

A L'ÈRE CYBER-IA, VOTRE MEILLEURE DÉFENSE EST **L'HUMAIN**



Résilience, Vérité, Cohésion : trois piliers pour renforcer **votre sécurité**.

ce que les dirigeants doivent entendre.





Une crise ne détruit pas une réputation

La
manière
d'y répondre,
oui.

Plus encore
à l'ère IA

A CE JOUR



votre entreprise est protégée par
une gouvernance de cybersécurité techno-centrée

Cartographie des Risques Identification des données critiques Conformité & Risque legal Simulation de Crise	Infrastructure IT SOC - SIEM/EDR/XDR Processus IT Patch Management Phishing Tests PenTest Audit Threat Intelligence
Cellule de Crise Plan de Crise Incident Response Escalade & Alerte Plan de Continuité	Canaux de Com sécurisés Messages pré-rédigés Formations Cyber Préparation Porte-Parole



où tout ce qui est TECHNIQUE est parfaitement maîtrisé.
(analysé, priorisé, monitoré 24/7)



soutenue par une communication de **crise** standardisée, séquentielle,
conçue pour des incidents IT

Tout est orchestré de manière **rationnelle** pour sécuriser vos systèmes, *le jour où*

mais vos interlocuteurs ne sont pas des machines

LE NOUVEAU RISQUE EST INVISIBLE



Avec la pression interne comme surface d'attaque

- Sous pression, les équipes deviennent plus manipulables, moins vigilantes.
- L'IA amplifie exactement les signaux qui déstabilisent : confusion, surcharge, doute.

A photograph of a man with a beard and curly hair, holding his hands to his temples in a gesture of distress or pain. The background is a light gray surface covered with dense, chaotic black scribbles and various symbols like dollar signs, question marks, and arrows, suggesting mental clutter or stress.

*Les hackers exploitent ce que
votre management fragilise*

Il attaque

- vos données
- vos modèles IA
- votre perception de la vérité
- vos émotions
- vos chaînes de dépendance



Déformer, amplifier et propager le fake le plus fort et le plus vite possible



Flouer vos repères culturels et informationnels



vos comportements et vos décisions, individuellement et collectivement



Pertes en domino

Crédibilité, Confiance

Cohésion, Engagement

Performance

Argent à court, moyen et long terme

Avoirs, Biens, Business, ... TOUT

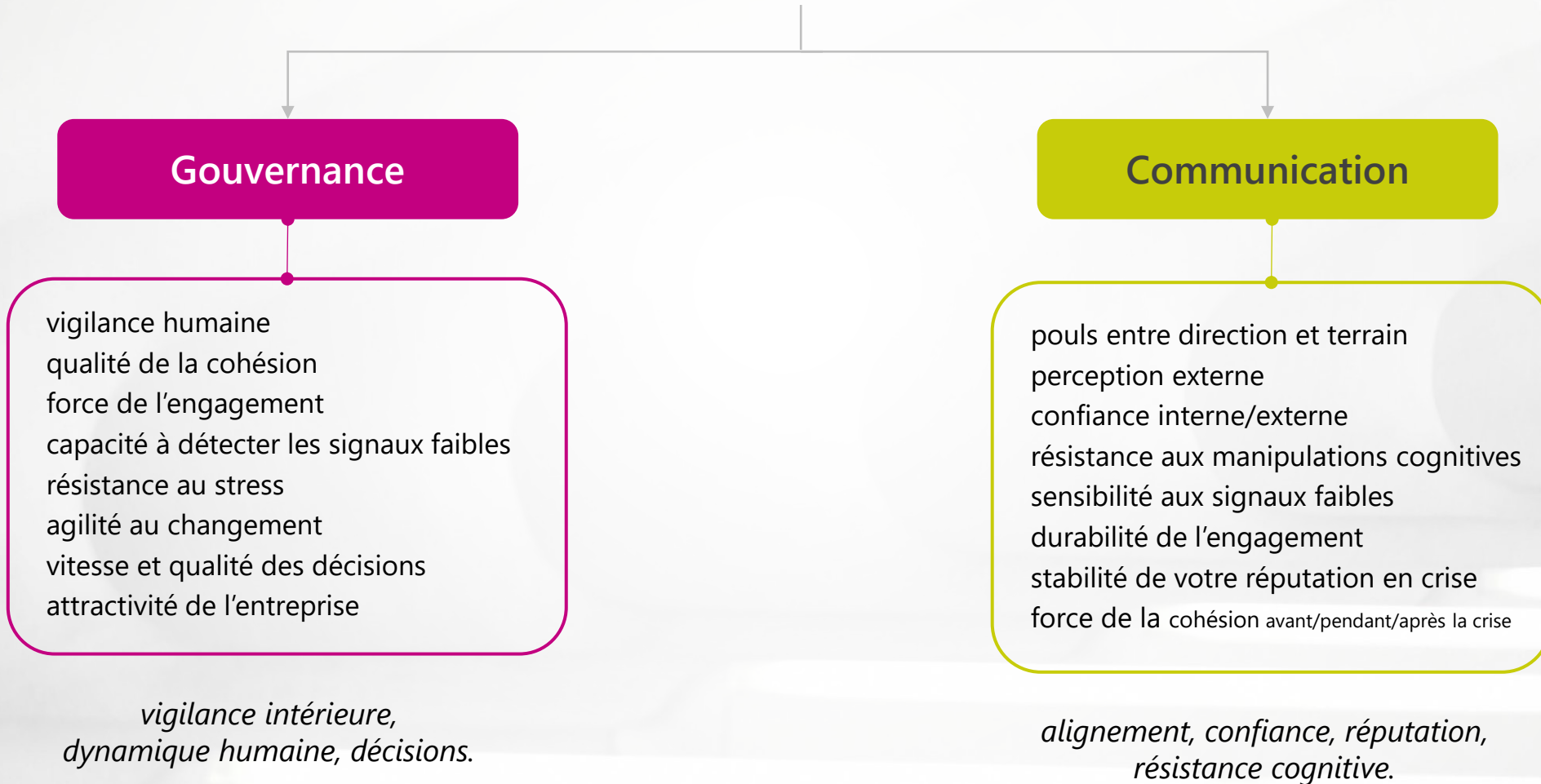
Quand la vérité se fragmente, l'unité se désagrège.

