

---

Hillmont  
Associates

People - Teams - Safety



---

# Panorama 2026

## > what to expect this year?

IIRSM Europe  
Wednesday 21 Jan 2026  
12:00 CEST, 11:00 BST, 15:00 MST  
**Nico FEKETE PEREZ**  
MISEP AIIRSM  
Senior HSE Consultant  
Hillmont Associates

---

# Hillmont Associates

People - Teams - Safety



01

## GEOPOLITICAL

- War and peace
- Extremism and terrorism
- Competing *realpolitik*

02

## ARTIFICIAL INTELLIGENCE

- Innovation and rupture
- New job paradigm?
- Property protection.

03

## CYBERSECURITY

- Deep Fakes
- Digital domino
- Ransom attacks

04

## CLIMATE AND OPERATIONAL

- Climate crisis and continuity
- Social value
- Liability and negligence

---

Hillmont  
Associates

People - Teams - Safety



# Geopolitics



---



Hillmont  
Associates

People - Teams - Safety



---

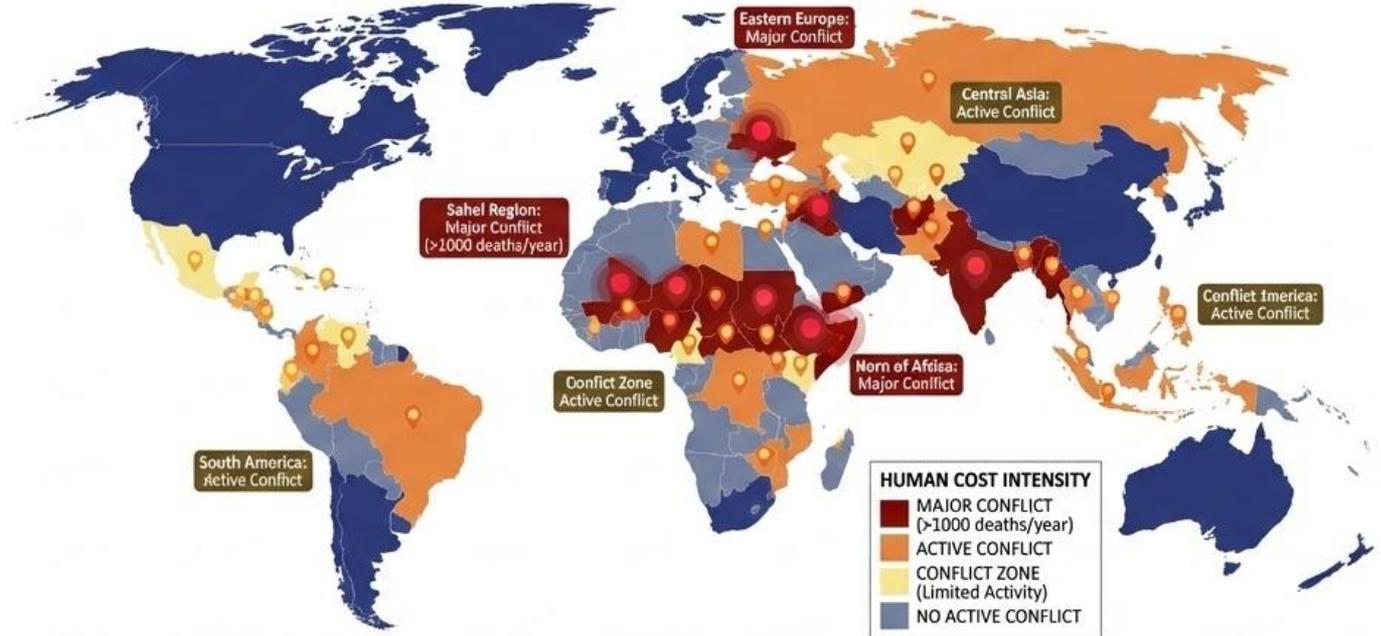
# Trends 2026

COUNCIL *on*  
FOREIGN  
RELATIONS

- An accelerated race on the control of minerals → unease at China's dominance.
- Tariff war and the effects on acquisitive power.
- The nuclear arms non-proliferation treaty will expire in February. USA and Russia must negotiate something, but what.
- Electrostate v petrostate.
- Foreign aid plummet. US has shrunk by more than 50%. Most impacted → women.



