise dans une entreprise ou dans une administration sans outil de communication professionnel est un exercice complexe... Le recours à des SMS ou à des groupes WhatsApp devient alors la pratique courante malgré le risque lié à la confidentialité des échanges (et encore faut-il avoir un annuaire des contacts intègre et disponible).

De même, la restauration du système d'information sans sauvegarde des données (au moins des données les plus stratégiques, qu'elles soient techniques ou fonctionnelles) dans un lieu sûr – électronique et/ou physique – reste encore un problème d'importance aujourd'hui en cas de cyberattaque.

Stratégiquement, comment se traduit cette perte de système d'information?

La cellule de crise stratégique a dans un premier temps deux priorités :

- Communiquer : au sein du dispositif de crise, avec les collaborateurs, les clients, les fournisseurs, les partenaires, les autorités, les régulateurs, les médias... la liste est longue !
- Poursuivre les activités essentielles de l'organisation, même en mode dégradé.

Cela requiert à la fois des capacités de communication – donc des outils externalisés que les dirigeants peuvent prendre en main aisément – et des plans de continuité d'activité (PCA) préparés en amont et soutenus si possible par des capacités informatiques en dehors de l'organisation. Ou, à défaut, par des outils plus simples, comme parfois le papier et le crayon ou le fax.

Plus tard, il s'agira d'étudier les options de restauration ou de reconstruction du système d'information et de faire des choix toujours délicats entre temps d'indisponibilité et risques résiduels (comme l'intégrité des postes de travail ou des données).

Peut-on anticiper ce risque ? Quelles sont, selon vous, les bonnes pratiques ?

Oui, bien sûr, même si on ne peut jamais imaginer le scénario exact de l'attaque.

Il faut travailler en amont avec les équipes pour identifier leurs activités essentielles, leurs données critiques. On pourra ainsi placer ces données dans un coffre-fort externe (sans oublier de les mettre régulièrement à jour) et pour chaque activité décrire un éventuel plan B. Cette liste permettra également d'établir un ordre de redémarrage lors de la restauration du système d'information.

Certaines organisations, mieux préparées, ont anticipé la perte de tous les composants du système d'information. Elles ont par exemple souscrit des abonnements chez

des fournisseurs de solutions de visioconférence, d'outils de gestion de crise (main courante, plan d'action), de messagerie de substitution, de centres d'appels, de sites Web... Elles peuvent ainsi mieux piloter la crise grâce à une communication plus aisée avec les parties prenantes, et faciliter le redémarrage de leur capacité informatique.

Comment ces recommandations s'articulent-elles avec les travaux actuels de cyberrésilience des administrations et des entreprises ?

Alors que la cybersécurité met l'accent sur la protection du système d'information, la détection d'attaques ou la sensibilisation des utilisateurs, la cyberrésilience offre une vision plus globale et décalée de réponse à la menace cyber. Il s'agit de prévoir la résilience des activités de l'entreprise ou de l'administration, et d'assurer dans les meilleurs délais la restauration de capacités informatiques intègres. On comprend mieux ce défi en se rappelant les attaques comme NotPetya en 2017, qui a contraint des entreprises à reconstruire le socle de milliers de postes de travail, chantier titanesque. Ou, plus récemment, un grand laboratoire pharmaceutique a dû arrêter tout son système informatique (y compris dans ses usines), pour reconstruire un système propre, opération qui prend en moyenne deux mois. On pourrait également évoquer les récentes attaques contre des hôpitaux contraints de fermer des lits, de transférer des patients, de retarder des interventions.

Ces exemples démontrent la nécessité de travailler sur la cyberrésilience de l'organisation en intégrant le scénario d'indisponibilité des systèmes d'information tant pour piloter la crise et assurer la continuité de l'activité que pour restaurer – si ce n'est reconstruire – les capacités informatiques. Cela requiert, selon moi, l'implication forte des dirigeants, un poste budgétaire dédié, la sensibilisation accrue des collaborateurs et des agents pour qu'ils anticipent cette situation très dégradée et s'entraînent régulièrement grâce à des exercices de cybercrise. C'est une obligation annuelle dans certaines entreprises.

La cyberrésilience n'est pas qu'une affaire technique et de direction informatique ! Loin de là... Les conseils d'administration nous sollicitent maintenant pour les aider à intégrer ce sujet dans leurs travaux.

Peut-on imaginer que la résilience des dispositifs de crise stratégiques soit prochainement intégrée à la quantification du risque cyber imposée par des donneurs d'ordre ou des assureurs ?

