EMERGENT RISK INTERNATIONAL

# Business in the Gray Zone

Strategic Intelligence Estimate 2026

# A Note from Executive Leadership

2025 was a norm-bending year unlike anything seen in decades. While events such as 9/11 or the Cold War reshaped geopolitical norms, none have resulted in such rapid changes in geopolitical relationships or trade in such a short period. The net effect has been mixed for business, markets, people, and entire countries. As we predicted in 2024, there were clear winners and losers in 2025, and this dynamic will continue this year. The upheaval of established rulebooks for international business and government left companies in reactive mode, unsure how to plan for supply and demand, pricing, taxation or major capital projects amid sharp political headwinds. Meanwhile, gray zone conflict eroded unity among Western powers and caused material damage to public and private interests in Europe and beyond. These same forces – primarily through information warfare – deepened social divisions, discouraged civic participation, and contributed to political violence.

## The operating environment and the gray zone

Taken together, these signals indicate that in the year ahead business must be more prepared than ever to operate and act decisively in an environment of extreme uncertainty and opacity. Leaders will be forced to make more decisions with incomplete information, less confidence in regulatory compliance, and greater ambiguity around supply and demand signals. Additionally, the risk of encountering bad actors, unattributed attacks, and threats driven by intentional and unintentional rogue AI will grow substantially. This is the environment that shapes our 2026 Strategic Intelligence Estimate. Gray zone conflict – war by other means – is now the de facto modus operandi for state and nonstate actors worldwide. As the technological tools of conflict become ever more affordable, more actors will use them for power projection, obscuring political and economic agendas, extracting economic advantage, and harming adversaries through nonattributable means.

## The gray zone information environment

In the following pages, you will find briefs that address some key challenges of gray zone conflict. These range from risks associated with well-known tactics, such as China's "creative" enforcement of its claims in the South China Sea, to a rapidly evolving regulatory landscape in which governments worldwide use punitive policies to advantage domestic industries and re-erect barriers to entry. Amid these power struggles, one of the most dangerous gray zone tactics has and will continue to be the weaponization of information to influence opinion.

In our 2020 annual estimate, we highlighted a then little-known AI tool, leaked to open source coding sites, called GPT2. Similar to a model under development by OpenAI at the time, the organization reportedly declined to release the full model initially because of concerns about its security implications. In that assessment, we argued that AI systems capable of generating fake news stories at scale, like GPT2, would pose serious risks to public trust in institutions, undermine business confidence, and distort electoral outcomes, hampering effective responses to major crises such as pandemics or natural disasters. Since that time, the world saw the 2022 release of Chat GPT accelerate global AI development at a pace more rapid than any previous technology – and along with it – a deepening loss of information integrity.

## 2025 developments and business implications

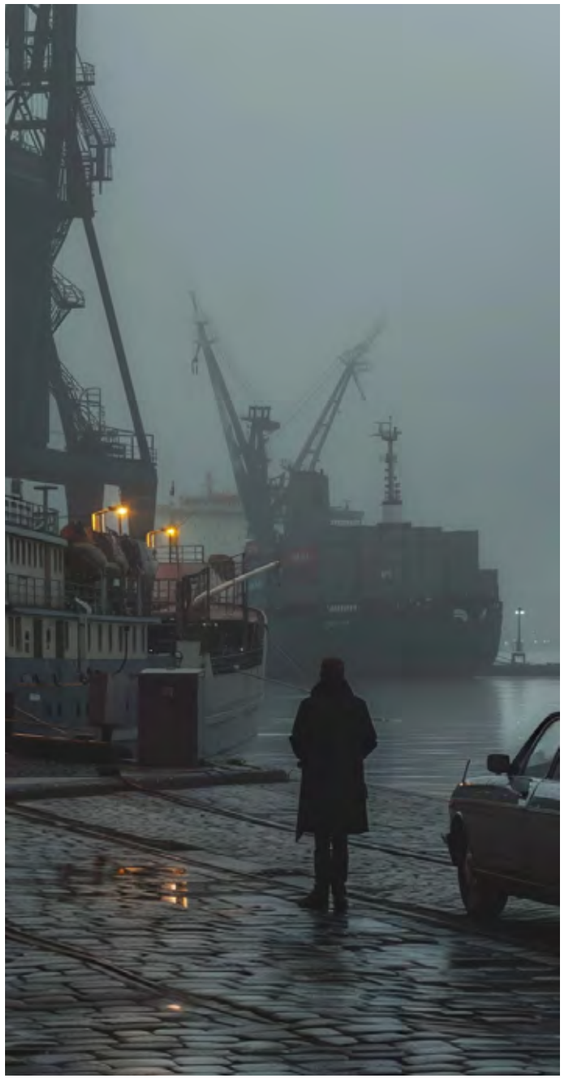
Fast forward to 2025, when the shutdown of USAID, broader US government reduction-in-force, and US Congressional decisions dismantled decades of systems and global funding designed to counter disinformation and censorship at home and abroad. While legitimate concerns with some programs existed, the depth of these changes had far-reaching effects, constraining domestic and international organizations that work to counter malign foreign influence and further shifting public opinion through emotive, inaccurate, and often false narratives.

