IN THE CYBER-AI ERA, YOUR BEST DEFENSE IS HUMAN

Resilience, Truth, Cohesion: three pillars to strengthen your security.

what leaders need to hear.

Its bad response does.

A crisis doesn't detroy a reputation

Even more in the AI era

AS OF TODAY

your organisation, at best, is protected by

A tech-centric cybersecurity governance

Risk Mapping	IT Infrastructure
Critical Data Identification	SOC SIEM/EDR/XDR
	IT Process
Compliance & Legal Risk	Patch Management
	Phishing Tests
Crisis Simulation	PenTest Audit
	Threat Intelligence
Crisis Team	Secured Com Channels
Crisis Plan	Approved Messages
Incident Response	Cyber Trainings
Escalation & Alert	Spoke-Person
Business Continuity	Preparation

📎 where everything TECHNICAL is perfectly under control.
(analysed, prioritised, monitored 24/7)

📎 supported by a standardised, sequential crisis communication,
Designed for IT incidents

Everything is orchestrated on a **rational** way to secure your systems, *for the day when*

but the people you talk to are not machines.

THE NEW RISK IS INVISIBLE
With internal pressure as an expanding attack surface

- Under pressure, teams become more manipulable, less vigilant.
- AI amplifies exactly the destabilising signals: confusion, overload, doubt.

Hackers exploit what your management weakens

THE 2026 HACKER

Oz'n'go

Distort, amplify, and spread fake news <u>as broadly and quickly as possible</u>

Blurring your cultural and informational reference points

He attacks

- your data
- your AI models
- your truth perception
- your emotions
- Your dependence chain

