Prepare your organisation for CyberAI crises

The battlefield is changing

ozngo

THE ATTACK SURFACE IS NO LONGER JUST A TECHNICAL ISSUE

YESTERDAY

— Systems & servers
— Networks & protocols
— Software failures
— Firewall & identities

IA

TODAY

— Emotions & cognitive biases
— Trust & perceived authority
— Decisions under pressure
— Beliefs & representations

It is also becoming informational and cognitive

ozngo

Today, the response to attacks remains technical

… to correct human error, assumed to be the weak link.

But 2026 hackers exploit less technical vulnerabilities than

organisational fragilities

A DANGEROUS MISALIGNMENT

A PLAYGROUND FOR HACKERS

Latent fears left adressed together

CEO-CFO

Deepfake – vishing
Reputational Damage
Loss of Trust

Teams

Social Engineering
Layoffs
Workplace disstress - Pressure

CIO - CISO

Ransomware · IT/AI/Cloud chain
Operational Continuity
System Resilience

misaligned decisions
ambiguities
counterproductive pressure
manipulation

WHERE ATTACKS START

The Hidden Damage

- Loss of Bearings
- Loss of Trust
- Loss of Credibility

The voice of my CFO on the phone — is it really him?

The information in this email — can I trust it?

If my AI analytics model — which cost a fortune — has been compromised, how would I know? And how long before I find out?

If fake news strikes, will I be able to keep control of the narrative?

How can I be sure I'm doing the right thing?

