Les quatre chantiers des dirigeants

Résister solidement à une crise cyber-IA

Juin 2026

Ce document n'est pas un guide de gestion de crise mais un outil de réflexion, sur la question « Que faire pour se préparer efficacement contre une crise cyber-IA ? »

Car attendre la stabilisation d'un contexte est une pure illusion devant les tensions géopolitiques croissantes, l'évolution technologique débridée, un paysage des menaces fluctuant, une réglementation de plus en plus stricte avec des interprétations différentes entre états, l'effondrement de la preuve, etc.

Il est alors hors de question d'improviser, de réagir à chaud, dans un monde interconnecté et globalisé, truffé d'interdépendances que nous ne maîtrisons pas toutes.

Ces conditions créent un brouillard, où les réactions sont difficiles à anticiper. Par conséquent, la seule solution est de se concentrer ce qu'on peut changer et influencer dans son écosystème.

Quatre chantiers s'imposent.

- Préparer une solide communication de crise cyberIA
- Maîtriser sa surface d'attaque
- Réduire ses failles organisationnelles
- Revoir sa posture et son leadership

Maryse Rebillot

Strategic Advisor on Cyber-AI crises and information integrity

une **solide**
communication de crise cyberIA

Une cyberattaque n'est pas une crise. C'est un déclencheur du désordre, d'une tempête émotionnelle et informationnelle, où la communication joue un rôle essentiel pour endiguer le chaos.

Elle définit qui parle, quoi dire, à qui, dans quel ordre, quand s'exprimer et comment. C'est d'autant plus crucial que l'IA compresse la dynamique des crises.

Lire notre article sur la dynamique des crises.

Or, la communication de crise reste le grand absent des préparations à la gestion de crise. Les organisations investissent dans la cybersécurité technique, mettent en place plus ou moins une cellule et un plan de gestion de crise. Mais très régulièrement, elles oublient la face humaine et organisationnelle de la préparation.

C'est une erreur structurelle à **l'ère de l'IA, où il faut répondre plus vite et plus juste avec un solide dispositif et contenu préparés en amont.**

De quoi parle-t-on exactement

Il s'agit d'une **stratégie de communication de crise systémique, adaptée aux nouvelles menaces IA.** Une stratégie qui prend en compte **l'ensemble de l'écosystème et ses interlocuteurs** — collaborateurs, partenaires, fournisseurs, médias, autorités, clients – car les pirates, quels qu'ils soient, exploitent les moindres failles et portes d'entrée.

Préparer cette stratégie, c'est comme préparer ses armes et savoir quand et comment les dégainer au moment de l'attaque et de la crise.

De quelles armes parle-t-on ?

Le socle indispensable est un plan qui détaille :

- les risques cyber-IA
- les simulations de crise en conditions réelles à mettre en place
- la politique et posture de l'organisation en cas de crise cyberIA
- l'équipe de gestion de crise, formée et entraînée, avec rôles et responsabilités
- le dispositif de détection et d'alerte mis en place pour tout type d'anomalies
- les canaux de communication alternatifs sécurisés
- les narratifs et les messages préparés, validés
- les contenus critiques de tout format à protéger, et le type de protection prévu
- les consignes de sécurité à transmettre
- les listes de contacts à jour
- le paysage médiatique (en ligne, local, régional, national, métier, tech, cyber)

Ce socle est la pointe de l'iceberg de la cybersécurité humaine et organisationnelle. C'est la **soupape de sécurité qui contient la pression** générée dans l'écosystème lors d'une crise cyberIA.

Moins votre organisation contient de failles humaines et organisationnelles, plus efficace sera la communication de crise cyber-IA, le jour J.

Maîtriser sa surface d'attaque informationnelle

Avant même qu'une crise survienne, chaque contenu publié, chaque prise de position, chaque déclaration officielle constitue de la matière pour un adversaire.