During the response to Hurricane Helene in 2024, false narratives and disinformation spread at scale, cutting those impacted off from lifesaving assistance and endangering emergency first responders. In 2026, risks driven by the information environment will be greater, amid the combination of AI tools that can produce near indistinguishable fake written, audio, and visual content, rising hate speech, and the availability of low-cost, high-tech weaponry. Grievance-based violence targeting high-profile individuals, brands, and state institutions will be increasingly likely. Polluted information systems will also heighten electoral volatility and distrust in electoral outcomes — even in countries once seen as having robust voting systems and electoral integrity.

## Operating in the Gray Zone

For business, operating in the gray zone will require creative approaches to information management, decision-making, corporate diplomacy, marketing, and strategy to counter legal, reputational, and security threats. For Emergent Risk International, it means doubling down on our global human source network, retraining our workforce to operate in this environment — from sourcing and verification to writing and consulting — and committing to illuminating facts and analysis that support informed decision-making. Our focus remains providing consistent clarity to clients across all of our work. Whether through data, intelligence, and analysis in Emergent RiskIQ™, executive consulting, training, or bespoke investigations, we will continue to emphasize investigation and reporting from firsthand sources to counter online information pollution and manipulation.

As you read this assessment, we hope that you will utilize it as a practical guide to assess your company's vulnerabilities to gray zone conflict, understand how your industry and organization may become entangled in these dynamics, and identify where you are most exposed. We designed it to assist you in considering strategies and contingencies that address gray zone risks, while optimizing mitigation, crisis response, and longer-term business strategy. By integrating these insights into planning and decision-making, your organization will be better positioned to navigate uncertainty and seize opportunities in an increasingly contested global operating environment.



## Executive Leadership Team



**Meredith Wilson**
Chief Executive Officer

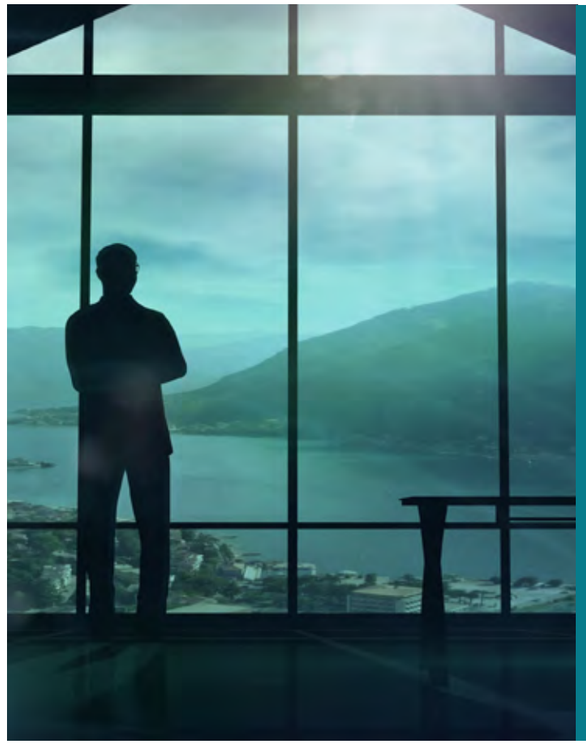
Meredith is the Chief Executive Officer & Founder of ERI. She has spent over two decades working in intelligence, first in government and then building some of the earliest private sector intelligence programs. She founded ERI in 2014 to build innovative intelligence programs that help companies leverage the best that intelligence can offer – but within the framework of business.