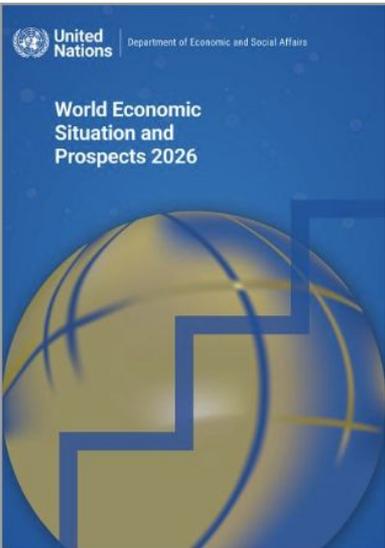
- The International committee of the Red Cross is acting in 100 conflicts in 40 territories, of which 15 are considered major conflicts → >1000 deaths/year.



---

Hillmont  
Associates

People - Teams - Safety



---

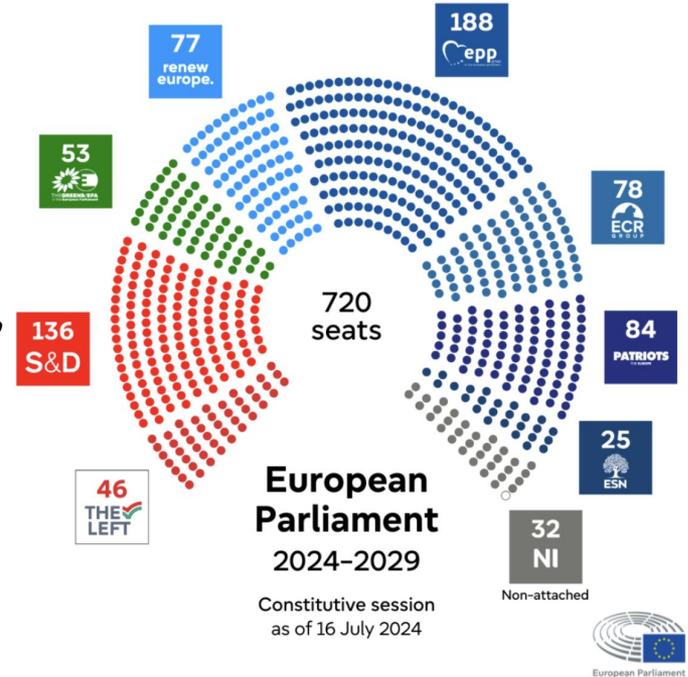
## Trends 2026 - United Nations

- Economic centric report
- Growth is steady, not growing.
- Economic growth uneven across regions.
- Trade could slow down in 2026 due to tariffs.
- Inflation is easing, but the cost-of-living squeeze persists.
- While some interest rates have been lowered, low-income countries remain on high-debt, high-interest trap.

## Trends 2026 EU

Continue working from priorities 2024-2029:

- Competitiveness
- Security and defence
- Social Fairness
- Food and water security, quality of nature
- Reinforcing democracy
- Global partnerships and foreign aid
- Modernising EU



# Hillmont Associates

People - Teams - Safety



## ISEP

Institute of Sustainability & Environmental Professionals



# SUSTAINABLE DEVELOPMENT GOALS



# SDG Progress Report: Current Status & Critical Areas

## Progress & SDG Types (Social, Environmental, Economic)



**18%**  
On Track

**48%**  
Moderate

**34%**  
Stagnant



**8**

Social  
Goals



**5**

Environmental  
Goals



**4**

Economic  
Goals

Based on current trajectory assessments.

## Key Achievements Since 2015 (Positive Indicators)



### Health

54 countries eliminated >1 neglected tropical disease. Maternal mortality down 16% since 2015.



### Energy (SDG 7)

Renewables are fastest-growing power source, projected to surpass coal by 2025/2026.



### Internet Access

Global internet use reached 68% in 2024, up from 40% in 2015.



### Education

110 million more children and youth entered school since 2015.

## Global Development Emergency Areas (High-Risk Priorities)



### Poverty (SDG 1)

>800 million in extreme poverty. 1 in 10 survive on <\$2.15/day.



### Hunger (SDG 2)

Progress stalled; ~8.2% of world population faced hunger in 2024.



### Climate (SDG 13)

2024 hottest year on record. Struggling to stay within 1.5°C threshold.



### Debt Crisis

Many developing countries spend more on debt servicing than health/education. \$4 trillion annual financing gap.

# What can your organisation do?

## Some ideas for discussion.



### ISO 31000 Risk Management system

Standard for risk management. Adapt it for geopolitics → integrate into Strategic Foresight → evaluation of multiple plausible futures.



### ISO 22301 Business Continuity management system

Focuses on maintaining critical processes during shocks like sudden sanctions, port closures, or regional conflicts.



