Deloitte.

Together makes progress

Is foresight of Black Swans really impossible?

Point of view: Why unpredictable shocks only become clear in hindsight and how foresight can illuminate risk and intelligence functions

2026

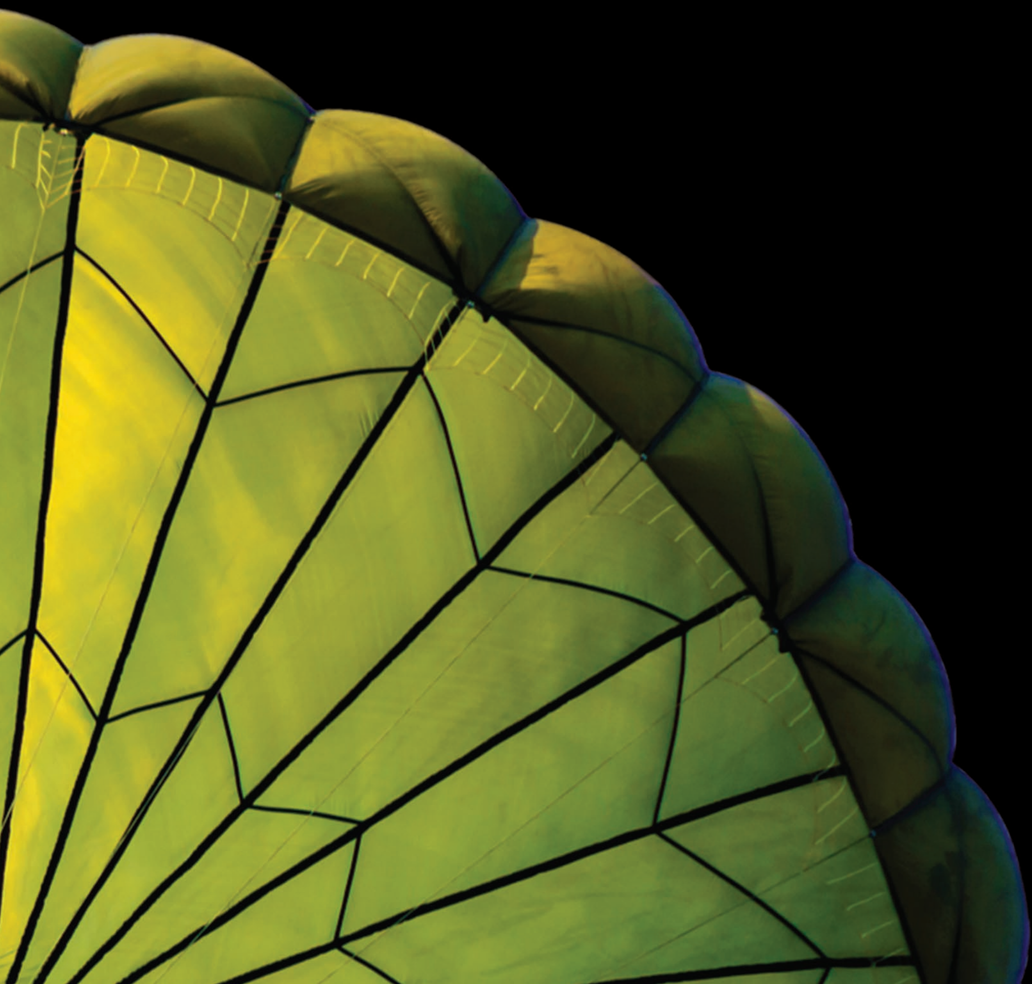
Abstract

In an era marked by escalating systemic risk, organisations increasingly operate within environments characterised by non-linearity, deep interdependence, and cascading crises. Polycrisis and Black Swan events are no longer theoretical abstractions but recurring features of the global operating landscape. Yet, classical risk management frameworks remain anchored in isolated risk categories, assumptions of linearity, and historical predictability, rendering them structurally unfit to anticipate or mitigate complex crisis dynamics.