Le *cyber rating*, ou « quantification du risque cyber », est un sujet en plein développement. On voit ainsi de grands donneurs d'ordre de l'industrie imposer à leurs sous-traitants une démarche de notation

cyber. En fonction du score, ils peuvent décider de ne plus consulter certaines entreprises lors d'appels d'offre ou de les éliminer de leur liste de « *preferred partners* ». Même si l'évaluation se fait encore souvent en mode déclaratif, on perçoit un durcissement dans la démarche. On retrouve les mêmes mécanismes chez certains assureurs lors de la souscription d'une police de cyberassurance, comme de votre police automobile d'ailleurs. Les critères de *cyber rating* sont nombreux, de la mise en œuvre d'outils et de procédures de protection de Système d'Information, de détection d'évènements jusqu'aux séances de sensibilisation des collaborateurs ou des agents aux bonnes pratiques de cybersécurité. La structuration, l'équipement, l'entraînement du dispositif de réaction à la cyber-attaque, donc de pilotage de cybercrise, sont des composants

de l'évaluation de la maturité cyber d'une organisation, entreprise ou administration.

On voit donc s'opérer dans la quantification du risque cyber un mouvement de prise en compte de la résilience des dispositifs de crise au niveau stratégique.

Le développement exponentiel du numérique repose sur la confiance de toutes les parties prenantes et impose donc des contrôles comme le *cyber rating* pour assurer une meilleure résilience de nos activités et, plus globalement, de notre pays ■

Évaluer une gestion de crise, l'appel pour une vision cognitiviste et alter-prospectiviste

par Raphaël De VITTORIS



À PROPOS DE L'AUTEUR

Raphaël De VITTORIS

Après une carrière internationale dans le secteur de l'hygiène, la sécurité et l'environnement, il est le gestionnaire de crise du Groupe Michelin depuis 2013. Il est aussi enseignant et chercheur en sciences de gestion sur les problématiques de gestion de crise, gestion des risques, communication de crise, négociation de crise et biais cognitifs en situation de crise. Docteur en sciences de gestion et qualifié maître de conférence, diplômé d'un master en physiologie en environnement extrême, d'un master en administration d'entreprise et d'un master en hygiène, sécurité et environnement, il enseigne dans divers masters et il est membre du board de l'Institut d'études des crises et d'intelligence économique et stratégique. Il est l'auteur de *Surmonter les crises*, paru en 2021 aux éditions Dunod et le fondateur d'Antifragile.fr



INTRODUCTION

L'actualité récente a rendu le concept de crise omniprésent dans les esprits. La gestion de crise fait désormais partie des fondamentaux de la plupart des organisations. Comme pour tout processus, il est naturel de s'interroger sur les indicateurs permettant à l'organisation de le suivre et de le piloter.

Or, il semble difficile aux organisations, pourtant rompues à l'art du suivi et du pilotage, de quantifier avec précision les niveaux de performance en gestion de crise. Cette difficulté pourrait selon nous être le fruit d'une imprécision quant à l'angle de conceptualisation de la gestion de crise même.

Après analyse de la littérature scientifique et des approches de diverses organisations, quatre grilles de lecture différentes des crises semblent émerger avec autant de voies d'évaluation de ce qu'est une « bonne » gestion de crise. Nous proposons de passer en revue ces quatre approches et d'en tirer des indicateurs potentiels.

UNE APPROCHE CLASSIQUE, LARGEMENT DÉPENDANTE DU RETOUR D'EXPÉRIENCE

L'évaluation des crises la plus fréquente repose sur une conception classique des crises où l'évènement est considéré par ses manifestations extérieures : ses conséquences. Cette approche est la plus intuitive, donc la plus aisée à appliquer. Les conséquences peuvent en effet se quantifier en nombre de victimes, en coûts, en nombres de références médiatiques ou de *posts*. C'est cette approche qui fournit *a priori* les données objectives les plus solides, car elles sont directement issues des constats.

On peut alors avoir la tentation de comparer les crises par leurs conséquences. Pourtant, dès les

premiers rapprochements, la comparaison n'est pas si évidente. Quelle crise fut-elle *réellement* la plus grave : Tchernobyl ou Fukushima ? Le Bataclan ou *Charlie Hebdo* ? Katrina ou Hugo ?

Les analystes de la crise admettent pourtant qu'à peu de choses près, les conséquences des crises affrontées auraient pu être tout autres pour une gestion pourtant totalement identique. La chance, le sort, la fatalité sont autant de facteurs qui viennent influencer les conséquences parfois de manière bien plus considérable que toutes les mesures proposées par les cellules.

Dans ce cas comment interpréter les indicateurs ? Sont-ils représentatifs de la gestion effectuée ? Doit-on y inclure un quotient de chance ? Une gestion maladroite mais heureuse doit-elle susciter davantage de reproduction ultérieure qu'une gestion habile mais malchanceuse ?

Une seconde approche classique consiste à qualifier les composantes de la gestion aux niveaux techniques, organisationnel et humain (approche TOP). Un tel diagnostic, plus structurel et moins opérationnel que l'approche précédente, permet de segmenter des familles d'éléments pour identifier avec davantage de finesse les forces et les faiblesses de la structure. Cependant, il amène à multiplier les indicateurs évaluant les moyens (fiabilité, disponibilité, maîtrise, etc.), l'organisation (simulations, etc.) et les personnes (formations, etc.). Certains auteurs ajoutent à ces paramètres l'influence de la culture

de l'organisation et la psychologie des décideurs¹.