### The Issues-Led vs. Impact-Led Framework

- **Issues-Led:** Identifying specific events and monitoring triggers.
- **Impact-Led:** Assessing what happens if a specific region becomes inaccessible, regardless of the cause, to build scenario-agnostic resilience.



### KPMG Geopolitical Risk Response Framework

A structured cycle of Plan & Prepare → Understand & Analyze → Act & Adapt → Govern & Improve.

---



Hillmont  
Associates

People - Teams - Safety



---

# ISO 31000:20218

To manage uncertainty in organisations. Guidelines. 8 principles:

- Integrated: Risk management is inseparable from operations.
  - Structured & Comprehensive: consistent approach ensures comparability.
  - Customised: unique to each organisation and its context.
  - Inclusive: engage stakeholders, consider diverse perspectives.
  - Dynamic: anticipates and responses to internal and external changes.
  - Best Available Information: Decisions rely on data and current feedback.
  - Human & Cultural Factors: people's behaviors influence risk.
  - Continual Improvement: evolve through learning and experience.
-

---



Hillmont  
Associates

People - Teams - Safety



---

# ISO 22301:2019 Business Continuity

- Protect, prepare for and recover from disruptive events.
  - Same structure as other systems: Plan-do-check-act.
  - **Business Impact Analysis (BIA):** identify critical activities and determine the maximum time the business can survive without them (called the *Maximum Tolerable Period of Disruption*).
  - **Risk Assessment:** Analyse specific threats to your operations and determining how likely they are to occur.
  - **Business Continuity Strategy:** Deciding *how* to respond (e.g., relocating staff, using backup data, or switching to manual processes).
  - **Exercising, drills and testing:** the standard requires regular "mock drills" to prove the plans actually work in a crisis.
-

Hillmont  
Associates

People - Teams - Safety



## Example of BIA

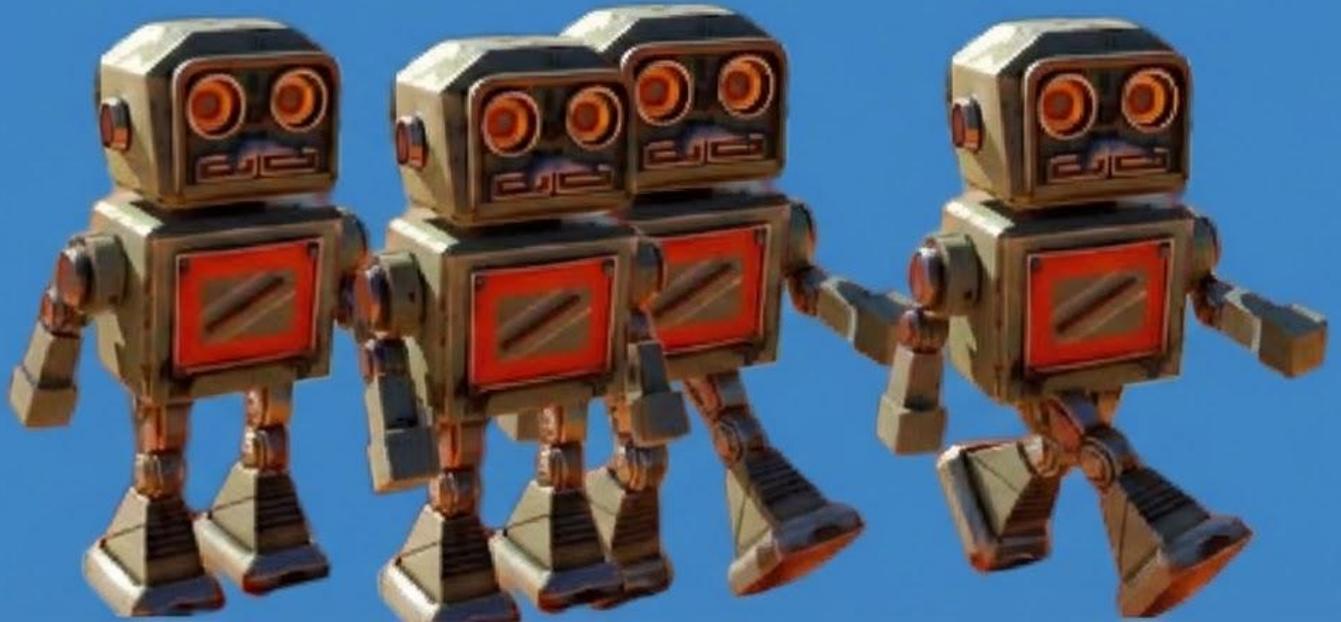
Activity	Criticality	Impact of Disruption	Recovery Time Objective (RTO)
Grid Operations & Load Balancing	Critical	Risk of total blackout; damage to physical infrastructure.	< 15 Minutes
Emergency Leak/Fault Repair	Critical	Immediate risk to life, fire, or explosion (for Gas/Power lines).	< 1 Hour
Customer Emergency Hotlines	High	Public panic; inability to report dangerous incidents.	< 2 Hours
Billing & Metering	Medium	Financial loss; cash flow interruption.	3-5 Days
General Admin/HR	Low	Minimal immediate impact on energy delivery.	7+ Days