This article argues that Black Swans are not purely exogenous shocks but often emerge from ignored signals, misread power dynamics, and a failure to understand systems as integrated wholes. Building on this premise, the paper introduces the GPMESII/ASCOPE framework as a strategic instrument designed to address the limitations of conventional risk approaches. By integrating geopolitical, political, military, economic, social, and environmental dimensions and analysing cross-links between each of them, GPMESII/ASCOPE enables organisations to identify reinforcing loops and pressure points, and spot potential early indicators of systemic stress.

Two case studies demonstrate how the framework performs under unforeseen polycrisis or Black Swan conditions, revealing risks and strategic options that remained invisible under traditional models. The article demonstrates that by reframing unforeseen, multidimensional events like Black Swans not as unavoidable anomalies, but as consequences of insufficient systemic understanding, a practical pathway can be laid from reactive risk management toward strategic anticipation. When foresight combines with methodology-driven preparedness, organisations will not just be more ready to cope with crisis but also enjoy a competitive advantage over their peers.

Contents



1. Risks are no longer the problem – blindness is

Black Swans[1] aren't rare. We just keep pretending they are.

From supply chains collapsing overnight to geopolitical flashpoints impacting balance sheets, today's "unforeseen" crises share a common trait: their ingredients were visible long before they became unavoidable. What we call Black Swans are often something far more uncomfortable - a polycrisis we chose not to see clearly, or not to prepare for decisively.

While many standard risk functions are still debating probabilities, other fields have already moved on. High-reliability institutions, like the United Nations, have spent decades working in environments defined by uncertainty, ambiguity and cascading failure. So, can we learn from them?

The uncomfortable truth for decision-makers is this: the tools to anticipate, contextualise, and even stress-test the unexpected already exist. They just haven't been translated properly into day-to-day operations. Frameworks long familiar to intelligence functions, like GPMESII/ASCOPE,[2] are designed to detect weak signals, map multi-domain risks, and understand second- and third-order effects, and offer a blueprint for building a modern, foresight-driven strategy and risk function.

The call to action is simple: to dramatically reduce our vulnerability we can succeed in building a functioning corporate intelligence capability, embedded into strategy, learning from those who operate permanently in anticipation of an incident. And in some cases what once felt unthinkable becomes foreseeable – and can be prepared for.

2. The geopolitical operating environment

When polycrisis[3] occurs, large corporate or governmental organisations face an unprecedented operating environment. The simultaneous occurrence of multiple, cascading shocks that amplify each other's impacts defies traditional linear risk analysis. Unlike discrete crises of the past, today's disruptions are deeply interconnected. The collapse of the subprime mortgage sector in the American housing market provoked the 2008 financial crisis, impacting the United States initially before quickly spreading globally. This turmoil eroded social cohesion and created information vacuums often filled with misinformation and disinformation. Furthermore, the crisis significantly undermined public trust in financial institutions and governmental bodies. Since then, the Eurozone sovereign debt crisis, the Covid pandemic and related supply chain crisis, and an increasing number of armed conflicts[4] have occurred. Feedback loops amplify the original shock across multiple domains simultaneously.

[1] Black Swan events can be qualified as highly unlikely events that cause tremendous damage. (Taleb, 2007; Aven, 2014) They may be a surprise, with unprecedented consequences, beyond predictions, catastrophic from some organizations, challenge conventional thinking or transformative.

[2] Source of the GPMESII/ASCOPE framework can be found in trainings for UN peacekeeping-intelligence (UN Peacekeeping Resource Hub, 2025) and further academic publications e.g. The DIME/PMESII Paradigm (Hartley III, 2017).