Il ne s'agit pas de se taire mais de décider ce qu'on publie, où, comment, avec quelles matières et quelles preuves associées. La vérité n'est plus une évidence à l'ère des deepfakes et des récits synthétiques.

La vérité doit être gouvernée, prouvée, traçable.

Sept questions concrètes à vous poser

- Êtes-vous capable de lister les données et contenus les plus sensibles de votre organisation, sans quoi votre organisation ne peut plus fonctionner ? Si oui, vos employés sont-ils au courant ?
- Sur quelles données/sources s'est bâti le discours ou la publication ? Sont-elles vérifiables, traçables, défendables ?
- Quels risques narratifs/manipulatoires prend-on vs. les avantages réputationnels ? Autrement dit, est-ce que le risque en vaut vraiment la chandelle ?
- Qui, en interne, valide le contenu avant publication ? Existe-t-il un protocole de double vérification pour les contenus sensibles ou critiques ?
- Ce contenu, une fois publié, peut-il être retourné contre nous dans un autre contexte — géopolitique, concurrentiel, médiatique ?
- Quels tiers de confiance peuvent authentifier ou relayer ce discours pour lui donner du poids face à une attaque ?
- En cas de contestation, a-t-on les preuves nécessaires pour défendre la version originale auprès du public, de ses interlocuteurs stratégiques, les autorités ?

C'est l'objet de la Gouvernance de la Vérité — mettre en place les mécanismes qui garantissent que l'information diffusée est vérifiable et défendable, avant qu'un adversaire ne la retourne contre vous.

Réduire les failles organisationnelles propices à la manipulation

La manipulation est une tactique vieille comme le monde.

La différence à l'ère IA, c'est sa perniciosité - on ne connaît pas son ennemi - son imprévisibilité - quand et comment elle va surgir - son amplitude et sa dynamique dans ce monde interconnecté.

Elle exploite les zones d'ombre humaines et organisationnelles, comme :

- le management qui ignore ou minore les signaux faibles
- les équipes désengagées qui ne remontent plus rien
- la pression qui fabrique des décisions mécaniques
- la présence de règles ambiguës
- une organisation en silo qui fragmente la communication et la cohésion
- etc.

Lire notre article sur les signaux faibles

Avant de subir une crise, il faut diagnostiquer sa propre vulnérabilité sur au moins quatre angles avec des questions précises.

- la circulation de l'information et des alertes
- la culture interne et ses fragilités
- les dépendances les angles morts
- l'engagement et la loyauté

Sur la circulation de l'information et des alertes

- Vos équipes savent-elles ce que sont les signaux faibles ?
- Si oui, les remontent-elles jusqu'en haut, ou sont-ils filtrés, édulcorés, normalisés en chemin ?
- Existe-t-il un canal formel pour signaler une anomalie, une incohérence, un comportement inhabituel ou déplacé sans passer par la hiérarchie directe ?

Sur la culture interne et ses fragilités

- Y a-t-il des zones de tension silencieuse, entre équipes et/ou niveaux hiérarchiques, qui pourraient être exploitées de l'extérieur ?
- Le langage interne est-il clair et cohérent, ou flou et manipulable ? Les mots ont-ils le même sens pour tout le monde ?
- Quelle est la part de conformisme dans les prises de décision ? Les désaccords s'expriment-ils ou s'autocensurent-ils ?

Sur les dépendances et les angles morts

- Quels fournisseurs, partenaires ou prestataires ont accès à certaines de vos informations sensibles ? Lesquelles et avec quelle garantie d'intégrité ?
- Y a-t-il des personnes-clés dont le départ ou la compromission fragiliserait l'ensemble du dispositif ?
- Quelles sont les décisions qui reposent sur une seule source, un seul outil, un seul modèle IA, sans contre-vérification possible ?