How to close the entry points

CEO-CFO

Deepfake – vishing
Reputational Damage
Loss of Trust

Clarify & Secure
the work environment

Lock Down Truth
in the Ecosystem

Teams

Social Engineering
Layoffs
Workplace distress - Pressure

Protect integrity
information, content, data, narratives

Strengthen cohesion
In case of incident

Define a common language

CIO - CISO

Ransomware · IT/AI/Cloud chain
Operational Continuity
System Resilience

Before the failure becomes technical

Our mission

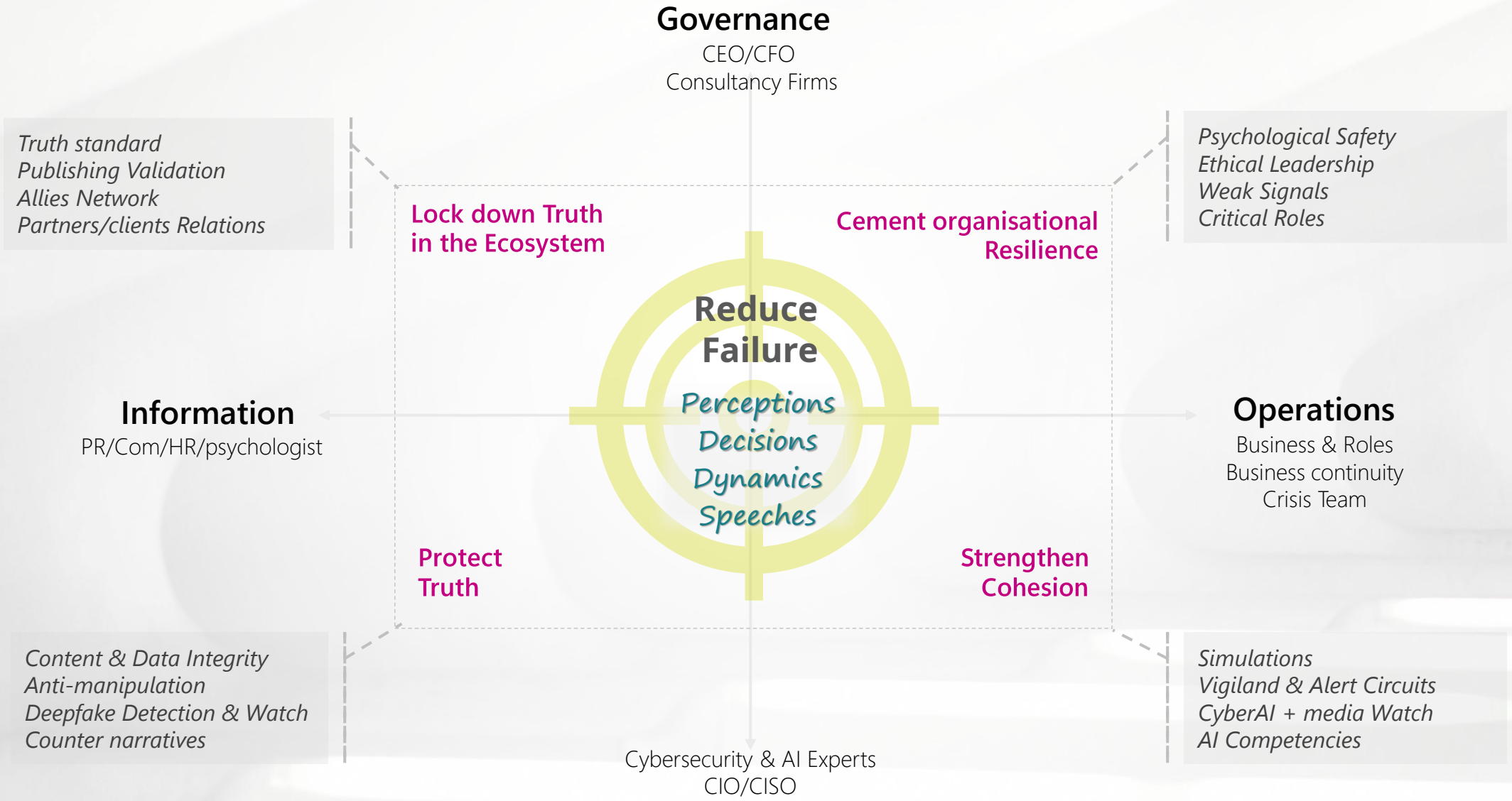
Help organisations face crises where cyberattacks and information manipulation combine…

… in an interconnected world, shaped by growing geopolitical tensions.