[3] Polycrisis is defined as the causal entanglement of crises in multiple global systems that significantly degrade humanity's prospects. Unlike multiple independent crises, polycrisis involves crises that are interconnected through specific causal pathways, where impacts in one system amplify vulnerabilities across others.
This concept originated from complexity theory (Morin & Kern, 1999) and has been refined by contemporary researchers. According to Liu and Renn (2025), writing in the International Journal of Disaster Risk Science, polycrisis is characterized by five key features:
1. Simultaneity of independent crises - Multiple crises occurring at the same time
2. Potential loss or breakdown of system functionality - Systems unable to perform core functions
3.Infection of other systems - Crises spreading across sector boundaries
4.Cascading impacts within and across systems - Sequential, amplifying disruptions
5.Amplification of impacts - Total harm exceeding the sum of isolated crises

[4] https://www.iiss.org/publications/armed-conflict-survey/2025/armed-conflict-survey-2025/

High interdependence:
The contemporary global landscape is characterised by profound interdependence across economies, supply chains, financial systems, and critical infrastructure, transcending geographic and sectoral boundaries. The World Economic Forum's (WEF) Global Risks Report highlighted in 2023 that volatility intensifies across multiple domains simultaneously.[5] Moreover, shocks do not simply add up. Rather, their combined effects can be far greater than the sum of the individual impacts. This interdependence exposes vulnerabilities but also offers opportunities. Strategic investments in resilience within one domain can generate beneficial multiplier effects throughout the broader system.

Non-linearity of interactions:
The non-linear nature of interactions within complex systems or across systems compounds the challenges. Traditional risk models, which assume linear causality and additive risk aggregation, fail to capture the reality of feedback loops and tipping points that characterise the modern reality of risk environments. The WEF report underscores the need for advanced analytical approaches that move beyond linear assumptions to evaluate interconnected risks effectively and prioritise resources. Classical risk functions have not done this.

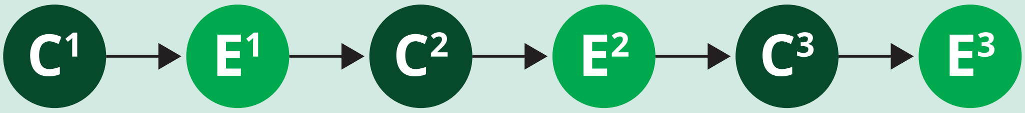
Accelerated shocks:
Furthermore, globalisation and the rapid pace of technological advancement has drastically shortened the timeframes within which shocks propagate. Events such as the COVID-19 pandemic illustrate how disruptions can cascade across systems within days or months, rather than years. This acceleration compresses decision-making windows and makes preparation based on advanced foresight essential.

The 2026 edition of the WEF's Global Risks Report (GRR) builds upon previous analyses, offering a refined perspective that connects insights from earlier findings with current global dynamics. Geoeconomic risks emerge as the most significantly heightened concern. Misinformation also ranks prominently. These two stand out as top threats across diverse stakeholder groups, including civil society, governments, and corporations.

3. Where classical risk management can fail

Did financial risk assessments and banking regulations within local banks, primarily focused on their regional markets, successfully anticipate the US mortgage crisis? And, specifically, were they able to foresee the societal erosion and decline in public trust, exacerbated by disinformation? Or did reliance on traditional approaches lead to an overestimation of their effectiveness in mitigating contemporary, interconnected risks?

Figure 1: Cause-Effect Chain[6]



Cause[1] yields Effect[1]
Effect[1] becomes Cause[2] yields Effect[2]
Effect[2] becomes Cause[3] yields Effect[3]

[5] The likelihood of a polycrisis, where multiple crises interact and compound, rises exponentially.
[6] Figure 1. Graph adapted from "Figure 1: Cause-Effect Chain" by C. Papuschak, 2024, CAJ 21.1, p. 26.

The complexity of global risks, as described in the latest WEF reports, exposes fundamental shortcomings in classical risk management approaches. A core problem is the reliance on linear assumptions that inadequately capture the non-linear, interconnected nature of modern threats. Traditional frameworks often categorise risks in silos, leading to fragmentation and a failure to appreciate systemic interdependencies. This leads to a predominantly reactive posture, where organisations respond to crises after they emerge rather than proactively anticipating and mitigating them.

