



La Cybersecurity non è più solo un problema IT. È una questione di sicurezza nazionale... e aziendale

WeSec 2026

Luca Boselli

Partner KPMG, Head of Cyber & Tech Risk



Recent megatrends and geopolitical risk drivers uncover new challenges in risk management

Defining Geopolitical Risks



Geopolitical Risks involve **emerging, unpredictable or hazardous events** with **political underpinnings** that could affect the strategic operations and activities of financial institutions.

Just like ESG risk, **geopolitical risks are risk drivers** which can directly or indirectly affect other risk types.

Concrete examples include:

- **Russia-Ukraine conflict**
- **Increasing threat due to national nuclear programs**
- **Middle East tensions**
- **Covid 19 pandemic response**

- Geopolitical risks are assessed through a **top-down approach**, starting with the analysis of **megatrends and trends**.
- Megatrends are **significant, slow-moving forces** that have a broad reach, longevity, and profound influence on economic, political, and social spheres. **The following two** should be closely looked at by businesses:

Global Fragmentation

- The world is transforming with **economic disengagement and new alliances**.
- Disruption of European peace drives protectionism, with possible manifestations including **Europe's economic isolation and rising tensions among major economies**.

Disruptive technologies

- Disruptive digital technologies are **destabilizing societies** at an accelerating pace.
- AI, social media, and other new tools **present both opportunities and risks**, including the unprecedented threat of technologies being used as **economic and political weapons**.



The Russia-Ukraine War **highlights global fragmentation**. Sanctions against Russia and its banks, companies, and individuals **have led to shifts towards self-reliance and changed alliances**, moving from **global unity to protectionism**. Possible outcomes include escalating geopolitical tensions or a de-escalation with a diplomatic resolution.

Developing a robust approach to geopolitical risks should prioritize selecting relevant risk drivers

Forecasting geopolitical risks

- Conduct **megatrend analysis** using diverse sources like social media, research (inclusive of **unconventional sources** like the economics department for risk controllers), and reports.
- Identify **relevant geopolitical risk drivers** from trends to then develop **impactful scenarios**.
- Multifaceted interactions between risk drivers **can increase scenario complexity unpredictably (Figure 1)**, highlighting the danger of ignoring geopolitical risks.
- Responding to geopolitical risks requires **understanding the complexity of the challenge**, determining necessary resources and expertise, and establishing a governance structure.
- Institution size, global reach, business model complexity, and strategy for dealing with geopolitical risks are **factors that influence the approach to addressing these risks**.