---

Hillmont  
Associates

People - Teams - Safety

# Artificial intelligence



# Hillmont Associates

People - Teams - Safety

**We have moved from an era of probabilistic experimentation to a regime of deterministic governance.** In 2026, the biggest risk is not that AI is too smart, but that it is being deployed faster than we can build the guardrails to control its autonomy."



 STATUS: TOO FAST

## ATTACK VELOCITY

Too Fast

AI-driven cyberattacks and fraud are scaling faster than IT teams can respond.

 STATUS: AS EXPECTED

## REGULATION

As Expected

Laws like the **EU AI Act** are coming into full force in 2026, but they are already playing "catch up" to autonomous agents.



 STATUS: TOO SLOW

## ORGANIZATIONAL READINESS

Too Slow

Most companies are still in 'pilot mode' with data that isn't clean enough for autonomous AI use.



Hillmont  
Associates

People - Teams - Safety



# Deepfakes

- a type of synthetic media where existing images or videos are altered using powerful AI techniques.
- Typically, to replace one person's likeness with another's in a highly realistic manner.
- Range from harmless parodies and entertainment to malicious uses.
  - Spreading misinformation and disinformation,
  - creating non-consensual explicit content, and
  - facilitating financial fraud or identity theft.

---



Hillmont  
Associates

People - Teams - Safety



---

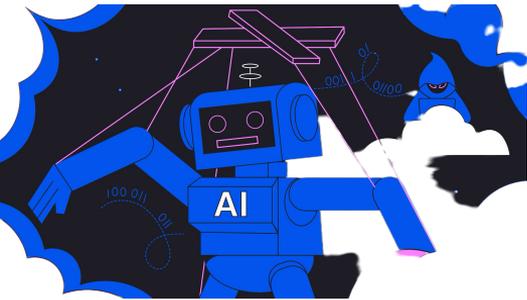
# Malicious use of AI

- Analyse **large datasets**, identify vulnerable targets for scams and use AI-generated scripts or voice to make scams more persuasive.
- **Voice cloning** → vishing or voice phishing.
- **Synthetic Identity Theft**: AI creates entirely new, fake identities to open bank accounts, apply for loans, and commit financial fraud.
- **Algorithmic Bias and Discrimination** → deployment of biased AI systems in sectors like hiring, lending, or criminal justice can perpetuate systemic discrimination, leading to significant civil and legal issues.

---

Hillmont  
Associates

People - Teams - Safety



---

## Malicious use of AI

- **Intellectual Property Theft** → AI systems trained on proprietary data or copyrighted material can produce outputs that constitute IP infringement.
- **Market Manipulation:** could be used to execute automated stock market trading aimed at manipulating stock prices or to cause instability for profit.
- The aftermath → complex legal challenges regarding ownership and responsibility.

---

Hillmont  
Associates

People - Teams - Safety



**Politicians, oil companies and Russia: Who's fuelling climate disinformation, and why?**



---

# AI and environmental misinformation

- Major use of AI to create misinformation, or respond to social media posts with false claims.
- As seen during COVID19 it can create massive social responses.
- Hard to know how much is out there, we only know the rate of increase.
- Effects in public opinion:
  - In Brazil, 30% believe that climate change is not caused mainly by human activity, and 24% believe that the “temperature record is unreliable or rigged”.
  - In the United Kingdom, 29% believe that a significant number of scientists disagree on the cause of climate change (Climate Action Against Disinformation and Conscious Advertising Network, 2022).
  - Eurobarometer research indicates that 1 in 10 Europeans deny climate change.