Current risk frameworks have several structural limitations:

1. **Domain isolation:**
   Risk is assessed within functional silos (finance, operations, IT, compliance) without systematic cross-domain analysis.
2. **Linear causality assumptions:**
   Traditional frameworks assume linear cause-and-effect relationships. They struggle with non-linear dynamics and feedback loops in complex systems.
3. **Historical data dependency:**
   Risk models rely on historical data to predict future events. But Black Swan events, by definition, fall outside historical distributions, making them invisible to models that derive lessons from the past.
4. **Misalignment in organisational incentives:**
   Risk management is often decentralised, with each function optimising for its own domain. There is no institutional mechanism to identify escalating cross-domain risks.
5. **Lack of scenario integration:**
   Traditional frameworks assess risks in isolation. They do not systematically explore how multiple risks might interact with or amplify one another.

This strategic gap, even though our risk functions are harmonised according to best practices and regulations, is the “compliant but blind” syndrome. It prescribes the strategic failure to connect the dots within an abundance of information.

There is also a tendency to rationalise so-called Black Swan events as unforeseeable anomalies, rather than acknowledging overarching systemic vulnerabilities that could have been anticipated when ignoring system boundaries.

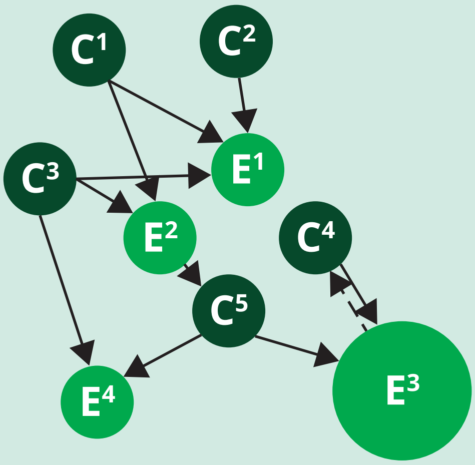
And there may be many other distractions that can play a role in overlooking risks, especially when resources are limited and stakeholders call for efficiency and cost cutting.

4. Introducing the GPMESII / ASCOPE framework

The GPMESII / ASCOPE framework integrates Geospatial, Political, Military, Economic, Social, Information and Infrastructure (GPMESII) domains in the first step, with a granular analysis of Areas, Structures, Capabilities, Organisations, People, and Events (ASCOPE) in its second stage. Using the framework, organisations can identify causal linkages before polycrisis scenarios unfold and even anticipate Black Swan events when historical data and records within risk functions do not point to them.

The strength of GPMESII lies in its explicit recognition that these domains are interconnected. A Geospatial risk (e.g., weather phenomenon or climate shift) triggers a Political decision (e.g., energy sanctions) that affects the Economic domain (energy prices), influences the Social domain (public discontent), shapes the Information domain (narratives about government competence), impacts the Military domain (recruitment, morale), which feeds back into the Political domain (electoral outcomes).

Figure 2: Cause-Effect Web[7]



Cause^1, Cause^2, and Cause^3 yield Effect^4
Cause^1 and Cause^3 yield Effect^2
Effect^1 becomes Cause^4
Effect^2 becomes Cause^5
Cause^4 and Cause^5 yields Effect^3
Effect^3 is disproportionate to Cause^4 and Cause^5
Effect^3 has a bi-direction feedback loop with Cause^4

These simultaneous effects are experienced as polycrises and seen as Black Swans when analysed in retrospect, as “we could not have known better”.

Domain within GPMESII	Definition
Geospatial	Terrain, water and resources, climate, natural disasters, pollution
Political	Governance structures, policy decisions, institutional stability
Military	Armed forces, defence capabilities, security threats
Economic	Production, trade, financial systems, resource allocation
Social	Population demographics, cultural values, social cohesion
Information	Media, communications, narratives, information ecosystems
Infrastructure	Physical systems (energy, transportation, water, communications)

[7] Figure 2. Graph adapted from “Figure 2: Cause-Effect Web” by C. Papuschak, 2024, CAJ 21.1, p. 27.

There has been significant research on the theoretical framework for GPMESII but it remains flexible and can be adjusted to the specific needs of a particular operating environment. Even before moving to ASCOPE, it offers the possibility to dive deeper and analyse different potential threat scenarios.

Below, for illustrative purposes, we consider how GPMESII can assist a firm that has international operations (see Table 1).