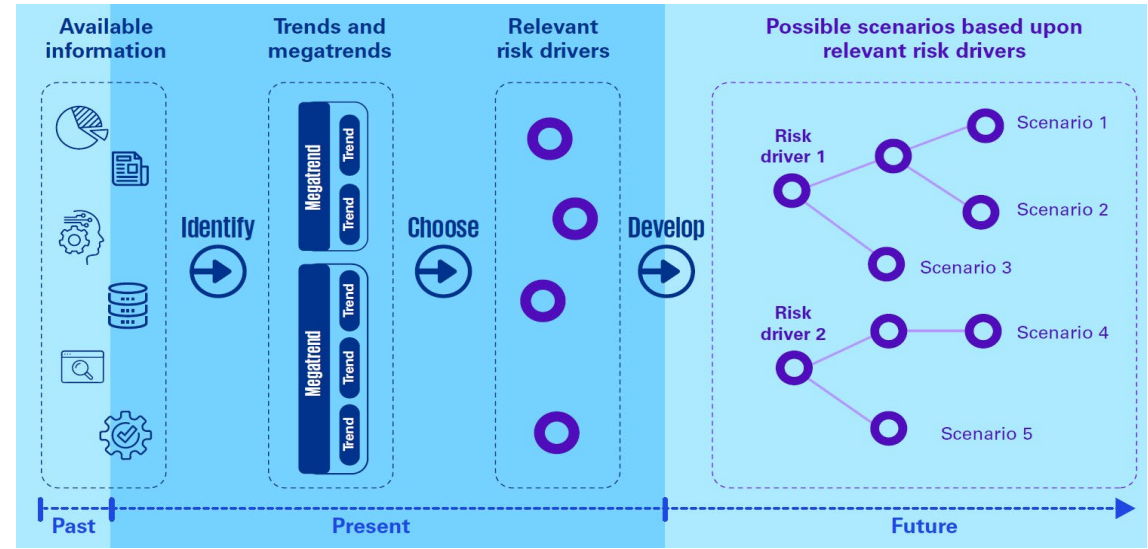


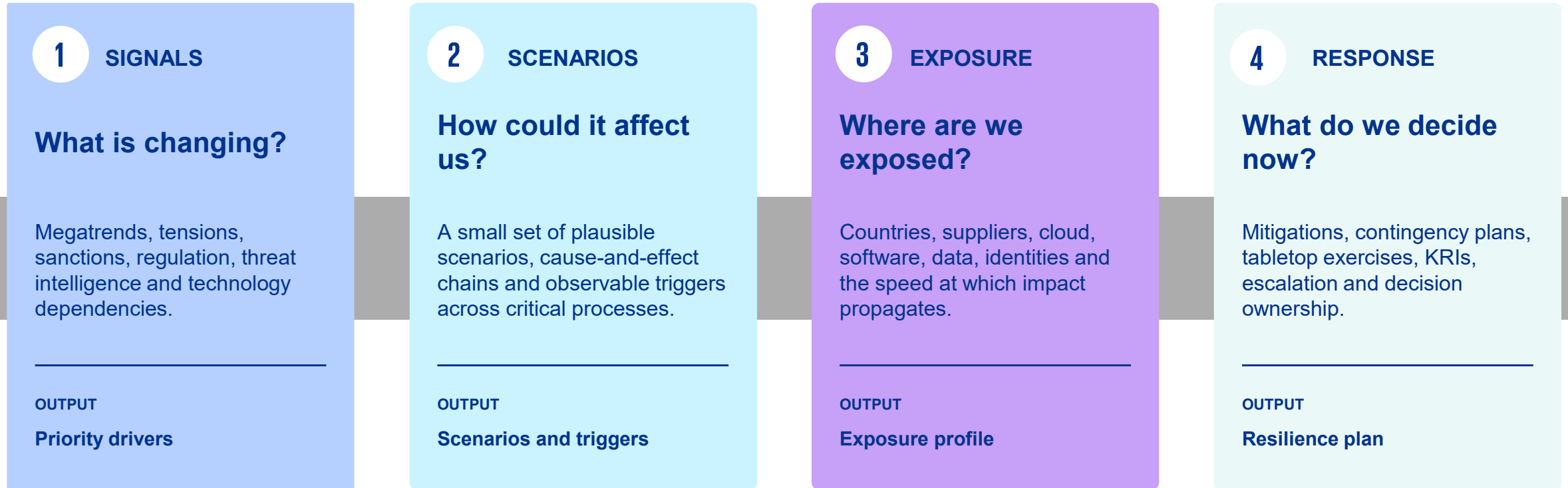
Figure 1 – Forecasting geopolitical risks

The focus is **neither on correctly calculating** the risk potential **nor the likelihood** of defined scenarios occurring. Instead, the objective is for business leaders to be **aware of relevant risk drivers** and to **actively address the resulting scenarios**.



Addressing geopolitical risks involves a structured initial analysis, recognizing that today's geopolitical instability **is a new norm, not a transient phase**. Begin by identifying a **few relevant risk trends and drivers**, conducting an **initial analysis**, and then **developing your approach**. With more experience, employ more sophisticated methods to identify central risk trends and drivers.

Analysis framework for turning geopolitical uncertainty into cyber priorities: from signals to decisions



Do not try to predict everything. Make dependencies visible, simulate impacts and prepare decisions.

Integrated governance (Business, Risk, CISO, Procurement, Legal, etc.)

La Comunicazione di Banca d'Italia e IVASS (1/2)

Comunicazione del 17.07.26 dei Regulator

Le tecnologie emergenti, e in particolare i sistemi di intelligenza artificiale, stanno trasformando il panorama della cybersicurezza e ponendo nuove sfide per le loro **possibili implicazioni per la riservatezza, l'integrità e la resilienza dei sistemi informatici e delle informazioni da essi gestite.**

In tale contesto, nel panorama finanziario e assicurativo italiano, **Banca d'Italia e IVASS** hanno inviato una comunicazione al mercato in cui segnalano la necessità che gli intermediari pongano in essere misure per **rafforzare la resilienza operativa digitale evidenziando che il rafforzamento della resilienza operativa digitale non rappresenta soltanto un'esigenza di conformità, ma una condizione essenziale per assicurare la continuità aziendale e la capacità di offrire servizi finanziari affidabili.**



COMUNICAZIONE AL MERCATO IN MATERIA DI RESILIENZA OPERATIVA DIGITALE E MODELLI AVANZATI DI INTELLIGENZA ARTIFICIALE

Le tecnologie emergenti, e in particolare i sistemi di intelligenza artificiale, stanno trasformando il panorama della cybersicurezza e ponendo nuove sfide per le loro possibili implicazioni per la riservatezza, l'integrità e la resilienza dei sistemi informatici e delle informazioni da essi gestite, anche nel settore assicurativo.