Cette approche classique, qu'elle se fonde sur les conséquences pures ou les éléments structurels du dispositif de gestion de crise, a l'avantage de fournir des données et de permettre une interprétation rapide de l'évènement. Toutefois, après autant d'années d'évaluation des crises multiples ayant fait l'objet d'analyses fines et de retours d'expériences détaillés, comment expliquer les fiascos retentissants des plus grandes crises qui secouent notre quotidien ?

Indicateurs de constat possibles : nombres de victimes, effet médiatique, nombre de posts, coûts, réactions des employés, impact psychologique, qualité des interactions dans la cellule, alignement des visions et des interprétations, etc.

ÉVALUATION PSYCHO-STRUCTURELLE

La littérature scientifique en sciences de gestion offre cependant des pistes intéressantes inspirées des sciences cognitives avec deux approches apparemment globalement similaires mais reposant sur des principes contraires. Elles abordent la notion de gestion de crise par la conceptualisation du phénomène de crise et l'influence de cette abstraction sur les décisions au niveau individuel ou collectif.

D'une part, le *decision-making* tel que développé par March² est une approche qui se base sur le présupposé que la réflexion précède l'action. Ce concept implique un phénomène de collecte et d'interprétation des données disponibles permettant ainsi une anticipation des conséquences. Dans ce cas, le processus décisionnel collectif est comparable à « la présence d'un

choix calculé entre les alternatives³ ». La gestion de crise est alors le fruit de décisions, les décisions sont le fruit de calculs d'alternatives, les alternatives sont le fruit d'analyses, les analyses sont le fruit d'une collecte et d'une interprétation des données. Le processus repose d'abord sur des modèles abstraits et conceptuels (principes, références à des situations similaires, valeurs et culture de l'organisation et du décideur, etc.), le plus souvent personnels, où les ancrages, les influences, les heuristiques et les autres biais cognitifs posent les limites de la rationalité des choix. L'idée précédant l'action, l'idée biaisée entraînera nécessairement une action peu pertinente.

D'autre part, le *sensemaking* tel que développé par Weick⁴, au contraire, considère que c'est bien l'action initiale qui nourrit la pensée en permettant une interprétation collective cohérente de la cellule de crise. Au moyen de l'analyse de catastrophes célèbres (Mann Gulch, Bhopal, etc.), il propose un « passage de la prise de décision au sens » en étudiant la création de sens. Une des particularités de cette approche est de considérer le processus de *sensemaking* d'abord comme un processus collectif et distribué qui repose sur des identités partagées ; ce qui le distingue du processus de *decision-making* inspirée par le choix rationnel et voyant son centre d'analyse dans l'esprit de l'individu. Selon une approche *sensemaking*, le décideur n'œuvre pas seul mais se réduit à un composant d'un collectif (la cellule de crise), dont l'action immédiate permet la réflexion et l'interprétation de la situation en vue d'un ajustement perpétuel (par bricolage) et d'une progression de la pertinence. Les influences, les heuristiques et les biais cognitifs peuvent alors être gérés de manière collective et l'organisation peut même en tirer bénéfice si cela permet une interprétation collective cohérente plus pertinente.

Indicateurs psycho-structurels possibles : succès/insuccès des alternatives choisies, collégialité des décisions, compréhension collective commune des évènements, présence/absence de points de situations réguliers, etc.

UNE APPROCHE ORGANISATIONNELLE OFFRANT DES DIMENSIONS NOUVELLES D'ÉVALUATION

Selon une vision d'abord organisationnelle de l'évènement, l'efficacité du pilotage peut être considérée comme la bonne réalisation des différentes missions devant être réalisées au sein de la cellule de crise. En effet, face à l'impossibilité d'embrasser la pluralité des évolutions et des dénouements potentiels d'une crise, il est possible d'admettre l'impossibilité de déterminer si les décisions prises ont été judicieuses ou non. L'évaluation de résultat étant impossible (car relevant uniquement du constat), les organisations peuvent se rabattre sur un résultat d'organisation. Il est alors possible de découper les missions de la cellule de crise en fonctions principales et d'évaluer le bon fonctionnement des différentes missions. Ces missions peuvent être découpées en cinq fonctions principales :

- Le leadership, dont la mission principale de prendre des décisions et de rendre des comptes aux reste de l'organisation.
- L'anticipation, dont la mission de fournir des éléments de projection qui permet de disposer d'un temps d'avance sur les évènements.

.....

(1) Mitroff, I. et Anagnos, G. (2001), *Managing Crises Before They Happen. What Every Executive and Manager Needs to Know about Crisis Management*, New York, Amacom, 2001.

(2) March, J. G. (1978), « Bounded rationality, ambiguity, and the engineering of choice », *The Bell Journal of Economics*, 9, p. 587-608 ; March, J. G. (1982), « Theories of choice and making decisions », *Society*, 20, 29-39 ; March, J. G. (1994), *A primer on decision making: How decisions happen*, New York, Free Press ; March, J. G. (2006), « Rationality, foolishness, and adaptive intelligence », *Strategic Management Journal*, 27, p. 201-214.