Sur l'engagement et la loyauté

- Les équipes comprennent-elles tous les enjeux et les risques cyber-IA auxquels l'organisation est exposée ? Si oui, comment pouvez-vous l'assurer sans dérive d'interprétation ?
- Vos équipes font-elles confiance à la direction pour gérer une crise, et respecteront-elles les consignes de sécurité scrupuleusement ? Sont-elles suffisamment engagées à détecter et remonter les anomalies, même sous pression ?
- Quel est le niveau de résistance face à l 'adoption de l'IA ? Par qui ? Pourquoi ?

La question la plus redoutable : "Si un adversaire voulait déstabiliser notre organisation de l'intérieur, par où commencerait-il ?"

C'est ce que le Resilience Culture Lab permet d'identifier et de corriger, non pas après l'incident, mais bien en amont. C'est le socle même de la résilience organisationnelle.

Revoir
sa **posture** et son **leadership**

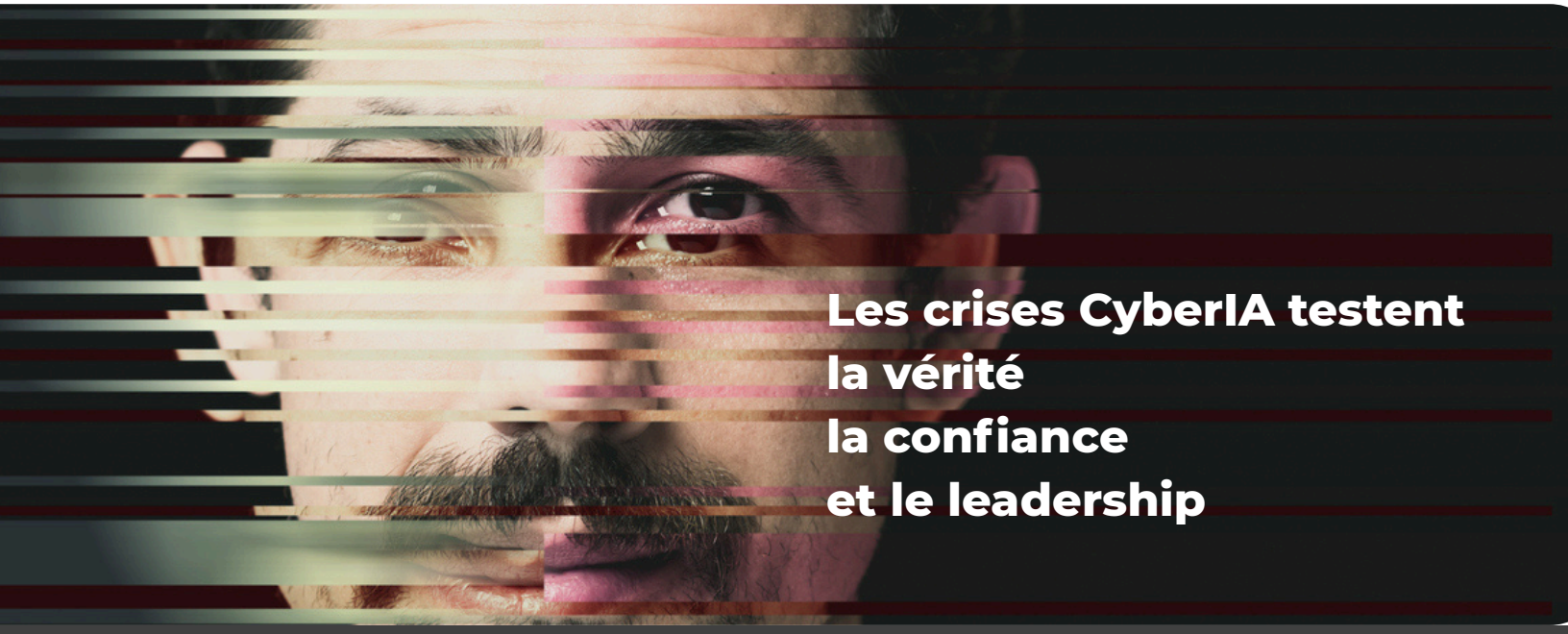
Vous le savez, seul l'exemple compte.