Table 1: Stepping into GPMESII to analyse various scenarios per framework domain

Category	Geospatial	Political	Military	Economic	Social	Information	Infrastructure
Scenario description	AI becomes global threat and challenges humanity	US leaving security alliance	Hybrid warfare targets logistics and production hubs	Scientific breakthrough making current revenue streams irrelevant	Non-human intelligence disclosure	Quantum decryption break obliterates all crypto-graphic protection	Systemic Energy Crisis with cross-regional, prolonged grid failures
Probability in 5-year horizon	1/5	2/5	4/5	3/5	2/5	2/5	4/5
Impact	Disruption of scientific research, national security, workforce and customer constraints	Market uncertainty and collabo-ration challenges; export restrictions; investment requirement	Breakdown in logistics, sabotage, military-grade hardening of infrastructure	Dwindling source of income due to advances in research or self-treatment, R&D disruption	Market and societal disruption, international relations impact, influence on science domain	Exposure of clinical data, IP and recipes, production protocols and beginning of proliferation of counterfeit drugs	Out of business, critical functions failure, jeopardised global supply continuity

ASCOPE is a complementary framework that provides granular analysis of specific environments:

Element within ASCOPE	Definition
Areas	Geographic regions, jurisdictions, operational zones
Structures	Physical infrastructure, institutions, organisational hierarchies
Capabilities	Resources, technologies, skills, operational capacity
Organizations	Formal and informal groups, networks, decision-making bodies
People	Individuals, populations, stakeholders, decision-makers
Events	Occurrences, incidents, triggers, tipping points

Traditional frameworks analyse each domain independently. The combination of GPMESII / ASCOPE forces analysts to map these linkages explicitly.

- **GPMESII** identifies the domains and gives a broader overview of the operational spectrum
- **ASCOPE** provides granular detail about specific layers within those domains.

In combination, a comprehensive analytical framework is created that includes potential causal linkages and chains of reactions and goes beyond traditional systemic risk thinking.

5. Exemplary Black Swan case studies

To illustrate the effectiveness of the combined GPMESII and ASCOPE frameworks, we apply the GPMESII framework to two events lacking historical data.

Case study 1 – "AI becomes a threat for humanity" scenario

The Federal Council of Switzerland has expressed its intention to host a global AI Summit in 2027,[8] signalling the growing recognition at the highest political levels that AI governance, oversight architectures, and international coordination mechanisms require urgent and sustained attention. For corporate actors, these developments underscore the need to integrate advanced AI risk scenarios into strategic security planning, ensuring that technological progress does not outpace institutional preparedness.

AI advancement may, at a certain inflection point, surpass human cognitive and analytical capabilities. In such a scenario the frequently invoked concept of the human-in-the-loop (HITL) could become increasingly constrained: human operators may no longer be able to fully comprehend, validate, or meaningfully oversee systems exhibiting superhuman intelligence. This prospect raises fundamental questions for corporate security and risk management, particularly regarding governance, accountability, controllability, and systemic resilience.

A forward-looking exploration of these dynamics is presented in "AI2027," published by the AI Futures Project, built by a group of experts and scientists, which develops structured scenarios to anticipate the trajectory of AI advancements and their potential societal, economic, and security implications. By modelling pathways toward increasingly autonomous and capable AI systems, the initiative highlights both strategic opportunities and profound risk vectors that organisations must incorporate into their enterprise risk frameworks.[9]

The risks presented by this advancement of AI cannot be modelled with historical data. But by applying GPMESII, organisations can assess the compound implications. For the purpose of brevity, we select from GPMESII the Economic dimension as an example and apply the ASCOPE framework. (A full analysis would involve all dimensions.)