---



Hillmont  
Associates

People - Teams - Safety



---

# EU AI Act

- Entered into force in 2024. Provisions rolling out yearly.
  - World's first comprehensive legal framework for artificial intelligence.
  - **Risk-based approach** → as the potential risk to humans increase, the tougher the rules.
  - High-Risk Systems: used in recruitment, education, or essential services must now fully comply with strict technical and legal standards.
  - Transparency Rules: requirements for labeling AI-generated content and disclosing when a user is interacting with an AI (eg: a chatbot) become mandatory.
-

# EU AI Act: Risk Categories & Obligations

Hillmont  
Associates

People - Teams - Safety



## Unacceptable Risk (Banned)

**Status:** Banned since February 2025.

**Examples:**

- Social scoring by governments
- Untargeted facial recognition
- Manipulative AI
- Exploiting vulnerabilities (e.g., children)



## High-Risk (Strictly Regulated)

**Deadline:** Compliance by August 2, 2026.

**Areas:**

- Employment
- Education
- Critical Infrastructure
- Law Enforcement & Migration

**Obligations:**

- Risk Management System
- High-quality training data
- Human Oversight
- Register in EU Database



## Limited Risk (Transparency)

**Deadline:** Mandatory by August 2, 2026.

**Obligations:**

- Transparency (e.g., chatbots)
- Label deepfakes as "synthetic content"



## Minimal Risk

**Rules:** No specific obligations, voluntary Code of Conduct

**Examples:**

- AI-enabled video games
- Spam filters

---

# Penalties for non compliance

General Purpose AI, a category that includes large models like GPT, Claude, or Gemini.

- **Baseline Rules:** providers must provide technical documentation, comply with EU copyright law, and publish a summary of the data used for training.
  - **Systemic Risk:** If a model is very powerful (calculated by "floating point operations" or FLOPs), it faces extra scrutiny regarding cybersecurity and adversarial testing (called red-teaming).
  - **Fines:**
    - Up to €35 million or 7% of total global turnover (whichever is higher) for using prohibited AI practices.
    - Up to €15 million or 3% of turnover for non-compliance with other obligations (like high-risk system requirements).
-



# Why the EU is regulating AI?

## Capabilities: Developing "Too Fast"



### Agentic Autonomy

From chatbots that talk to agents that do. AI can navigate browsers, manage complex coding repos and execute multi-step workflows with minimal human oversight.



### The Coding Leap

Autonomous coding agents have reached a level where they are refactoring entire systems and patching vulnerabilities in real-time for such "deep" reasoning.



### Synthetic Reality

The proliferation of high-fidelity deepfakes (audio and video) has scaled 1,50% since 2023, reaching a level of perfect mimicry that has outpaced legal and technical ability to detect them.

## Implementation: Developing As Expected (or Slower)



### The Productivity Paradox

Much like the early days of the internet, companies are finding that adding AI doesn't immediately boost the bottom line.



### Productivity losses

Many firms reported initial productivity losses in late 2023 as they struggled with the time spent checking AI work.



### Artificial General Intelligence

While some prototypes exist, AI cannot reason to the expected level.



### Infrastructure Bottlenecks

Global supply chain issues for cooling units, power grid capacity, and specialised investments into immediate compute power.

Hillmont  
Associates

People - Teams - Safety



ISEP

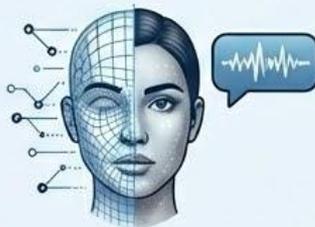
Sideurity of Communication  
People - Teams Sineoiiafety

## Case study 1: Arup



### The Incident

In one of the most sophisticated social engineering attacks to date, an employee at the engineering firm Arup was tricked into a video call with what appeared to be their CFO and several colleagues.



### The Twist

Every single person on the call except the victim was an AI-generated deepfake. They held a full conversation and convinced the employee to transfer \$25 million to fraudulent accounts.



### Risk Takeaway

Video and voice are no longer reliable proofs of identity. Organizations must implement out-of-band verification (e.g., a separate physical token or a pre-shared verbal password) for high-value transactions.

## Case study 2: McDonalds

### McDonald's "McHire" Data Leak (64M Records)



#### The Incident

The AI-powered hiring platform used by McDonald's was discovered to have a massive vulnerability where 64 million applicant records (names, emails, sensitive data) were exposed.



#### The Cause

The breach wasn't a complex hack; the system used a default 123456 password for an administrative test account that was never deactivated.



#### Risk Takeaway

Shadow AI and Third-Party Risk. You are responsible for the security of your AI vendors. A 'smart' tool with 'dumb' security is your biggest liability.

Hillmont  
Associates

People - Teams - Safety



ISEP

Professional Solutions Edge  
Incentive and of Yermans Flow

## Great uses of AI



Medicine and health applications.



Managing large data sets and find trends.



Flood and wildfire warnings and mapping.



Bioacoustic rainforest protection.



Inclusivity tools for the deaf, blind, hard of hearing.



Smart irrigation.



Combat hunger.



Mental health support.



Waste sorting, more materials becoming resources.