➔ Your behaviours and decisions, <u>individually and collectively</u>

Domino effect Losses

Credibility, Trust

Cohesion, Engagement

Performance

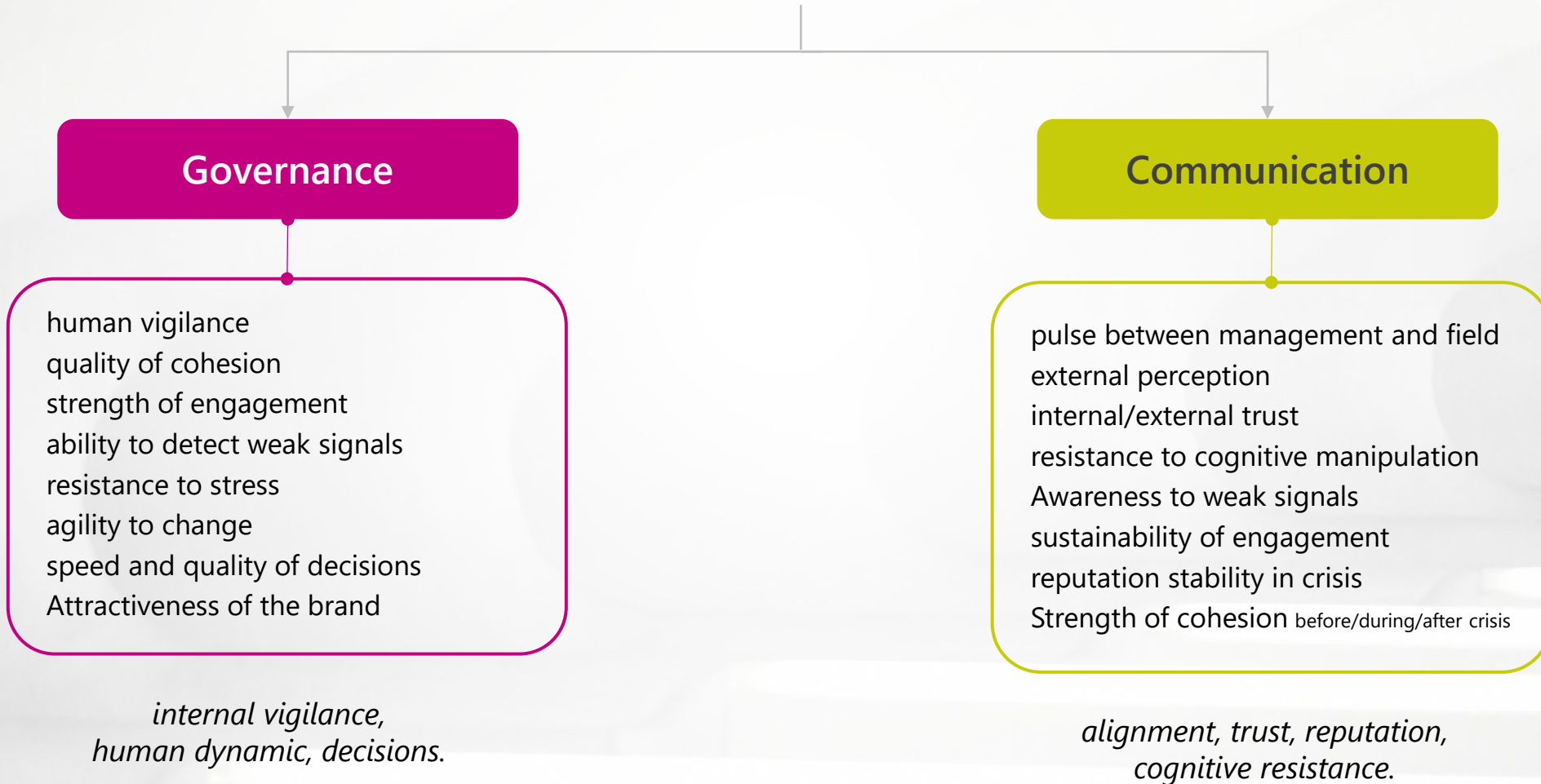Money in short, medium, and long term

Assets, business... EVERYTHING

When truth fragments, unity disintegrates.
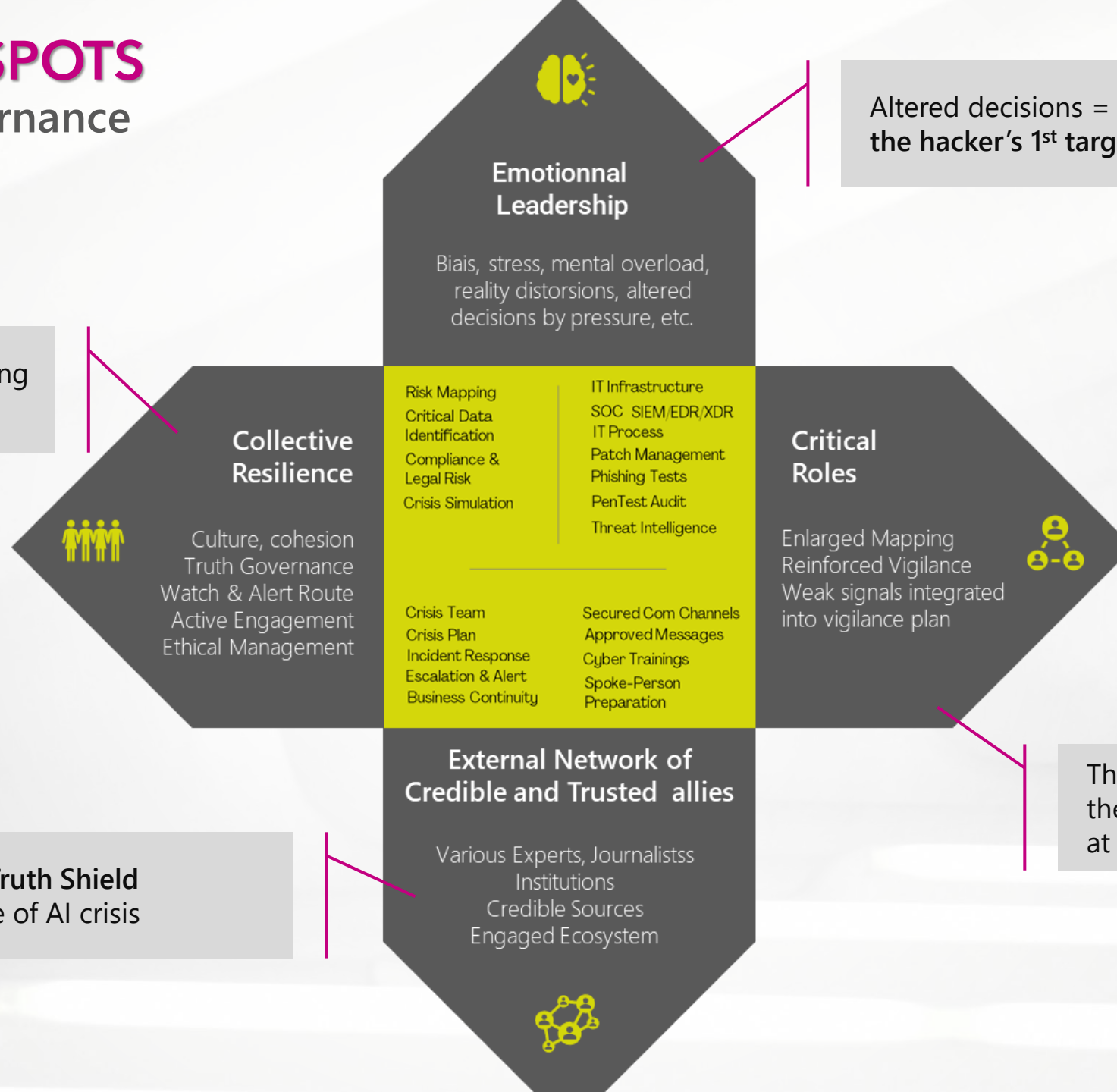
The battlefield has evolved.