(3) Schulz, M. (2014), *Logic of consequences and logic of appropriateness*, in M. Augier et D. Teece (dir.), *Palgrave Encyclopedia of Strategic Management*, Londres, Palgrave Macmillan, p. 1-6.

(4) Weick, K. E. (1993), « The collapse of sensemaking in organizations. The Mann Gulch disaster », *Administrative Science Quarterly*, 38, p. 628-652 ; Weick, K. E. (1995), *Sensemaking in Organizations*, Thousand Oaks, Sage ; Weick, K. E. (1996), « Drop your tools. An allegory for organizational studies », *Administrative Science Quarterly*, 41, p. 301-313 ; Weick, K. E. (2010), « Reflections on enacted sensemaking in the Bhopal Disaster », *Journal of Management Studies*, 47, p. 537-550 ; Weick, K. E., Sutcliffe, K. M., et Obstfeld, D. (2005), « Organizing and the process of sensemaking », *is 16*, p. 409-421.

- La facilitation, dont la mission de fluidifier le fonctionnement de la cellule de crise et d'en assurer la pérennité (fonctionnement longue durée).
- L'intervention, dont la mission principale est d'intervenir sur le terrain.
- La communication, dont la mission est de fournir un plan de communication couvrant les parties prenantes internes et externes

Indicateurs organisationnels possibles : *type de leadership développé, fourniture de scénarios de rupture pour l'anticipation collective, survenue des développements de la crise anticipée, langage et codes communs, interprétation commune, manque de moyens, capacité d'intervention, prise en compte/négligence de la communication interne, existence/absence d'un plan de communication, etc.*

ÉVALUATION ALTER-PROSPECTIVISTE

Dans l'approche précédente, nous avons souligné que l'évaluation de résultat est impossible en gestion de crise puisque les conséquences observées ne relèvent que du constat et ne peuvent être comparées aux conséquences possibles mais n'étant pas (par définition)

survenues. La recherche probabiliste permet toutefois de contourner cette apparente impossibilité factuelle. Des outils probabilistes peuvent modéliser des trajectoires d'évènements. En effet, des logiciels comme « Monte Carlo » sont couramment utilisés pour mesurer les champs des possibles. Une telle approche permet ainsi de comparer une situation réelle face à la multitude des situations possibles et ceci de manière statistique. Si une telle approche a peu de sens pour les gestionnaires de crises à cinétiques très rapides et à portée réduite, elle prend en revanche pleinement son sens pour les organisations ayant à affronter des mégacrisis couvrant des échelles spatio-temporelles très vastes (comme la pandémie de Covid-19 de 2020 ou l'éruption de l'Eyjafjöll en 2010). Si les entreprises peuvent difficilement tirer un bénéfice immédiat de telles approches au vu de leur implication dans la gestion de crises à magnitudes plus faibles, des organisations étatiques ou supraétatiques pourraient en revanche revoir leur approche de la gestion de crise en ce sens. L'évaluation alterprospectiviste offre ainsi une perspective nouvelle à l'anticipation et donc à la prise de décision de la cellule de crise.

Indicateurs de trajectoire possibles : *Enchaînements d'évènements les plus extrêmes, pattern d'enchaînements d'évènements les plus récurrents, présence/absence de boucle d'auto-alimentation des évènements, etc.*

CONCLUSION

La plupart des organisations publiques et privées sont familières d'une approche classique avec retour d'expérience (malgré leurs biais caractéristiques susceptibles d'en déformer significativement les conclusions⁵) qui offrent des indicateurs de constat.

Toutefois, de nombreux acteurs s'accordent à constater que ces outils d'évaluation sont insuffisants pour qualifier les dynamiques psycho-structurelles, organisationnelles ou alterprobabilistes des gestions de crise et piloter le progrès.

Une approche « *blended* », en mesure de proposer des indicateurs variés combinant des approches complémentaires, permettrait peut-être une qualification plus pertinente des gestions. Une telle approche ouvrirait à de nouvelles perspectives dans une discipline où les organisations ne doivent plus se contenter de « se préparer à être surprises » mais plutôt assumer pleinement le fait qu'elles le seront ■

.....

(5) De Vittoris R. (2021), *Surmonter les crises. Idées reçues et vraies pistes pour les entreprises*, Paris, Dunod.



POINT DE VUE

LES DÉFIS ET LES STRATÉGIES DE LEADERSHIP EN GESTION DE CRISE

par le Colonel Pierre Le BASTART de VILLENEUVE



Colonel Pierre Le Bastart de Villeneuve

Actuellement à l'État-Major des armées / Inspection des armées / chef de la division de l'audit interne.

Commandant des formations militaires de la sécurité civile à Paris (20^e) 2017-2020.

Chef du centre opérationnel interministériel de la sécurité civile (COGIC) – 2012- 2017.