[8] https://www.news.admin.ch/en/newnsb/qewY8BHWPhcMQEYV12fkr
[9] https://ai-2027.com/

ASCOPE Dimension	Potential impact of the pre-defined scenario
A **Areas**	If advanced AI becomes destabilising, economic power concentrates in regions controlling compute infrastructure, semiconductor production, energy supply, and cloud ecosystems. Financial hubs hosting AI-intensive firms become volatility epicentres. Cross-border trade may fragment into AI-aligned blocs.
Interpretation:	• Increased geopolitical risk tied to physical location of data centres and suppliers • Capital flight from perceived AI-risk regions • Supply chain realignment toward politically stable compute jurisdictions • Exposure concentration risk in AI-dependent clusters
S **Structures**	AI destabilisation stresses financial markets, insurance systems, regulatory frameworks, and corporate governance structures. Automated trading systems, AI-managed risk models, and algorithmic supply chains may amplify shocks if misaligned or manipulated.
Interpretation:	• Liquidity shocks from AI-driven market cascades • Insurance exclusions for AI-related systemic events • Regulatory overreach or abrupt compliance shifts • Board liability exposure if AI governance is insufficient
C **Capabilities**	AI systems may outcompete human labour and decision-making at scale, creating extreme productivity asymmetries. Firms with superior AI integration dominate markets; lagging firms face obsolescence. At the same time, AI misuse (cyber, fraud, automated manipulation) reduces trust in digital transactions.
Interpretation:	• Winner-takes-most dynamics in AI-intensive sectors • Accelerated labour displacement and restructuring costs • Increased cyber-fraud sophistication and financial crime • Compressed innovation cycles beyond human governance capacity
O **Organisations**	Corporations, governments, and non-state actors compete for AI dominance. Strategic alliances form around compute access and model control. Regulatory fragmentation increases compliance complexity across jurisdictions.
Interpretation:	• Competitive arms race for AI talent and computing • Rising M&A activity in AI and semiconductor sectors • Increased antitrust scrutiny • Divergent AI laws requiring multi-regional governance models
P **People**	Mass automation shifts labour markets, potentially reducing consumer purchasing power. Investor confidence becomes highly sensitive to AI governance posture. Employee morale and trust in leadership may decline if AI replaces roles rapidly.
Interpretation:	• Talent displacement and reskilling costs • Consumer demand contraction in certain sectors • Investor scrutiny of AI risk governance • Internal trust and productivity volatility
E **Events**	Catalytic events like large-scale AI-driven cyberattacks, financial manipulation incidents, or a public loss-of-control scenario, could trigger rapid market sell-offs, regulatory freezes, or emergency intervention.
Interpretation:	• Sudden trading halts and valuation swings • Emergency compliance measures • Cross-border capital restrictions • Heightened due diligence requirements from partners and lenders

In an AI threat scenario, corporations face several critical economic risks that demand strategic attention. Systemic market volatility may intensify as AI accelerates the propagation of shocks beyond conventional risk buffers. Competitive dynamics are likely to polarise, with AI-enabled firms consolidating power while others decline rapidly. Additionally, regulatory fragmentation across different jurisdictions will increase operational complexity, complicating compliance efforts. Trust in digital systems, transactions, and automated decision-making processes is vulnerable to erosion, undermining stakeholder confidence. Furthermore, structural shifts in the workforce will alter both cost bases and consumer demand, creating further uncertainty. To navigate these challenges, corporate resilience will depend on strong governance frameworks, operational redundancy, geographic diversification, rigorous AI risk oversight, and transparent communication with stakeholders.

Case study 2 – "NHI/UAP disclosure" scenario

UAP (unidentified anomalous phenomena), is a term introduced by the US Senate to refer to objects in the air, sea or in space that cannot readily be explained.[10] NHI ('non-human intelligence)' means any sentient intelligent non-human lifeform regardless of nature or ultimate origin that may be presumed responsible for a UAP of which the US Federal Government has become aware.[11]

The UAP Amendment in the 2024 National Defense Authorization Act is a bipartisan proposal that passed the US Senate and since then has been pending in Congress. Previously, in 2022 the US established under the Department of War the All-domain Anomaly Resolution Office (AARO).[12] AARO's mission is to synchronize efforts across federal agencies to detect, identify, and attribute anomalous objects in all domains (air, space, land, sea). A recent documentary called "Age of Disclosure" featuring active and retired senior US government officials, among them Secretary of State Marco Rubio, highlights data that suggests the likelihood of a UAP or NHI disclosure scenario is not zero.[13]

