LA RESILIENCE ORCHESTRÉE

La communication stratégique qui soude votre écosystème humain.

*Pour affronter les **crises** amplifiées par l'IA et les tensions sociales.*

Une crise ne détruit pas une réputation

La manière d’y répondre, oui.

Ce que vous appliquez aujourd'hui pour protéger votre entreprise

Une gouvernance des risques techno-centrée

Soutenue par

Une Communication de Crise

MAIS A L'ÂGE DU CYBER-AI

Les **règles du 'jeu'** changent

Tendances 2026

Ingénierie sociale et hameçonnage basés sur l'IA

Les pirates exploitent l'IA générative pour créer des e-mails d'hameçonnage très convaincants, des messages vocaux/vidéo deep-fake et des interactions par chat qui imitent des personnes ou des marques de confiance.

Data Poisoning & Manipulation de Modèle AI

Les pirates injectent des données malveillantes ou trompeuses dans les ensembles de données d'entraînement, ce qui corrompt l'intégrité des modèles d'IA.

Inversion et extraction de modèles

Les pirates tentent de procéder à une ingénierie inverse ou de voler des modèles d'IA propriétaires en effectuant des requêtes répétées ou en exploitant des API exposées.

Machine Learning Antagoniste

Les pirates créent des entrées subtiles et malveillantes, conçues pour tromper les modèles d'IA et les amener à mal classer les données (ex: système de reconnaissance d'images qui ne détecte pas une arme)

Chaîne logistique de l'IA et attaques par dépendance

Threat actors exploit third-party AI components, libraries, or pre-trained models that organizations integrate into their systems.

Le hacker d'aujourd'hui…

… n'est plus seulement un génie de l'informatique, mais un **directeur de campagne**, assisté par l'IA et un écosystème de fournisseurs de micro-services dans des domaines spécifiques.

… **altère le fonctionnement ou la crédibilité de l'IA utilisée**.

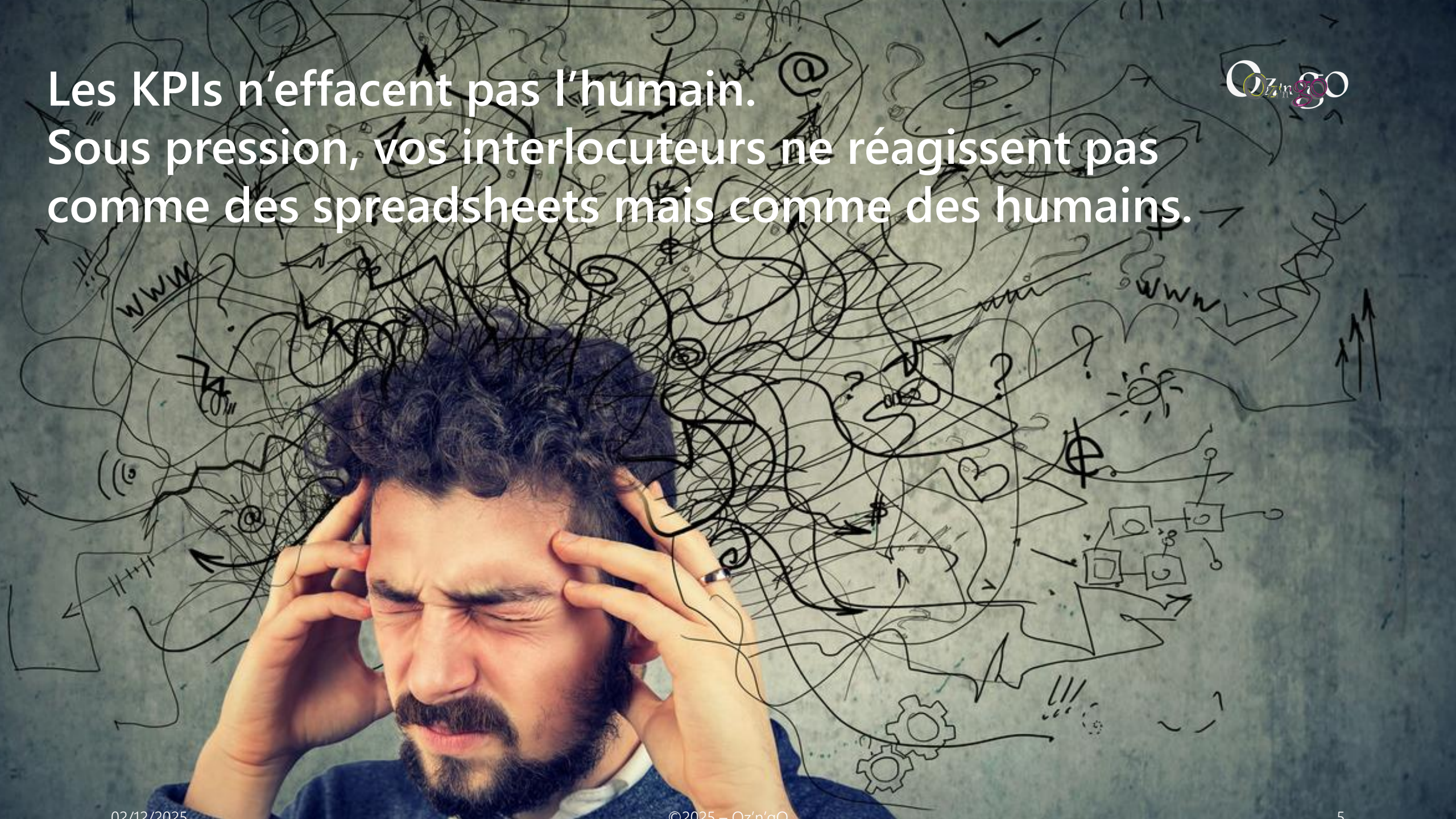
… **exploite les chaînes logistiques**.