Officier des formations militaires de la sécurité civile, soldat de l'infanterie, ancien chef de corps du 7^e régiment d'instruction et d'intervention de la sécurité civile (RIISC) de Brignoles et chef du centre opérationnel de la DGSCGC de juillet 2012 à juillet 2016, j'ai pu expérimenter à quel point la question du leadership reste et doit rester un sujet complexe et étendu. Pour faire face et réussir, il est nécessaire de s'appuyer sur son expérience, de se connaître (qualités et défauts), d'assurer une méthode pour obtenir un travail adapté et adaptable. Et après plusieurs années, il s'agit aussi de croire à sa chance, voire de la provoquer !

Sans chercher à fixer ici définitivement les règles ou les moyens d'action, tant le sujet est complexe, je peux proposer, très modestement, quelques axes de réflexion permettant à chacun d'appréhender avec intelligence et professionnalisme une façon de faire face aux défis de la gestion de crise.

L'expérience acquise lors des opérations civiles et militaires, à l'étranger ou en France, de façon inopinée ou planifiée, au niveau tactique ou politique, conduit à envisager plusieurs axes de stratégies. Il s'agit d'abord de bien définir sa mission : faire face à un ou plusieurs événements qui bouleversent, plus que d'habitude, le climat ou la vie quotidienne dans laquelle s'accomplissent les missions de sa structure et de « jouer son rôle ». Je n'aborde pas volontairement la notion de *sensibilité particulière*, qu'elle soit politique ou médiatique. Le professionnel reste dans le champ de l'analyse opérationnelle « froide et précise ». Il laisse volontairement et clairement cette « sensibilité » s'exercer par d'autres spécialistes qui viennent automatiquement affecter son champ.

Les points suivants seront successivement développés. Il s'agit de comprendre sa *liberté de manœuvre* et son champ

d'action, puis de *préparer l'équipe* disponible au scénario le plus difficile pour acquérir des *mécanismes communs* et, enfin, de se ménager régulièrement (et pratiquement) le *temps de réflexion* indispensable à la prise de décision et à son exécution. Il s'agit surtout, et de plus en plus, de *s'armer du courage* nécessaire à la décision qu'impose l'analyse toujours plus rapide et risquée d'une situation.

IDENTIFIER SON CHAMP DE MANŒUVRE

Quelle que soit l'entité engagée dans la crise (détachement, centre opérationnel, réservoir de force...), il existe des contraintes qui limitent la liberté d'action ou de réaction. Par exemple, dans un détachement opérationnel comme celui de la Chine en 2008, le chef de mission doit « coller » à son autorité directe pour suivre les informations et apprécier les emplois tactiques de son détachement. Sa liberté de mouvement est réduite mais sa position « au plus près » facilite l'engagement tactique sur le terrain.

Dans un cadre interministériel, l'unanimité des décisions est souvent recherchée. Cependant, la crise exige toujours des engagements directs et rapides de première urgence. Cette liberté d'engagement doit être acceptée et comprise même au plus haut niveau. Il s'agit alors de laisser chaque échelon jouer son rôle et d'informer ou de rendre compte (le plus régulièrement possible et en termes compréhensibles) à l'autorité, qui dispose alors d'éléments de langage qui la rassurent devant son chef ou l'opinion publique. Cette liberté de manœuvre correspond aussi à une prise de responsabilité personnelle sachant assumer une partie des décisions et sachant les expliquer de différentes manières en fonction des interlocuteurs. Décider, présenter et expliquer.

Il est évident qu'avec l'expérience et le récurrence des crises (exemple des inondations de 2016), les mécanismes sont plus connus, les décisions mieux comprises et la liberté permise plus importante, surtout si le pouvoir en place n'a pas trop changé. Cela est apparu très clairement lors des campagnes « feux de forêt d'hiver » en Corse à partir de 2016. D'abord lent à mettre en place, le renforcement immédiat des moyens « feu de forêt d'hiver » est devenu un mécanisme opérationnel normal, comme lors des feux en été.

Cependant, cette liberté d'action est subordonnée à certains mécanismes de conduite permettant de conserver la capacité à anticiper et à prendre le « temps d'avance ».

PRÉPARER SON ÉQUIPE

Toute gestion de crise passe par la constitution d'équipes de crise. Personne, ni aucun organisme, ne peut prétendre régler une crise à lui seul. Nos organisations et nos capacités de travail horizontales imposent le travail en équipe ou en pool spécialisé. Ce travail ne s'improvise pas et passe par des processus, surtout lorsque les cultures sont différentes et la compréhension des enjeux éloignés. Ce n'est pas au moment de la crise, de la tension, des difficultés, ou dans la douleur que se constitue une capacité de travail immédiate. Parfois, bien au contraire, le choc des cultures contribue à amplifier les crises. Il est indispensable de préparer l'équipe avec des formations et des entraînements réguliers.