**Brady Roberts**
Chief Operating Officer

Brady is the Chief Operating Officer and is based in Austin, Texas. He joined the company in January 2018, where he oversees ERI's daily operations, trains clients and consults directly with customers, leveraging over 20 years of experience in the intelligence field.

# About Us



## Our Vision

At ERI, we believe that intelligence is a strategic asset — not a report on your desk. True business resilience begins with clarity: clarity that enables leaders to anticipate disruption, seize opportunities, and protect enterprise value.

We deliver intelligence that moves beyond data — providing context, foresight, and actionable insight tailored directly to your business and value chain. Partner with us to build #FutureForwardResilience and transform intelligence into decision advantage.

"FutureForward Intelligence.
RealWorld Resilience."

> **In uncertain times, clarity is the ultimate advantage**

## Our Mission

**We create and protect business value.**

Guided by this mission, ERI delivers industry leading business risk intelligence, technology, training, and talent solutions designed to strengthen your organization from the inside out. Our intelligence services are purpose-built for the pace and complexity of international business.

We ground our analysis in verifiable data and transparent sourcing — underpinned by rigorously vetted ground truth, intelligence, and analytics that together deliver a holistic understanding of your operating environment.

In a world flooded with information, we separate the signal from the noise and communicate what truly matters — empowering informed, confident, and agile decision-making.





## Focused Expertise

**We build capacity, not dependency.**

ERI builds sustainable capability, while others just deliver outputs. Our client-partner model helps organizations stand up their own self-sustaining intelligence functions, fully aligned with corporate strategy.

Our professionals bring decades of experience from the highest levels of business and government — combining operational insight with industry-recognized training to unlock lasting value and decision advantage.

## Intelligence & Forecasting

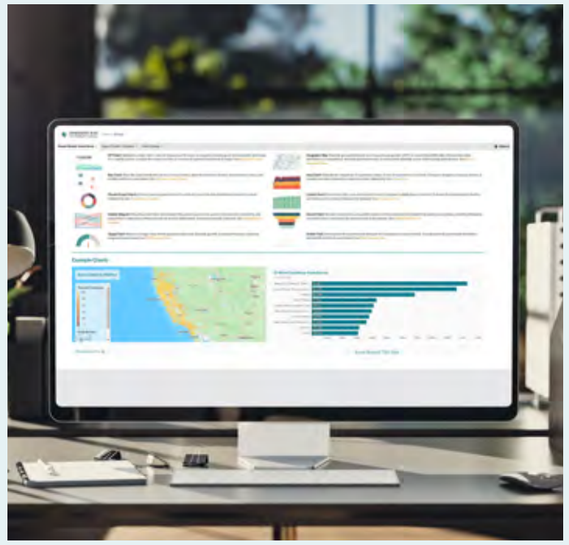
**Subscription and Bespoke Intelligence Products.**

ERI provides world-class subscription and bespoke intelligence solutions covering the full spectrum of business risk — with direct linkage to how these risks shape your value chain. Our globally distributed analysts and sources bring critical cultural and regional context, delivering insight that competitors miss.

## Technology: Emergent RiskIQ™

**Uncover insights. Analyze risks. Drive decisions.**

The Emergent RiskIQ™ platform fuses ERI's trusted intelligence with curated datasets, dynamic visualizations, and real-time partner integrations from Factal, ACLED, and other leading providers. In one intuitive interface, analysts can assess threats, model impacts, and communicate credible, decision-ready findings to executives with unprecedented speed and precision.