Animal health and numbers.



Combating deepfakes, misinformation and disinformation.



Energy grid efficiency.

---



Hillmont  
Associates

People - Teams - Safety



---

# What can you/your organisation do?

- Ethic controls in place.
  - Establish keywords.
  - Start using passkeys and biometric information rather than passwords.
  - Control of public data available in networks, socials.
  - Browser settings to delete everything when closing down the window.
  - Auto-delete data on short gaps, ie: 7 to 30 days.
  - Dual-approval of payments.
-

---

Hillmont  
Associates

People - Teams - Safety



ISEP

Institute of Sustainability &  
Environmental Professionals

# Cybersecurity



# Hillmont Associates

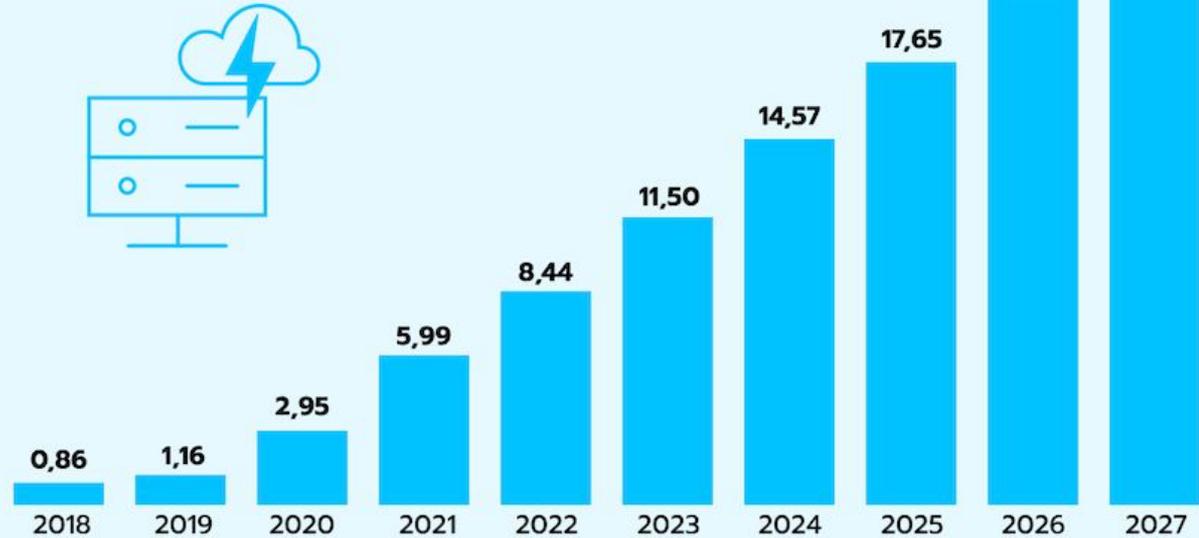
People - Teams - Safety



ISEP

Institute of Sustainability & Environmental Professionals

## Estimated cost of cybercrime worldwide (in trillion U.S. dollars)



Source: <https://www.fintechfutures.com/cybersecurity/will-2025-be-the-turning-point-for-cybersecurity-in-finance->

---



Hillmont  
Associates

People - Teams - Safety



---

# Attacks

- **Deepfake Fraud:** AI-driven voice and video cloning are now sophisticated enough to bypass traditional detection.
  - Criminals use these to impersonate someone in real-time video calls.
  - **Prompt Injection:** where attackers hide malicious instructions in files or websites that your company's AI assistant might read, tricking the AI into leaking sensitive data or performing unauthorised actions.
  - **Predator Bots:** traditional bot *scrapers* have evolved into self-learning bots that can probe a network's defenses, learn from failures, and adapt their strategy without human input.
  - Harvest Now, Decrypt Later → collect data sets, keep them, do something with them in the future.
-

## Case study 3: Ferrari

### The Incident



### The Incident

A senior executive at Ferrari received a series of WhatsApp messages and then a phone call from someone claiming to be CEO **Benedetto Vigna**. The voice sounded to exactly like Vigna, complete with his specific southern Italian accent and emotional cadence.

### The Risk Moment



### The Risk Moment

The fake CEO claimed he needed to discuss a confidential acquisition and requested a large, urgent currency transaction.

### The Save



### The Save:

The executive became suspicious when the "CEO" sounded too insistent. He asked a security question: "**What was the name of the book you recommended I read last week?**" The caller hung up immediately.