Pourtant, dans un centre opérationnel comme le COGIC, tout pousse à ne pas le faire (rythme, rotation des gardes, disponibilités, crises...). Il s'agit alors de tout faire pour s'entraîner très régulièrement, en particulier dans la capacité à monter en puissance. Passer d'un centre de veille suivant une actualité à froid à un centre de coordination à chaud ne s'improvise pas. Lors des attentats de Paris en novembre 2015, le COGIC est monté en puissance en deux heures avec renforcements et premières productions, alors même que le chef du COGIC quittait le stade de France pour rejoindre la place Beauvau ! À son arrivée, le premier document de synthèse était présenté selon le formalisme éprouvé lors des séances d'entraînement mensuelles.

Ces entraînements sont aussi le moyen de connaître chacun, de trier ou de positionner les individus selon leurs capacités ou leur façon de travailler en équipe. Le mot « discipline » prend alors toute sa force car il s'agit d'abord et surtout de créer une conduite commune s'appuyant sur une vision commune, décidée par le chef, de la crise en développement. Chaque étape, chaque document est accepté par chaque individu, ce qui permet d'engager une véritable action coordonnée.

Pour illustrer ce propos, je me permets un aparté sur l'emploi des téléphones personnels lors des attentats de Paris. L'existence de telles sources d'information a rendu difficile dès les premières heures le traitement des informations, car chaque téléphone constituait une nouvelle intrusion ou une perturbation dans les premières actions réflexes. J'ai même fermé BFM TV au sein du COGIC pour reprendre la main sur le fonctionnement de l'équipe, dont certains membres étaient choqués, bien qu'ils soient en sécurité.

PENSER, RÉFLÉCHIR ET DÉCIDER

La crise vient bouleverser tous les temps de la réflexion et incite à prendre ou à proposer des décisions rapidement et de façon désordonnée. La crise impose son rythme. Tout l'art consiste à prendre le pas sur le rythme de la crise pour y imposer le plus possible la coordination, la logique et l'action, seuls gages d'efficacité pour revenir, à terme, à une situation stabilisée.

Par nature, la crise bouscule les cadres, les structures ou les limites habituelles ; tout l'effort intellectuel et l'organisation visent à rétablir un équilibre pour permettre à tous de reprendre pied et, surtout, de réagir. L'existence de plan, de mécanismes ou de mesures barrières permettent cette

« reprise en main ». Chacun des acteurs cherche à connaître le rythme nouveau et à s'organiser en toute subsidiarité pour peu qu'il dispose d'un premier plan d'action, d'une intention ou d'une manœuvre. Dans la planification militaire, ce travail est pratiquement automatisé dans chaque centre opérationnel et vise surtout à redonner une cohérence d'ensemble à la réponse alors que l'adversaire a bousculé le premier dispositif.

L'efficacité d'un dispositif de gestion de crise se mesure forcément à sa capacité à redonner du sens et un rythme à ce qui était bousculé ou désorganisé. Cette réflexion est donc organisée et intégrée au sein de la résolution de crise. Ce type de briefing à l'autorité impose une certaine discipline pour laisser parler certains acteurs professionnels avant de se lancer dans la prise de décision. Il est assez fréquent que dans des organisations mal préparées, l'autorité ne laisse pas la parole à ces spécialistes et impose parfois trop vite sa propre sensibilité. Il est courant de voir même la COM prendre la place de l'opérationnel. Le cadre, la forme, le cérémonial donnent sens et rassurent pour permettre de repartir.

EXERCER SON COURAGE

Enfin, la gestion de crise impose à chacun une forme de courage qui permet d'agir ou de réfléchir, sans forcément attendre que le brouillard de la crise se dissipe totalement. Il faut savoir évaluer ce qu'il y a « derrière la colline » sans nécessairement disposer chaque fois d'un paysage précis et certain. L'engagement de détachement sur des tremblements de terre ou des inondations exige des informations ou des précisions, mais ils sont forcément une aide précieuse pour les populations concernées sans pour autant connaître parfaitement et précisément leurs tâches sur le terrain. Le départ d'un détachement peut être déclenché quitte à faire demi-tour s'il s'avère ne pas être nécessaire. Les hommes et les femmes en alerte savent. Il s'agit souvent de gérer la frustration.

Le courage doit aussi s'exercer vis-à-vis de ces autorités qui peuvent attendre un feu vert ou un accord hiérarchique alors même que la structure administrative n'est pas organisée pour répondre rapidement. Combien de fois faut-il s'armer de courage au moment d'interrompre une réunion ou un CODIR pour lancer un détachement ou une action ?