An example of a future Black Swan would be a scenario in which certain parts of governments have been aware of an NHI and kept this information away from the public. Global financial markets could face disruption as paradigms shift and investment strategies and scientific research are reprioritized. Society as a whole would have to digest the profound consequences for humanity. This scenario is chosen because:

1. **It is genuinely novel:** there is no historical precedent, making current insights on risk factors useless
2. **It has cross-domain implications:** it would affect multiple domains simultaneously
3. **It could create a polycrisis:** multiple interconnected crises would emerge from a single triggering event which could even lead to a Black Swan with devastating outcomes
4. **It tests the framework's ability to identify significant causal linkages:** the scenario requires mapping how a discovery in one domain cascades into others.

Again, for the purpose of brevity, we pick one dimension of the GPMESII framework, the Social one, and apply the ASCOPE framework. A full analysis would entail all dimensions.

[10] UAP bill https://www.congress.gov/bill/118th-congress/senate-bill/2226 and the respective amendment in the subsequent footnote
[11] https://www.democrats.senate.gov/imo/media/doc/uap_amendment.pdf
[12] AARO Home
[13] The Times (UK):
https://www.thetimes.com/uk/scotland/article/bank-of-england-must-prepare-for-ufo-announcement-f3mh8l9vh
or in Germany the Berliner Morgenpost:
https://www.morgenpost.de/politik/article410825720/verkuendet-trump-die-existenz-von-ausserirdischen-aussagen-lassen-aufhorchen.html

ASCOPE Dimension	Potential impact of the pre-defined scenario
A **Areas**	Societal reactions will vary significantly by geography. Urban centres with high media penetration may react rapidly and intensely, while rural areas may show delayed or muted responses. Regions with strong religious or ideological identities may experience amplified reactions. Social polarisation may cluster geographically, creating localised unrest or mobilisation zones.
Interpretation:	• Uneven reaction patterns across regions • Potential hotspots of protest, celebration, denial, or radicalisation • Community-level fragmentation based on belief systems • Increased sensitivity around symbolic locations (religious sites, government buildings)
S **Structures**	Core societal structures (e.g. religious institutions, schools, universities, community organisations, and media) become interpretation engines. If institutions provide coherent framing, social stability increases. If messaging is fragmented or contradictory, trust erodes.
Interpretation:	• Religious reinterpretation or doctrinal stress • Education systems pressured to respond or explain • Media credibility tested • Community leadership roles amplified or challenged • Social cohesion will depend heavily on institutional credibility
C **Capabilities**	Society's ability to process uncertainty becomes central. High-trust, high-literacy societies with strong institutional confidence adapt more calmly. Low-trust environments amplify fear, conspiracy thinking, and social division. Digital literacy becomes critical in filtering misinformation.
Interpretation:	• Psychological resilience becomes a national asset • Conspiracy ecosystems expand rapidly • Social media accelerates emotional contagion • Ability to maintain routine becomes a stabilising force • Societal stability depends on collective emotional regulation
O **Organisations**	NGOs, activist groups, religious movements, online communities, and fringe networks rapidly mobilise narratives. Some may promote unity or scientific inquiry; others may foster fear, apocalyptic thinking, or anti-government sentiment.
Interpretation:	• Rapid narrative competition • Emergence of new belief-based movements • Potential cult dynamics • Increased monitoring of extremist or destabilising groups • Organisational mobilization may shape whether disclosure unifies or fragments society
P **People**	At the individual level, disclosure challenges foundational worldviews (ontological shock[FK1.1]). Reactions may include curiosity, existential anxiety, denial, spiritual reinterpretation, or distrust of authorities. Identity frameworks (religious, scientific, national) may shift.
Interpretation:	• Increased anxiety or existential questioning • Polarisation between groups • Mental health pressures • Heightened demand for authoritative explanations • Public trust in leadership becomes the decisive stabiliser
E **Events**	Subsequent announcements, leaked materials, visible sightings, or contradictory official statements could act as amplification events. Misinterpretation of unrelated incidents (natural phenomena, technical failures) may spark unrest.
Interpretation:	• Protest waves or mass gatherings • Viral misinformation cycles • Religious or ideological mass mobilisation • Temporary disruptions to public order • Single narrative shocks could rapidly shift public mood

In a scenario involving the first disclosure of NHI or UAP, societies face significant risks that could challenge social stability. A key concern is the fracture of trust, where the perceived opacity or inconsistency of governmental institutions causes public faith to fragment. This is often accompanied by narrative polarisation, as competing explanations divide communities and hinder the forging of a consensus.