---

# Directive 2022/2555 NIS2

- Uphold cybersecurity → government and organisations.
- Each State to adopt a national cybersecurity strategy.
- Consider:
  - Supply chain (of technology and information).
  - Vulnerability management.
  - Cybersecurity education and awareness.
- 18 critical infrastructure and sectors.
- Requirements for certified professionals on-site.
- Notify authorities of incidents.
- National response teams.
- New proposals 2026 → expect amendments.

## What your organisation can do?

- Identity weakness points in the system.
- High-profile, tech-savvy European firms are being targeted with precision-engineered social engineering.
- Auto-delete information.
- Agreed certain things in person, off-grid.
- Identify where information flows inside → outside the organisation.
- Control systems in place.
- Dedicated AI + cybersecurity experts.
- Build expertise and awareness.



---

Hillmont  
Associates

People - Teams - Safety



ISEP

Institute of Sustainability &  
Environmental Professionals

# Climate and operational



**Table ES.5 Assessment of major risks**

Climate risks for 'Economy and finance' cluster	Urgency to act	Risk severity			Policy characteristics		
		Current	Mid-century	Late century (low/high warming scenario)	Policy horizon	Policy readiness	Risk ownership
European solidarity mechanisms	Urgent action needed	Critical	Critical	Critical	Short	Medium	Co-owned
Public finances	Urgent action needed	Substantial	Critical	Critical	Medium	Medium	Co-owned
Property and insurance markets	Urgent action needed	Substantial	Critical	Critical	Medium	Medium	Co-owned
Population/economy due to water scarcity (hotspot region: southern Europe)	Urgent action needed	Substantial	Critical	Critical	Medium	Medium	Co-owned
Population/economy due to water scarcity	Further investigation	Substantial	Substantial	Substantial	Medium	Medium	Co-owned
Pharmaceutical supply chains (*)	Further investigation	Substantial	Critical	Critical	Short	Medium	EU
Supply chains for raw materials and components (*)	Further investigation	Substantial	Critical	Critical	Short	Medium	EU
Financial markets	Further investigation	Substantial	Critical	Critical	Short	Medium	Co-owned
Winter tourism	Sustain current action	Critical	Critical	Critical	Medium	Advanced	National

<b>Legends and notes</b>		
<b>Urgency to act</b>	<b>Risk severity</b>	<b>Confidence</b>
Urgent action needed	Catastrophic	Low: +
More action needed	Critical	Medium: ++
Further investigation	Substantial	High: +++
Sustain current action	Limited	
Watching brief		

(\*) Wide range of evaluations by authors and risk reviewers.

Source: <https://nordsip.com/2024/04/02/europe-faces-e1-trillion-of-annual-climate-change-costs-by-2100/>

---

# Important for EU 2026

January → Bulgaria adopts the Euro.

June 2026

- **Carbon Border Adjustment Mechanism (CBAM)**
  - Levy on CO2 emissions of imported goods.
- **EU Deforestation Regulation (EUDR)**
  - \*New Deadlines: Compliance deadline for large and medium-sized companies is December 30, 2026.
  - Companies must prove products like cocoa, coffee, palm oil, rubber, timber, etc are not sourced from deforested land.
  - Small/Micro enterprises have until June 2027.

---

# Sustainability Reporting + transparency

- **Expansion of CSRD Reporting:** companies that were not previously subject to the **non-financial reporting Directive** but meet large company criteria has to collect 2025 data as a baseline year. And publish their first CSRD-compliant reports in 2026.
- In mid-2026, the EU Commission is expected to adopt the **revised European Sustainability Reporting Standards**. Including, simplified standards for SMEs and sector-specific requirements that have been under review to reduce administrative burdens.
- **ESG Ratings Supervision:** As of July 2, 2026, **ESG rating providers operating in the EU will be subject to direct supervision by ESMA (European Securities and Markets Authority)** to ensure transparency and prevent conflicts of interest.
- **Right to Repair Directive:** Member States must transpose this into national law by July 31, 2026. It grants consumers a new right to request repairs for products like washing machines, vacuum cleaners, and smartphones, even after the legal guarantee period has expired.

---



Hillmont  
Associates

People - Teams - Safety



---

## Circular economy + conservation

- **Empowering Consumers for the Green Transition:** This directive will apply from **late 2026**. It bans generic environmental claims (like "eco-friendly" or "green") unless they are backed by recognized excellence or specific legal requirements.
- **Circular Economy Act:** Expected in **Q3 2026**, this new legislative proposal will likely introduce horizontal standards for product durability, recyclability, and the use of "Digital Product Passports."
- **Ocean Act (expected Q4 2026):** Based on a revision of the current **Maritime Spatial Planning Directive**, this Act is meant to help meet the objectives of the non-legislative Ocean pact, such as restoring degraded coastal marine habitats and boosting a sustainable maritime economy.