Le courage consiste aussi à dire ce qui n'est pas forcément accepté ou compris. Certains départs interviennent dans des circonstances politiques où le corporatisme l'emporte sur l'efficacité ou la rapidité. Il est ce moment où le chef se sent seul et accepte de ne pas être suivi dans ses propositions. Faire des propositions est déjà un courage essentiel car il permet une première réaction, qu'elle soit positive ou négative. Un compte rendu sans proposition est une faiblesse. Nous avons appris très jeunes : « Je suis, je fais, je demande. »

Enfin, la crise passée, le courage est aussi de prendre le temps de faire le retour sur expérience pour améliorer vraiment ce qui peut l'être et confirmer ce qui fonctionne. Cette phase tombe souvent dans l'oubli et empêche l'amélioration des dispositifs. Or, cette évolution est primordiale pour pouvoir s'adapter à des changements et à des cinétiques de crise de plus en plus rapides et complexes ■



RECHERCHE

PROJET APRIL



Programme Agence Nationale de Recherche (ANR) :

Ouragans 2017 - Catastrophe, risque et résilience

Référence projet : ANR-18-OURA-0001

Date et durée du projet scientifique : juin 2018 – juin 2022 (48 mois)

Optimiser l'Anticipation et la Prise de décision en situation de crises extrêmes pour maintenir la Résilience de la société

Confrontés à des situations de crise de plus en plus nombreuses, complexes et hors normes, faisant peser des risques sur les populations et les enjeux vitaux, les organisations publiques et privées sont confrontées à un défi majeur : « Comment optimiser la prise de décision en contexte d'incertitude et comment anticiper la reconstruction et restauration d'un territoire ? »

Sur la base de la récente crise cyclonique aux Antilles, le projet APRIL mettra en perspective l'impact des décisions prises à chaud, sur la base de connaissances évolutives et partielles, sur le maintien de la résilience du territoire à court terme (résilience d'urgence) et moyen terme (relèvement du territoire). Un accent particulier sera porté sur l'anticipation et la prise de décision sous incertitudes liées aux prévisions météorologiques et aux dimensions socio-économiques du territoire (réseaux vitaux, contexte assuranciel, juridique, tissu économique, précarité des populations, insularité, etc.). Tous les échelons du dispositif ORSEC seront considérés depuis la commune jusqu'au niveau interministériel.

L'objectif du projet étant d'améliorer la capacité d'analyse des acteurs dans leur prise de décision. APRIL poursuivra deux grandes finalités :

- Capitaliser l'expérience d'IRMA, MARIA et JOSE sur la base d'enquêtes pour apporter des recommandations de pratiques et des méthodologies pour mettre en œuvre une anticipation court terme (phase d'urgence) et moyen/long terme (reconstruction du territoire) lors de futurs événements hors norme et améliorer la planification ORSEC ;
- Créer des outils d'aide à la décision (Système d'aide à la prise de décision et représentation des paramètres de décision via la cartographie heuristique) appréciant les différentes composantes de la vulnérabilité d'un territoire, les incertitudes et permettant d'anticiper des mesures transversales de protection et de remédiations afin d'optimiser la résilience court et moyen terme du territoire.

Au-delà de son volet « recherche et développement », APRIL propose de mettre en œuvre dès la réalisation du projet un transfert des résultats vers les acteurs de la sécurité civile et de la gestion des crises. Une mise en situation des personnels en poste sera organisée en fin de projet et permettra notamment de tester la méthode d'anticipation proposée. De manière

plus générale, les résultats du projet APRIL seront largement diffusés auprès des différents organismes de formation des cadres de l'Etat et mis à disposition des pouvoirs publics via le comité de suivi composé de professionnels de la sécurité civile et de la gestion des crises. Ce comité sera le garant que la recherche menée dans le projet APRIL répond aux problématiques opérationnelles et trouve un écho dans la mise en œuvre de mesures concrètes et l'évolution des doctrines.

APRIL est un projet de recherche-action et se positionne à ce titre dans un cadre de développement expérimental.

PARTENAIRES

IHEMI : Institut des hautes études du ministère de l'Intérieur, représenté par Cheila DUARTE COLARDELLE, coordinatrice scientifique du projet

BRGM : Bureau de Recherches Géologiques et Minières, représenté par Sophie LECACHEUX

LATTS : Laboratoire Techniques, Territoires et Sociétés, représenté par Valérie NOVEMBER

EFH : Ecole Française de l'Heuristique, représentée par Frédéric LE BIHAN

POUR EN SAVOIR PLUS

> <https://ihemi.fr/etudes-recherches/projet-de-recherche-anr-april>

> **Publication :**

Chevillot-Miot E., Canovas I., Duarte Colardelle C., Lasio C., November V., Un retour d'expérience graphique sur la crise cyclonique de 2017 aux Antilles, Responsabilité et Environnement, Annales des Mines, avril 2020, http://www.annales.org/re/2020/re_98_avril_2020.html

Canovas I., Chevillot-Miot E., November V., Lasio C., Intégrer l'anticipation dans le processus de décision en situation de crise extrême : de l'événement à la méthode. LIREC, INHESJ, pp. 15-19, N° 60 – octobre 2019.

Chevillot Miot E., et Le GUEDARD M., « Cyber Ouragan et crise climatique augmentée », Mise en perspective des vulnérabilités et dépendances au numérique. LIREC, INHESJ, pp. 22- 29, N° 62 - juin 2020.