## Embedded Intelligence Services

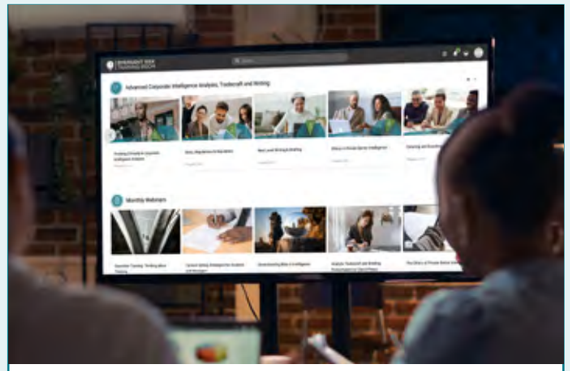
ERI's embedded staffing programs give clients a near immediate, full-service intelligence capability. We deploy trained analysts who deliver foresight, rapid crisis response, and strategic assessments from day one. Our integrated approach combines all ERI capabilities — analysis, technology, and training — to embed intelligence at the core of your business.

## Executive Advisory

**Where insight meets influence.**

ERI's Executive Advisory team bridges strategic intelligence with top-tier advisory. We combine access to unparalleled industry and government networks with deep analytic expertise to help leaders stay ahead of the curve.

From horizon scanning and geostrategic forecasting to tailored market-entry and in-house intelligence strategies, our consultants deliver clarity at the speed of leadership — enabling executives to anticipate risk, drive innovation, and make confident, future-ready decisions.



## Intelligence Training

Our training programs equip analysts with the skills, tradecraft, and judgment needed for enduring success in modern intelligence roles — from foundational tradecraft to advanced analytics.

Industry recognized courses include:

- Corporate Intelligence Analysis, Tradecraft, and Writing
- Advanced Intelligence Analysis
- Data Visualization and Analysis
- AI for Intelligence Analysts
- Analyst-to-Manager Transition
- Bespoke courses tailored to your unique business needs

EMERGENT RISK INTERNATIONAL

# What's Inside


| | | | |
|---|---|---|---|
| A Note from Executive Leadership | 2 | Technology Powering the Gray Zone | 16 |
| About Us | 4 | Crime as a Gray Zone Tool | 18 |
| Credits & Content | 7 | Resources, Supply Chains and Coercion | 20 |
| The Gray Zone in 2026 | 8 | Weaponizing Trade | 22 |
| Conflict in the Gray Zone | 10 | Weaponizing Finance | 24 |
| Political Violence, Intimidation & Manipulation | 12 | Weaponizing Regulation | 26 |
| Critical Elections in 2026 | 14 | The Regulatory Uncertainty Trap | 28 |






EMERGENT RISK INTERNATIONAL

# Credits


**Chief Editors**
Kieran O'Leary
Hannah Poppy
Meredith Wilson

**Marketing & Copy Editing**
Erol Yalciner
Misty Lynch

**Contributors - Emergent Risk International Global Intelligence Team**
Cameron Evers
Cameron Tisshaw
Devyansh Dullar
Judd Tennant
Neil Thompson
Madison Honsinger
Pearl D'Souza
Poornima Balasubramanian
Sachin Singh

**Design and Front Cover Image**
Studio Gilchrist

Strategic Intelligence Estimate 2026.

Published January 2026.

©2026 Emergent Risk International.

All Rights Reserved.

No part of this publication may be printed, reproduced or stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the author.

**Image Sources**

Page 3 – Image generated on Midjourney and edited by Studio Gilchrist

Page 4 – Adobe Stock, by conceptcafe
Adobe Stock by pressmaster
Adobe Stock by guteksk7
Adobe Stock by guteksk7

Page 6 – Unpsplash by samsonyyc

Page 9 – Image generated on Midjourney and edited by Studio Gilchrist. Infographic sources: ERI research

Page 11 – Infographic sources: ERI research

Page 13 - Infographic sources: ERI research. Image generated on Midjourney and edited by Studio Gilchrist

Page 14 - Infographic sources: Emergent RiskIQ™

Page 17- Infographic sources: Portulans Institute (high score = better) & International Energy Agency

Page 19 - Image generated on Midjourney and edited by Studio Gilchrist. Infographic sources: ERI Research & Emergent RiskIQ™ & [Image credit]

Page 21 – Infographic sources: Wikimedia Commons, UNFAO, SEAFDEC, Europarl. Image generated on Midjourney and edited by Studio Gilchrist