In particolare, i modelli di ultima generazione hanno la capacità di identificare le vulnerabilità dei sistemi *software* e generare contemporaneamente le relative modalità di sfruttamento in tempi estremamente ridotti e senza la necessità di specifiche competenze tecniche. Ciò comporta una sensibile riduzione dell'intervallo temporale tra l'individuazione delle vulnerabilità e il loro sfruttamento, con conseguente incremento dei rischi di subire attacchi cyber efficaci.

Le nuove tecnologie di intelligenza artificiale potrebbero, quindi, accrescere l'asimmetria tra attaccanti e difensori, a scapito di questi ultimi, tale da rendere necessario un adeguamento



Comunicazione al mercato in materia di resilienza operativa digitale e modelli avanzati di Intelligenza Artificiale

Le tecnologie emergenti, e in particolare i sistemi di intelligenza artificiale, stanno trasformando il panorama della cybersicurezza e ponendo nuove sfide per le loro possibili implicazioni per la riservatezza, l'integrità e la resilienza dei sistemi informatici e delle informazioni da essi gestite, anche nel settore finanziario.

In particolare, i modelli di ultima generazione hanno la capacità di identificare le vulnerabilità dei sistemi *software* e generare contemporaneamente le relative modalità di sfruttamento in tempi estremamente ridotti e senza la necessità di specifiche competenze tecniche. Ciò comporta una sensibile riduzione dell'intervallo temporale tra l'individuazione delle vulnerabilità e il loro sfruttamento, con conseguente incremento dei rischi di subire attacchi cyber efficaci.

La Comunicazione di Banca d'Italia e IVASS (2/2)

COMUNICAZIONE AL MERCATO: a chi è indirizzata?

la Comunicazione di **Banca d'Italia** è rivolta ai soggetti direttamente vigilati dal Dipartimento Vigilanza Bancaria e Finanziaria:

- Banche e gruppi bancari meno significativi (inclusa Bancoposta)
- Istituti di pagamento e istituti di moneta elettronica (IMEL)
- Imprese di investimento
- Fornitori di servizi per le crypto-attività
- Gestori di fondi di investimento alternativi e società di gestione (SGR)
- Fornitori di servizi di crowdfunding
- Intermediari finanziari ex art. 106 TUB

La comunicazione di **IVASS** è rivolta a:

- Imprese di assicurazione
- Imprese di riassicurazione

GLI ADEMPIMENTI RICHIESTI

- **Avvio dei lavori:** seduta congiunta del Consiglio di Amministrazione e del Collegio Sindacale per l'esame della Comunicazione.
- **Relazione articolata:** stesura di una Relazione, articolata per ciascuna delle sei aree indicate (cfr. slide successiva), che rappresenti il livello attuale di esposizione al rischio e l'adeguatezza dei presidi esistenti, individuando le principali carenze e le relative priorità di intervento.
- **Piano di lavoro:** definizione di un piano di lavoro allegato alla Relazione, con azioni, tempi e investimenti necessari, proporzionato al profilo di rischio e all'operatività dell'intermediario, incluse le modalità con cui il CdA ne verificherà l'avanzamento.
- **Punto di responsabilità:** individuazione e comunicazione alla Vigilanza di uno specifico punto di responsabilità aziendale (ad esempio, la funzione di controllo dei rischi ICT di secondo livello).
- **Trasmissione della Relazione, con il piano di lavoro allegato, entro il 31 dicembre 2026.**



Le sei aree di analisi e intervento

01

Governance

Revisione del RAF per rischi da tecnologie di frontiera

Presidi contrattuali sui fornitori ICT competenze AI nel board

La revisione del RAF per incorporare i rischi da tecnologie di frontiera, in coerenza con le decisioni strategiche e di investimento ICT è responsabilità degli organi con funzione di amministrazione e di gestione.

02

Igiene informatica

Approccio 'defence-in-depth'

Autenticazione e autorizzazione rigorose

Gestione granulare degli accessi

Segmentazione di reti e ambienti

03

Gestione delle risorse informatiche e della potenziale superficie d'esposizione

Inventari completi e affidabili

Classificazione per criticità ed esposizione internet/cloud

Modernizzazione legacy

04

Gestione delle vulnerabilità e degli aggiornamenti (patch)

Scansione evoluta anche con AI

Priorità a open source e sistemi esposti, incluse zero-day

05

Monitoraggio, rilevazione e misure di difesa

Rafforzamento del monitoraggio anche con AI per anomalie in tempo reale

Sincronizzazione con l'inventario

06

Attività di test

Test di resilienza operativa e di risposta/recupero allineati a DORA

Requisiti TLPT dove applicabili