FORMATION

10^e SESSION NATIONALE « MANAGEMENT STRATÉGIQUE DE LA CRISE » 2022 – 2023



TÉMOIGNAGES D'ANCIENS AUDITEURS



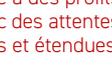
Ecoute, dialogue, professionnalisme, bonne humeur :
une véritable pause de bien-être dans un agenda pro.



La mixité privé/ public, donneurs d'ordres/
consultants a été un des facteurs du succès.



Très grande richesse grâce à des profils
très différenciés avec des attentes
complémentaires et étendues.



INFORMATIONS SUR LE SITE INTERNET DE L'IHEMI



Renseignements :

Didier POULHAZAN

Clara LEBRIS

> formationcrise@ihemi.fr

Tél: +33 (0)1 76 64 89 97
+33 (0)6 47 47 27 76

La neuvième session nationale spécialisée « Management stratégique de la crise » débutera en septembre 2022.

Cette formation d'excellence a pour objectif de permettre aux participants de mettre en place dans leurs structures une politique efficace de gestion des risques et de réponse aux crises.

ORGANISATION DE LA SESSION

✓ Des séminaires mensuels

Leur progression vise à couvrir tous les champs du processus de crise, de la prévention au retour à la normale. Cet objectif intègre l'enjeu majeur d'une coopération et d'une coordination entre pouvoirs publics et acteurs privés.

✓ Des grands témoins

Tout au long de l'année, les séminaires associent de nombreux intervenants qui partagent leurs savoir-faire et leurs expériences sur de nombreuses crises nationales et internationales. Ils échangent avec les auditeurs et apportent leurs conseils pour définir des stratégies et mettre en place une culture de crise pérenne.

✓ Des exercices de crise

Les installations techniques du centre de formation à la gestion de crise du département « Risques et Crises » sont utilisées pour les exercices de mise en situation. Les auditeurs sont ainsi immergés dans des situations de crise réalistes permettant d'appréhender les contraintes de la prise de décision en environnement complexe.

✓ Des visites de centres opérationnels

Elles sont organisées dans des structures nationales (ministérielles, régionales...) ou au sein de sièges de grandes entreprises.

✓ Des travaux de groupe

Les auditeurs sont répartis en plusieurs groupes de travail (GDS : groupes de diagnostic et de stratégies).

PUBLIC

Cette formation s'adresse principalement aux cadres de l'entreprise ou du secteur public ayant en charge la gestion des crises ou étant appelés à participer au sein des cellules dédiées.



AGENDA DU 18/05 > 24/09

18 au 20 mai 2022

Milipol Asie – Pacifique : Salon international sur la sécurité du territoire pour la région Asie-Pacifique

Milipol Asia-Pacifique est consacré au thème de la sécurité intérieure.

Public : Des professionnels, du secteur privé et public, nationaux et internationaux de la sécurité.

Lieu : Sands Expo & Convention Centre (Marina Bay Sands), Singapour

Pour en savoir plus :

[Home - Milipol Asia-Pacific \(milipolasiapacific.com\)](http://milipolasiapacific.com)



24 au 26 mai 2022

Milipol Qatar : 14^e salon international consacré à la sécurité intérieure des Etats, des équipements de Police, de la sécurité des sites industriels et de la protection des populations

Public : Des professionnels nationaux et internationaux de la sécurité

Lieu : Doha Exhibition & Convention Center, Qatar

Pour en savoir plus :

[Milipol Qatar | International Event for Homeland Security & Civil Defence](#)



13 au 17 juin 2022

Eurosatory, 1^{er} salon international de Défense et de Sécurité terrestres et aéroterrestres

Public : Professionnels du secteur de la sécurité et de la défense : industriels, Délégations Officielles, VIP experts, opérationnels utilisateurs, responsables achat, bureaux d'études, chercheurs, investisseurs et journalistes qui suivent les problèmes de défense et de sécurité.

Lieu : Parc des Expositions Nord Villepinte, Paris

Pour en savoir plus :

[Le salon | Eurosatory](#)



20 au 25 juin 2022

INTERSCHUTZ, salon international des professionnels de la prévention et de la lutte contre les incendies, de la protection civile, du sauvetage et de la gestion des catastrophes

Public : Professionnels de la sécurité et protection civile

Lieu : Hannover Exhibition Grounds, Messegelände, 30521 Hannover, Allemagne

Pour en savoir plus :

[INTERSCHUTZ 2022 - SAFE Cluster](#)



21 au 24 septembre 2022

La 128^e Congrès national des Sapeurs-Pompiers de France

Public : Sapeurs-pompiers de France et professionnels de la sécurité civile

Lieu : Nancy, France

Pour en savoir plus :

[Accueil - 128^eème congrès national des sapeurs-pompiers de France](#)



LIREC



ABONNEZ-VOUS À NOTRE LETTRE



»»» lirec@ihemi.fr


**RÉPUBLIQUE
FRANÇAISE**
*Liberté
Égalité
Fraternité*


IHEMI
INSTITUT
DES HAUTES ÉTUDES
DU MINISTÈRE DE L'INTÉRIEUR

DÉPARTEMENT ÉTUDES ET RECHERCHES