Page 23 – Infographic sources: Canadian Government, CSIS, Australian Institute of International Affairs, Institute for Energy Economics & Wilson Center [Image credit]

Page 25 – Infographic sources: IMF COFER, ERI Research. Image generated on Midjourney and edited by Studio Gilchrist

Page 27 – Infographic sources: ERI Research. Image generated on Midjourney and edited by Studio Gilchrist

Page 29 – Infographic sources: ERI Research & Emergent RiskIQ™

# Introducing The Gray Zone in 2026

**Democracies, autocracies and non-state actors will use gray zone tactics, with new technologies, regulation, finance and trade becoming new fields of gray zone competition.**

### Indicators of change:

- Counter-drone capabilities available and legal for use in regulated airspace
- Dual-purposing new commercial technologies for use in conflict
- Increased use of punitive trade measures between allied countries
- More prosecutions of journalists, media or NGOs in states with free speech laws

**Democratic governments are more openly operating in the gray zone against rivals and allies as hard power international politics return.**

The gray zone of conflict, war by means other than direct conflict, has traditionally been the domain of authoritarian governments or extremist groups seeking to exploit their opponents' belief in the rule of law for strategic advantage. This has changed as the world enters an era where using all the resources of national power matters.

In this changing reality, economic coercion, cyber warfare, and information operations become the norm, rather than the exception. State actors of all kinds will use these tools against rivals and competitors as well as against their traditional allies and partners, including during elections. The most critical votes in 2026 are set out on pages 14-15.

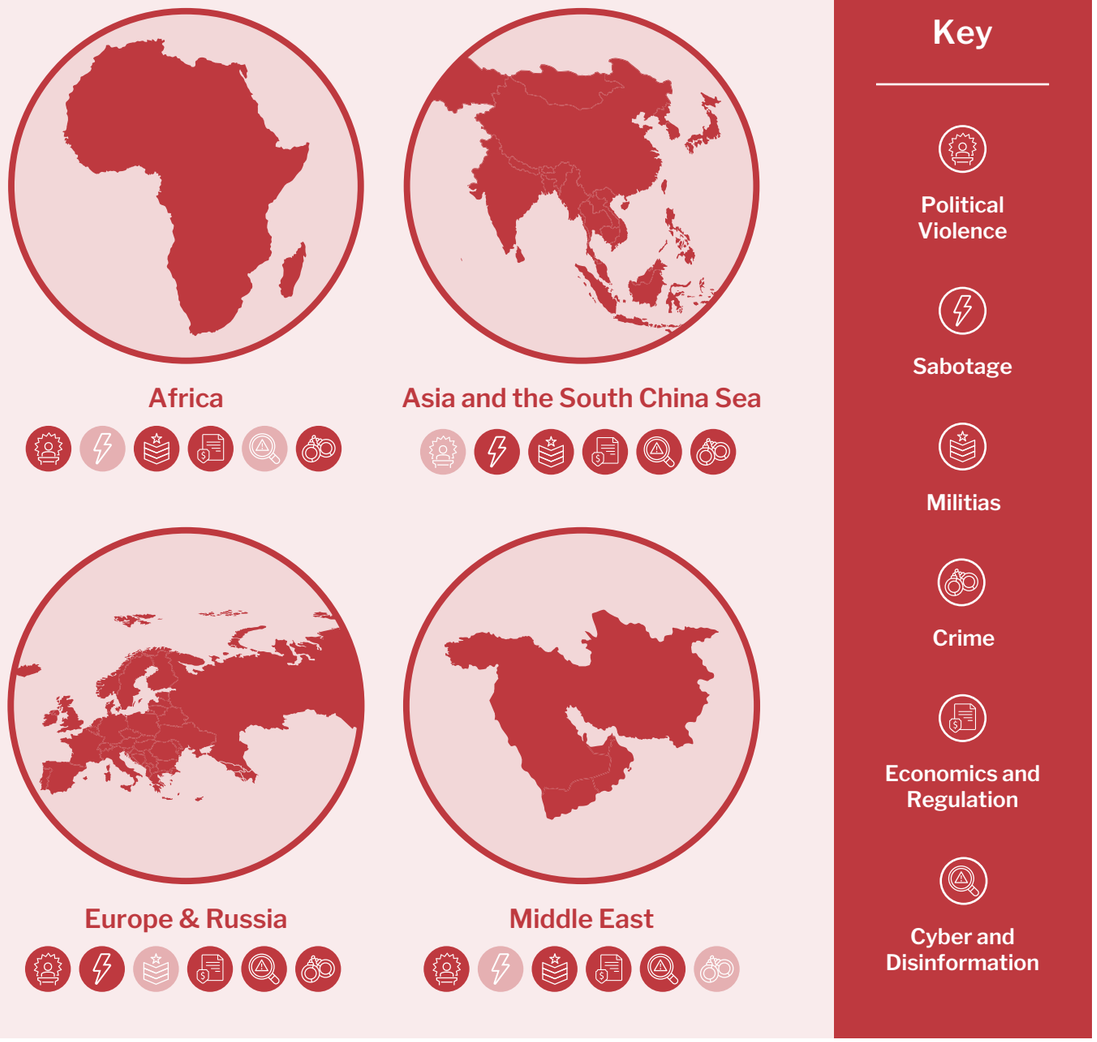
International business is now firmly wedged in between countries like China and Russia conducting sabotage or political influence campaigns and the US, Europe and others wielding tariffs and regulations in coercive ways. Trade, finance and regulation will be the new frontiers in gray zone conflict as powerful economies weaponize their strength to contain or damage their rivals. We explore these themes on pages 22-29.