Le champ de bataille a évolué



VOUS DEVEZ CHANGER pour garder le contrôle

Ce que vous pouvez influencer



LES 4 ANGLES MORTS

que votre gouvernance actuelle ne couvre pas



Leadership Emotionnel

Biais, stress, surcharge mentale, distorsions de la réalité, décisions altérées sous pression, etc.

Décisions altérées = 1^{ère} cible du hacker

Résilience Collective



Culture, cohésion
Gouvernance Vérité
Circuit de Veille et Alerte
Engagement actif

Culture, cohésion et partage vos meilleures défenses

Cartographie des Risques
Identification des données critiques
Conformité & Risque légal
Simulation de Crise

Infrastructure IT
SOC SIEM/EDR/XDR
Processus IT
Patch Management
Phishing Tests
PenTest Audit
Threat Intelligence

Cellule de Crise
Plan de Crise
Incident Response
Escalade & Alerte
Plan de Continuité

Canaux de Com sécurisés
Messages pré-rédigés
Formations Cyber
Préparation Porte-Parole

Rôles Critiques



Cartographie élargie
Vigilance renforcée
Signaux faibles intégrés au dispositif

Les bonnes personnes doivent voir les bonnes anomalies au bon moment

Réseau externe d'Alliés crédibles & de confiance

Experts variés, Journalistes
Institutions
Sources Crédibles
Ecosystème engagé

Votre bouclier Vérité en cas de crise IA



La **crise**
se gère.

Communication Crise

Réactive



Court-
Terme



Raison



Exclusive



Focus
Réassurance



Interne



Préser-
vative



Communication Résilience

Proactive



Long-
Terme



Emotion



Inclusive



Focus
Engagement



Eco
système



Trans-
formative



La **résilience**
se construit.

*L'IA attaque vos
perceptions.*

*Votre communication doit
protéger vos équipes.*

L'ARCHITECTURE DE NOS SERVICES



Communication de Crise CyberAI

Diagnostic (crise, médias, modèles & usages IA)

Scénarios & Simulations (cyber. deepfake, rumeurs)

Cellule & Plan de Crise (rôles, messages, canaux, matériel)

Circuit Interne d'Alerte & Signaux Faibles

Protection des Contenus Officiels

Accompagnement, Formations & Coaching

Gouvernance de la Vérité

Diagnostic de la chaîne de vérité

Cellule Vérité

Stratégie de la preuve

Réseau d'alliés crédibles

Coordination AI/Cloud

Authentification officielle
(processus + preuves)

Tableau de bord de perception & d'information

Résilience Culture Lab

Baromètre & Grille de Maturité de Résilience

Programmes de Formation : Vigilance & Esprit Critique

Politique et Monitoring des signaux faibles

Simulations & Exercices de Résilience

Leadership Résilient & Confiance Interne

Disclaimer

Les missions Oz'n'gO supposent que le socle vital de cybersécurité technique est en place. Si ce n'est pas le cas, nous faisons appel à nos experts qui travailleront avec vos partenaires techniques habituels.

QUI EST OZ'N'GO

Votre partenaire en Communication de Crise & Résilience Cyber.



Maryse Rebillot

Fondatrice
Résilience & Communication de Crise



- 20+ ans en marketing-communication dans le High Tech et la Cybersécurité
- Experte en gestion de crise & Communication sensible
- International Executive Marketing Master, INSEAD

[linkedin.com/in/maryse-rebillot](https://www.linkedin.com/in/maryse-rebillot)

Réseau d'Experts

(mobilisables selon les missions, en fonction des besoins)



Cybersécurité

Cyber défense, White Hacking, Gouvernance Cyber, Gouvernance des données, Légal & Assurance



IA & Technologies

IA Générative, LLM, IA Vertical, Autres IA



Humain & Communication

Psychologie, Médias & Journalistes, Sociologie

Oz'n'Go, le guide des dirigeants pour maîtriser les crises que l'IA crée, amplifie ou manipule.



À L'ÈRE DE L'IA,
LA SEULE DÉFENSE DURABLE
c'est la cohésion humaine.



Maryse Rebillot

contact@ozngo.com

+41 77 533 77 67

www.ozngo.com