On peut avoir les plus beaux discours du monde, mais…

- s'ils ne sont pas suivis d'actions et de décisions alignées aux paroles
- si vous maintenez de l'ambiguïté dans vos règles
- si vous tolérez des comportements toxiques de grands performers
- si vous n'écoutez pas l'écho du terrain sur vos décisions stratégiques
- etc.

…. Vous ouvrez grand le portail aux menaces cyber-IA, qui jouent sur les perceptions, les incertitudes et les doutes.

Au-delà de l'éthique, la cohérence est un bouclier, qui génère de la confiance et de la cohésion. Un dirigeant dont les actes et les mots s'alignent est infiniment plus difficile à décrédibiliser. Ce travail sur la posture, ce que les équipes perçoivent, ce que les parties prenantes lisent, ce que les adversaires cherchent à retourner, est au cœur du Leadership Résilient & Éthique.



Quelques questions à vous poser personnellement en votre for intérieur

Sur la crédibilité personnelle face aux attaques

- Si j'arrange la réalité à ma convenance, sur les résultats, les engagements, les faits, etc., quelle surface d'attaque est-ce que je crée pour un adversaire qui voudrait me faire dire, via un deepfake, ce que je n'ai jamais dit ?
- En cas de deepfake, ma parole aura-t-elle assez de crédit pour être crue — ou le doute s'installera-t-il trop facilement parce que "ça lui ressemble" ?

Sur la tolérance aux comportements toxiques

- Si je laisse des hauts performeurs se conduire de manière contraire aux valeurs que j'affiche, quel message réel est-ce que j'envoie à l'organisation ? Et si demain je dois incarner l'éthique face à une crise, qui me croira ?
- L'écart entre ce que je tolère en interne et ce que je prône en public est exactement ce qu'un adversaire cherche à exposer ou à amplifier.

Sur l'isolement décisionnel

- Est-ce que je laisse mes managers décider seuls, sans filet, avec le sentiment d'être abandonnés face à la difficulté ? Les hackers et les manipulateurs exploitent le sentiment de solitude — une personne isolée est une personne vulnérable, perméable à la pression, au chantage, à la manipulation sociale.
- La résilience se construit dans la relation quotidienne entre un dirigeant et ses équipes, notamment dans les moments où rien ne va.

La réflexion centrale qui chapeaute les trois : "Ce que je fais, quand personne ne regarde, finira toujours par définir ce que je suis quand tout le monde regarde »

5 leçons à retenir

1. **Attendre la stabilisation est une erreur** — dans un environnement d'instabilité fluctuante, rien ne se stabilise. La seule solution est de se concentrer sur ce qu'on peut changer et influencer.

2. **La communication de crise cyber-IA est le grand absent des préparations** — c'est une erreur structurelle à l'ère de l'IA, où il faut répondre plus vite et plus juste avec un dispositif solide préparé en amont.

3. **La vérité doit être gouvernée, prouvée, traçable** — chaque contenu publié est de la matière pour un adversaire. Maîtriser sa surface d'attaque information-nelle, c'est décider ce qu'on expose et comment on le défend.

4. **La manipulation exploite les failles humaines et organisationnelles** — les angles morts managériaux, les silos, le désengagement sont les portes d'entrée que les attaquants visent en priorité.

5. **La cohérence du dirigeant est un bouclier** — l'écart entre ce qu'on tolère en interne et ce qu'on prône en public est exactement ce qu'un adversaire cherche à exposer.

Dans un monde où la réalité se manipule, la préparation n'est plus une option.

Où en est votre organisation ?

25 questions. 15 minutes. Résultat immédiat et anonyme.

Testez-vous gratuitement

contact@ozngo.com