**Hard power, including military force, will not diminish as a tool of coercion, but authoritarian governments will increase their use of deniable proxy actors, while new technologies bring new capabilities to non-state actors.**

Hard power and the use of force are not diminishing as a tool of power. Authoritarian governments will still threaten political violence against opponents or use their militaries to harass their opponents and test responses, as Russia is doing to NATO and China is doing to Taiwan. The nature of gray zone violence will change, however, as bad actors lean ever more on civilian proxies, including organized criminal groups, to conduct hard to attribute sabotage, foment political violence, or assassinate dissidents. These are themes we examine in pages 10-13 and 18-19.

Violence has never been the sole preserve of governments – rebels, extremists and organized crime have always used bombings and assassinations to further their causes. However, as we consider in pages 16-17, today low-cost drones, AI-enabled planning, 3D-printed weapons and other new technologies give non-state actors capabilities previously only available to governments.

Governments and corporations are also investing in stronger, more coordinated cyber defenses and defenses against new technologies, like counter-drone systems. Meanwhile, authoritarian governments are building defense against financial and regulatory gray zone pressure, such as establishing parallel financial and currency systems to evade sanctions and diminish Western control of global finance.




**The global fight for control of the information environment will see governments leverage the gray zone against media and online spaces, deepening distrust and uncertainty.**

Propaganda and information operations are among the oldest gray zone tactics. State-sponsored manipulation of elections and societies through social media has been a staple of Russia, China, Iran and others. But pressure on the reliability of the global information environment is rapidly growing as the US, some European states and other democracies and autocracies alike, undermine journalists and NGOs. Such organizations can safeguard against corruption through lawsuits, corporate acquisitions, and other legal means.

In the coming year, more political actors will be emboldened to contest control of the global information environment to advance their interests and harm their opponents, leaving organizations to assess risk versus reward in a more politicized, uncertain and unreliable world.



EMERGENT RISK INTERNATIONAL

# Conflict in The Gray Zone

**Rising political and economic costs of traditional warfare will drive a proliferation of gray zone tactics, and ultimately the risk of war, globally.**

### Indicators of change:

- Government GDP spend on defense rises by over a percentage point
- High non-wartime conflict casualty rates
- New border skirmishes, conflict in contested geographies
- Dehumanizing rhetoric about adversaries from political leaders

**As more states adopt less costly alternatives to overt war, gray zone tactics will spread geographically, exposing businesses to proliferating security risks, underscoring the need for constant assessment of the operating environment alongside business decisions.**

The soaring costs of war will deter potential aggressors from invading their adversaries in 2026. One estimate of the financial harm from Russia's war in Ukraine is $2.4 trillion, and another suggested this could be even higher because of pressure on growth from preparing the economy for war. The political cost is less quantifiable, but even in authoritarian states like Russia and China, political accountability and rising casualty figures can act as strong deterrents to warmaking.