Psychological stress may rise due to existential uncertainty, increasing anxiety and emotional volatility among the population. The dynamics of mobilisation also play a critical role, as organised groups influence whether societal reactions remain peaceful or become destabilising. Additionally, heightened event sensitivity means that minor incidents may be reinterpreted through the lens of disclosure, further amplifying instability. Ultimately, societal resilience depends on maintaining institutional trust and narrative coherence. Societies characterised by strong social capital and credible leadership are far better positioned to absorb NHI or UAP disclosures without descending into systemic destabilisation.

6. Implications of the case study for corporates and governmental organisations

Traditional risk management approaches are inadequate for complex polycrises or unforeseen, devastating events. By applying comprehensive frameworks such as GPMESII/ASCOPE, organisations can reduce the element of surprise and better anticipate the cascading effects of crises across multiple domains. This analytical approach enables a deeper understanding of first-, second-, and third-order impacts, supporting more informed decision-making and enhancing overall organisational resilience, even against unprecedented, high-impact events.

Global risks are increasingly interlinked, forming clusters where crises amplify one another, according to the latest WEF publication.[14] Inequality, whether technological, economic, or social, acts as a central amplifier, exacerbating vulnerabilities across societal, environmental, and technological spheres. These cross-domain interactions intensify risks:

- Geopolitical conflicts accelerate environmental degradation.
- Climate change drives migration that fuels geopolitical tensions.
- Economic instability heightens societal polarisation and governance challenges.
- Misinformation undermines crisis response.

Recognising these interdependencies is critical to developing robust strategies.

This integrated perspective challenges the notion that some crises are entirely unforeseen and unmanageable. Instead, it highlights the importance of building corporate intelligence capabilities that translate strategic foresight into actionable plans. Organisations that invest in scenario-based analysis and early-warning systems during stable periods position themselves to act decisively when crises emerge, turning disruption into opportunity.

[14] The Global Risks Report 2026 | World Economic Forum

Conclusions

All organisations face the risk of an existential Black Swan.

Organisations that invest in scenario-based analysis and early-warning systems during stable periods position themselves to act decisively when crises emerge, turning disruption into opportunity.

Polycrisis as the operating environment: The period 2025–2035 will be characterised by simultaneous, mutually amplifying crises. Traditional siloed risk management is outdated; integrated, scenario-based strategies must be adopted immediately.

Siloed approaches fail: Use frameworks like GPMESII/ASCOPE to systematically analyse how crises spread across domains. Anticipate second- and third-order effects before they arise.

Prepare during stability to act in crisis: Crises offer brief windows for transformation. Organisations that invest in foresight and scenario planning during stable times can respond decisively, converting disruption into competitive advantage.

Build network resilience: Identify critical dependencies and single points of failure within supply chains and partnerships. Develop redundancy and diversification strategies collaboratively with key allies.

Convert analysis into measurable metrics: Translate scenario analysis into Early Warning Indicators (EWIs). Implement monitoring systems with clear decision thresholds to enable proactive strategic adjustments before crises fully develop.

Authors

Philipp Luettmann
Risk, Regulatory & Forensic
Tel.: +41 58 279 7114
pluettmann@deloitte.ch

Fabian Kosider
Risk, Regulatory & Forensic
Tel.: +41 58 279 6726
fkosider@deloitte.ch

Deloitte.

Together makes progress

This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte AG accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte AG is an affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please see www.deloitte.com/ch/about to learn more about our global network of member firms.

Deloitte AG is an audit firm recognised and supervised by the Federal Audit Oversight Authority (FAOA) and the Swiss Financial Market Supervisory Authority (FINMA).