YOU MUST CHANGE to keep control

Oz'n'go

What you can influence

Governance

human vigilance
quality of cohesion
strength of engagement
ability to detect weak signals
resistance to stress
agility to change
speed and quality of decisions
Attractiveness of the brand

*internal vigilance,
human dynamic, decisions.*

Communication

pulse between management and field
external perception
internal/external trust
resistance to cognitive manipulation
Awareness to weak signals
sustainability of engagement
reputation stability in crisis
Strength of cohesion before/during/after crisis

*alignment, trust, reputation,
cognitive resistance.*

THE 4 BLIND SPOTS
your current governance don't cover

Oz'n'go

Altered decisions = the hacker's 1st target

Emotionnal Leadership

Biais, stress, mental overload, reality distorsions, altered decisions by pressure, etc.

Culture, cohesion & sharing your best defenses

Collective Resilience

Culture, cohesion
Truth Governance
Watch & Alert Route
Active Engagement
Ethical Management

Risk Mapping	IT Infrastructure
Critical Data Identification	SOC SIEM/EDR/XDR
	IT Process
Compliance & Legal Risk	Patch Management
	Phishing Tests
Crisis Simulation	PenTest Audit
	Threat Intelligence
Crisis Team	Secured Com Channels
Crisis Plan	Approved Messages
Incident Response	Cyber Trainings
Escalation & Alert	Spoke-Person
Business Continuity	Preparation

Critical Roles

Enlarged Mapping
Reinforced Vigilance
Weak signals integrated into vigilance plan

The right people must see the right anomalies at the right time

External Network of Credible and Trusted allies

Various Experts, Journalistss
Institutions
Credible Sources
Engaged Ecosystem

Your Truth Shield in case of AI crisis

Crisis Communication

Crisis is managed.

Reactive	⏱
Short-Term	⏳
Reason	🧠
Exclusive	🚪
Focus Reassurance	🛡
Interne	🏠
Préservative	🔒

+

Resilient Communication

Resilience is built.

Proactive	🕐
Long-Term	🔭
Emotion	💖
Inclusive	🚪
Focus Engagement	🤝
Eco système	♻
Trans formative	🔄

AI attacks your perceptions. Your communication must protect your people.

Oz'n'go

ARCHITECTURE OF OUR SERVICES

CyberAI Crisis Communication

Diagnoses (crisis, medias, AI models & usages)

Scenarios & Simulations (cyber. deepfake, rumours)

Crisis Team & Plan (roles, messages, channels, material)

Internal Alert Route & Weak Signals

Protection of Official Content

Support, Training & Coaching

Governance of Truth

Truth-Chain Diagnosis

Truth Team

Proof Strategy

Credible Allies Network

AI/Cloud Coordination

Authentication of Official Content (process + evidence)

Dashboard of perception & information

Resilience Culture Lab

Resilience Barometer & Maturity Framework

Training Programs: Vigilance & Critical Thinking

Framework for Dialogue and Alert

Organisational Resilience Simulations & Exercises

Resilient and Ethical Leadership (including human & reputational indicators to reduce blindspots)

Disclaimer

Oz'n'gO's engagements assume that the essential foundation of technical cybersecurity is already in place. If this is not the case, we bring in our experts, who will work alongside your existing technical partners.

WHO IS OZ'N'GO

Your Partner in Crisis Communication & Cyber Resilience.

Maryse Rebillot

Founder
Resilience & Crisis Communication

- 20+ years in marketing-communication in High Tech, Cyber security
- Expert in Crisis Management & Sensitive Communication
- International Executive Marketing Master, INSEAD

🔗 *linkedin.com/in/maryse-rebillot*

Experts Network

(mobilisables selon les missions, en fonction des besoins)

🔒 Cybersecurity

Cyber defense, White Hacking, Cyber Governance, Data Governance, Legal & Insurance

🤖 AI & Technologies

Gen AI, LLM, Vertical AI, Other AI

🧠 Human & Communication

Psychology, Medias & Journalists, Sociology

Oz'n'Go, the guide for leaders to master the crises AI creates, amplifies, or manipulates.

IN THE AGE OF AI,
THE ONLY SUSTAINABLE DEFENSE

Is Human Cohesion

Maryse Rebillot

contact@ozngo.com

+41 77 533 77 67

www.ozngo.com