Instead, governments are turning to gray zone tactics such as covert assassinations and sabotage of critical infrastructure to pressure their adversaries. Publicly available counts suggest there were between 36 and 114 wars in 2025. But those numbers do not include gray zone interstate wars: Russia and Europe, India and Pakistan, China and Taiwan. The spread of their conflicts, including to neighboring states, will make more places less safe, leading security teams to reconsider the risk of previously stable countries.

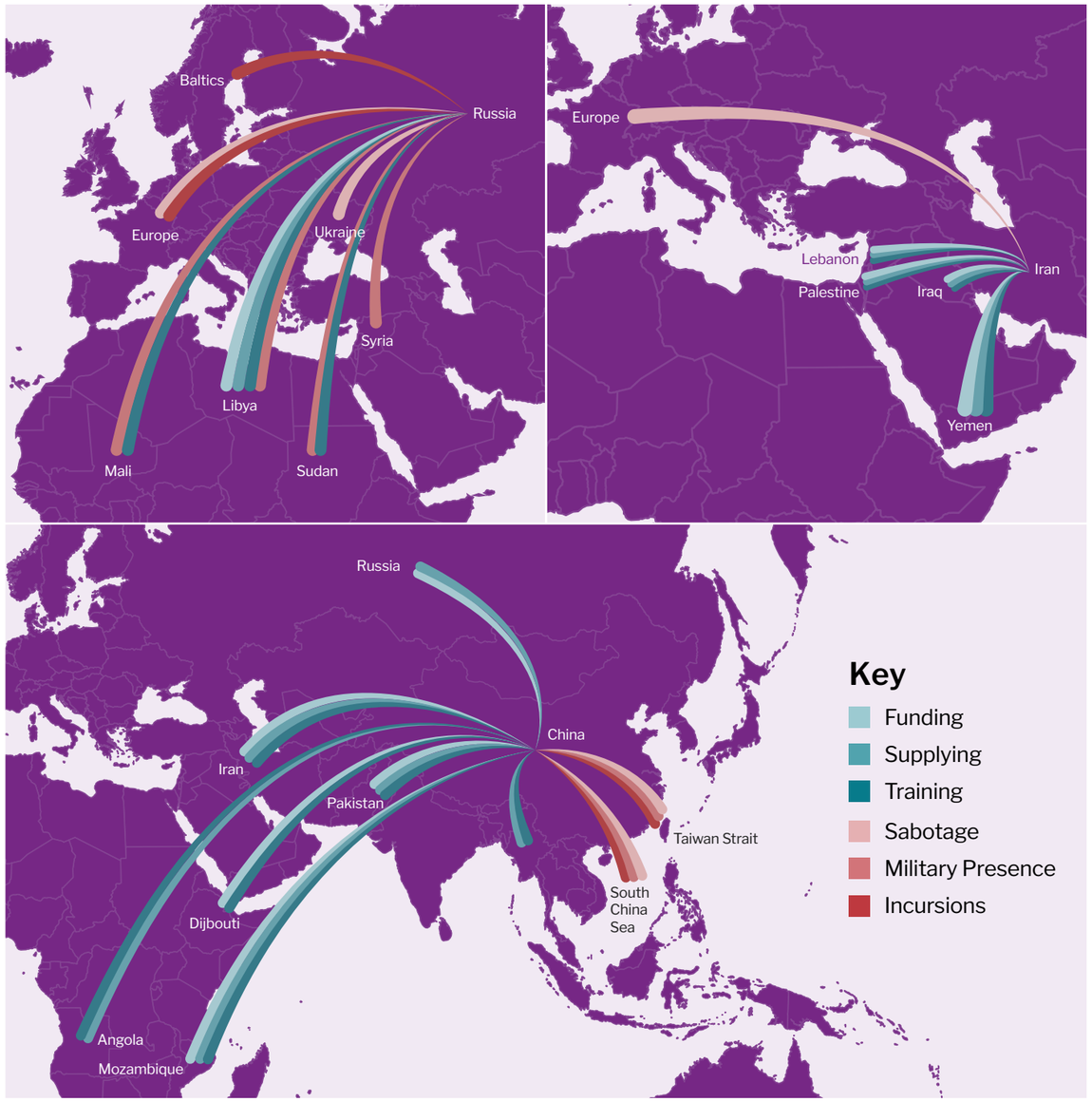
Africa and the Middle East will account for a significant proportion of wars in 2026. The DRC, Ethiopia and Israel-Iran are among the conflicts that will drag on business and supply chain continuity. Proxy wars, where such actors train, arm and fund militia, and state and non-state groups, will also continue across those regions as well as in Asia and Latin America. Worsening conflict risk in Europe from Russian gray zone activity is likely to drive a greater corporate willingness to consider business in areas previously considered too dangerous.