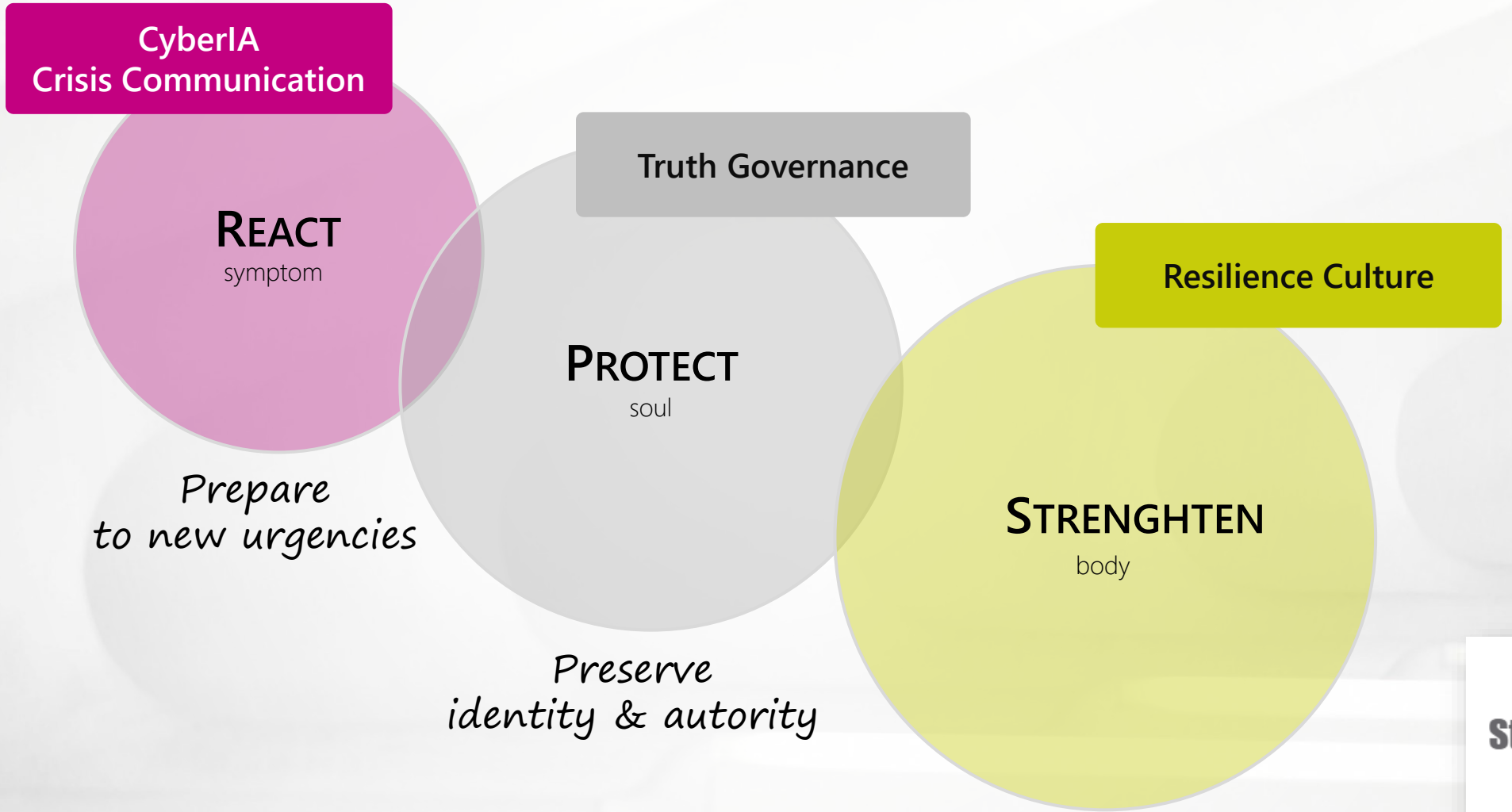
This requires a thorough understanding of three key dimensions:

- maintain a reliable reading of reality
- decide in situations of uncertainty
- maintain organisational coherence

Our area of operations



THE ARCHITECTURE OF SERVICES



Act Right
Stand Strong
with Audacity

We cover the invisible attack surface

ozngo

+60% Covered

IT Infrastructure

Systems

≈30% Covered

AI Gouvernance

Traditional Crisis Management

Crisis Simulations

Cyber + AI + Media Watch

Cyber-Training/Social engineering

<10% Covered

AI Manipulation (deepfake, vishing)

Vigilance, Detection & Alert Circuit

Information/content Integrity

Psychological Safety

Weak Signals

Organisational Resilience

Unique
Area of operations

Systemic
Approach

Attacks exploit **interactions** and **perception gaps**.
We work on these **dynamics**, **internal and external**.

THE STRATEGIC VULNERABILITY ASSESSMENT

Identify your real breaking points, and the gap between what leadership perceives and what teams experience.

1 Online questionnaires

Leaders
Strategic vision
Governance
Decision-making

Teams
Fields perception
Weak signals
Lived vulnerabilities

1 week

2 Interviews

Individuals
Critical roles
Targeted deep-dive

Group
Validation des décalages identifiés

1-2 days on site or remote

3 Delivrables

- Vulnerability mapping by dimension
- Leadership vs. field gaps highlighted
- Communication dynamics mapping
- 3-5 actionable priorities
- Executive debrief

10 day | Outline of a personalised action plan | Roadmap to maturity

WHO IS OZ'N'GO

Your Partner in Crisis Communication & Information Integrity

Maryse Rebillot

Strategic advisor on Cyber-AI crises and information integrity | Founder of Oz'n'gO |

- 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

ozngo

Maryse Rebillot

rebillotm@ozngo.com

+41 77 533 77 67

www.ozngo.com