# 2026 Global Climate & Environmental Risks Overview



## EXTREME WEATHER

- Increased frequency of heatwaves, floods, wildfires.
- Impact on infrastructure, agriculture, health.



## WATER SCARCITY

- Growing water stress in many regions.
- Conflicts over water resources.



## BIODIVERSITY LOSS

- Accelerated extinction rates.
- Disruption of ecosystems.



## POLLUTION

- Air and water pollution affecting health.
- Plastic waste accumulation.



## CLIMATE MIGRATION

- Displacement due to climate change.
- Social and political challenges.

Source: Various reports and projections

Hillmont  
Associates

People - Teams - Safety



ISEP  
Institute of Sustainability  
Environmental Professionals

---

# Finance and financial EU regulations

- Amendments to the **Sustainable Finance Disclosure Regulation** (expected Q3 2026): The EC proposed SFDR amendments (November 2025) to simplify disclosures and introduce new product labels (transition finance, ESG basic, sustainable products). The European Parliament and Council are expected to agree on the final text in 2026.
- **Revision of the Taxonomy Climate Delegated Act** (expected Q1 2026): Adopted by the Commission on 4 July 2025, the revision completed its six-month scrutiny period. It will now enter into force. Simplification measures apply retroactively from 1 January 2026 (for the 2025 financial year), but undertakings can opt to apply them from the 2026 financial year.

---



Hillmont  
Associates

People - Teams - Safety



---

# What can your organisation can do?

- Map your exposure to key raw materials and create China plus one strategies.
  - Integrate the Carbon Border Adjustment Mechanism (CBAM) levy into cost and pricing strategies for imported goods.
  - Implement a deforestation-free sourcing strategy with the correct papertrail in place.
  - Ensure data is collected and reports are CSRD ready.
  - Expand the adoption of lifecycle thinking and analysis to products and services.
  - Review and validate green claims.
  - Treat geopolitical and climate risks as recurring Board agenda items, integrating resilience measures into executive compensation.
-

---

Hillmont  
Associates

People - Teams - Safety



---

# Thank you.

Nico FEKETE PÉREZ  
MIEMA CEnv TechIOSH AIIRSM  
Sr. HSEQ consultant  
Hillmont Associates  
nico@hillmontassociates.com  
www.hillmontassociates.com

---

# GEOPOLITICAL RISKS 2026: A FRACTURED LANDSCAPE

Anticipating Key Global Threats and Trends



## GLOBAL POWER SHIFTS & CONFLICT

Escalated Proxy Wars, Naval Standoffs, Resource Competition (e.g., Arctic, Deep Sea)

**POTENTIAL IMPACT:** Disrupted Supply Chains, Energy Price Spikes, Regional Instability

**TREND:** Increasing Tensions & Incidents



## TECHNOLOGICAL DISRUPTION & CYBER THREATS

Weaponized AI, Critical Infrastructure Attacks, Digital Sovereignty Conflicts, Quantum Threat

**POTENTIAL IMPACT:** Financial Market Disruption, Data Theft, Public Trust Erosion, Infrastructure Failure

**TREND:** Rapid Evolution, Lower Barrier to Entry



## ECONOMIC FRAGMENTATION & TRADE WARS

Supply Chain Decoupling, Protectionist Policies, Currency Volatility, Debt Crisis

**POTENTIAL IMPACT:** Reduced Global Growth, Inflationary Pressures, Market Uncertainty, Economic Nationalism

**TREND:** Fragmenting Global Market



## CLIMATE CHANGE & RESOURCE SCARCITY

Extreme Weather Events, Water & Food Insecurity, Climate Migration, Resource Nationalism

**POTENTIAL IMPACT:** Humanitarian Crises, Political Unrest, Migration Flows, Infrastructure Damage

**POTENTIAL IMPACT:** Futures Crises

**TREND:** Accelerating Impacts, Compounding Vulnerabilities



## POLITICAL POLARIZATION & GOVERNANCE FAILURE

Erosion of Democratic Norms, Rise of Populism, Civil Unrest, Election Interference

**POTENTIAL IMPACT:** Policy Paralysis, Social Fragmentation, Weakened International Institutions, Internal Conflict

**TREND:** Deepening Divides, Weakening Trust



2024

2025

→ 2026

---

Hillmont  
Associates

People - Teams - Safety



---

# Thank you.

Nico FEKETE PÉREZ  
MIEMA CEnv TechIOSH AIIRSM  
Sr. HSEQ consultant  
Hillmont Associates  
nico@hillmontassociates.com  
www.hillmontassociates.com

---