… **réduit le temps nécessaire à l'exploitation.**

Sur quoi les organisations doivent se focaliser

- **Une gouvernance de la vérité**
- **Un concept de résilience étendu aux aspects humains et sociaux**
- **Un partage en interne des connaissances et experiences à utiliser en levier**
- **Une culture de pensée et de reactions critiques (vigilance)**
- **Des tests de communication sous pression en conditions réelles**
- **Un engagement individual et collectif, interne et externe**

Les KPIs n’effacent pas l’humain.
Sous pression, vos interlocuteurs ne réagissent pas comme des spreadsheets mais comme des humains.



LES ANGLES **MORTS** DE LA GOUVERNANCE DES RISQUES **TECHNO**-CENTRÉE

Sécuriser le système IT ≠
Sécuriser l'organisation

Préparer sa Communication de Crise

est VITAL

avec un plan qui :

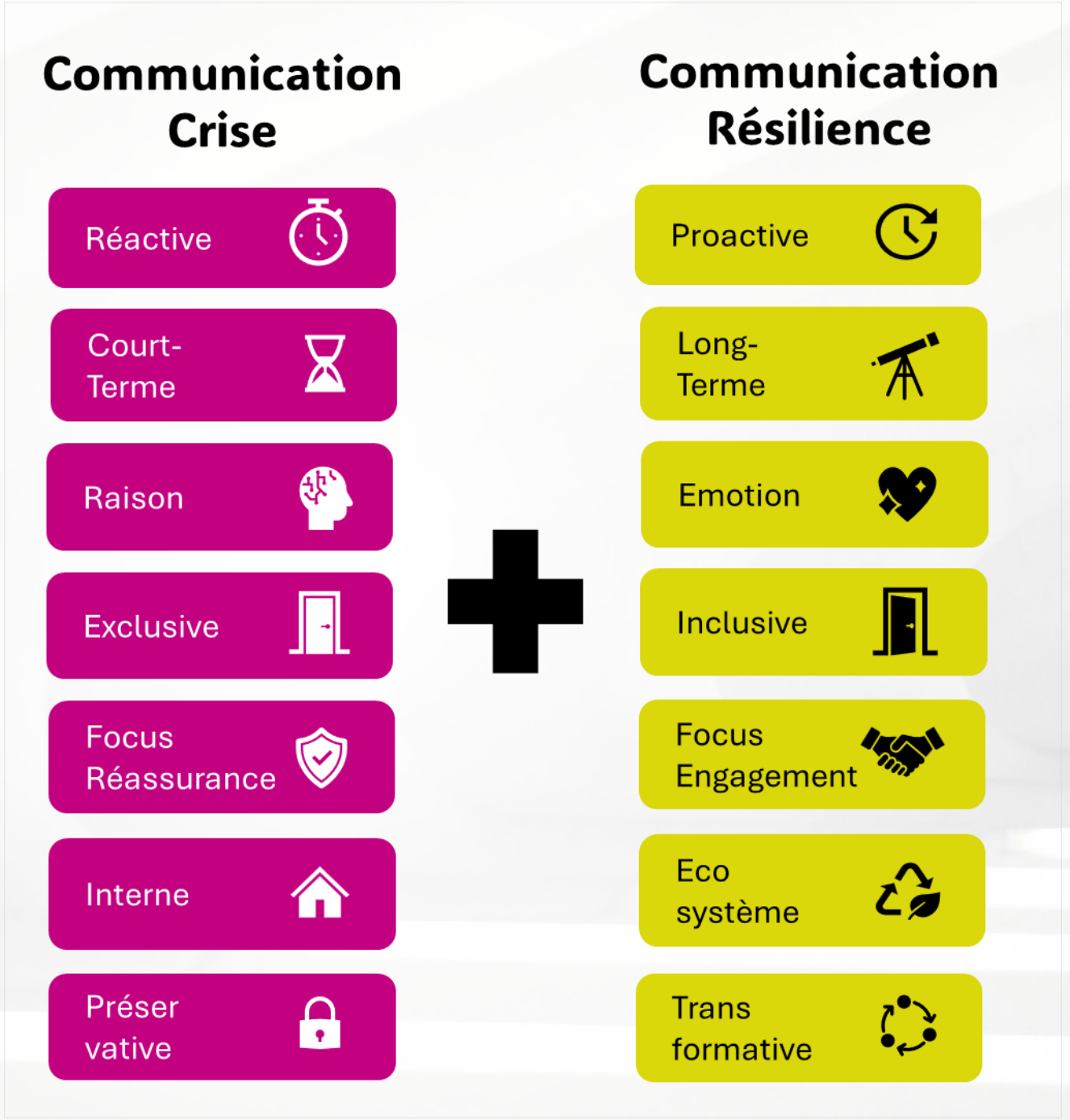
- dépasse la technique et l'aspect juridique
- est inclusif
- intègre l'émotionnel, le psychologique, le social

👉 base de la résilience

COMMUNICATION DE CRISE

vs.

COMMUNICATION DE RESILIENCE



LES 7 LEVIERS DE LA CYBERCULTURE DE RESILIENCE

Basés sur la boussole de cyber-résilience du WEF

Vision, Stratégie

Co-création avec les interlocuteurs externes

Cadre & Orientation

Intégration des angles morts

Comportement & Mental

Liens Business & Vulgarisation

Transition vers l'Agilité

Source: World Economic Forum

QUI EST Oz'n'gO

Réseau d'Experts

Réseau d'Experts

Cyber Gouvernance

Cybersécurité & White Hacking

Cyber défense

Légal & Assurance

Gouvernance des Données

Psychologie

IA Générative

Autres AI

Media & Journalistes

Maryse Rebillot

- 20+ and dans le marketing-communication, dans le High Tech et la Cybersécurité
- Solide expérience en gestion de crise
- International Executive Marketing Master, INSEAD

MENEZ VOTRE ORGANISATION À LA RÉSILIENCE

Une résilience centrée sur l'humain, adaptée à l'ère des menaces cyber et de l'IA.

Maryse Rebillot

contact@ozngo.com

+41 77 533 77 6