**Interstate wars will still occur, with all the commensurate impacts on staff safety and supply chain disruption, but the deployment of gray zone tactics will make them harder to predict and so it will fall on intelligence and security teams to assess and inform leadership of their true goals.**

Militarily powerful states like the US, India, China and Israel will not avoid open war altogether. They continue to eye the benefits of what a short or focused conflict can bring. Azerbaijan would arguably not have managed to convince Armenia to agree to a peace deal if it had not pushed for a limited conflict in 2023. Conflict can also weaken adversaries – temporarily – as Israel has shown in its confrontations with Hezbollah and Iran, among others.

Not all those states are spoiling for a fight. The US extraction of Nicolas Maduro of Venezuela provides a model for emulation of targeted, limited military action far short of full-scale war or occupation. India would much prefer to avoid a costly open confrontation with Pakistan. We doubt that China wants to invade Taiwan anytime soon, and the same goes for Thailand and Cambodia. However, to convince the other side that they are serious, countries will continue to pressure their rivals in the uncertain gray zone.

In other instances, militaries prefer to avoid alerting the adversary. This can involve maintaining a war footing for months before suddenly acting.




Or leaders might attend peace talks without intending to follow through with them. For teams whose businesses depend on them to forecast conflict disruption, like freight re-routing or insurance costs, there will be even more pressure to forecast accurately. They will be expected to back up against-the-grain assessments with data and human insight.

**When looking to determine which countries will remain at risk of conflict in 2026 – civil and international – tried and tested indicators like military spending will remain powerful.**

Despite their best efforts to disguise their immediate intentions, there will still be indications when states are moving closer to war. Those include existing disputes over territory and interests – particularly when they overlap, in the case of resources in disputed territories. Military strength, spending and hostile rhetoric, notably when it is sectarian or "othering", are others. An additional, and more subtle, area to watch is the extent to which political and military decision-makers are accountable, not to the public, but instead to economic elites whose interests are aligned with stability.

With that in mind, countries where there is a high risk of new or recurring conflicts to watch for in 2026 include: India and Pakistan over Kashmir, the DRC and Rwanda, Ethiopia and Eritrea, Israel with Hezbollah (Lebanon), Iran and the Houthis (Yemen). That is, of course, in addition to existing conflicts, like that between Russia and Ukraine, and a host of intense or lingering and localised civil conflicts, ranging from Sudan to Myanmar and Mali.

EMERGENT RISK INTERNATIONAL

# Political Violence, Intimidation & Manipulation

**Conflict, elections, shifting ideologies and damage to the global information environment will drive high levels of political violence in many countries in 2026, complicating organizational risk and response options.**

### Indicators of change:

- New political crises or contested elections in Western democracies
- New attack vectors driven by the misuse of new technologies
- Closer collaboration among previously distinct ideological actors
- Attacks or constraints on peaceful opposition to government actions

**International conflict and contentious elections will drive gray zone-style political violence globally in 2026, creating physical security threats for politically-involved companies and executives.**

Political violence is a key gray zone strategy. It is deployed directly through state power, such as the police or covert warfare, or through deniable non-state proxies. Much political violence is an outcome of conflict, and global conflict levels have doubled since 2020. 2026 is likely to see elevated levels of political violence across much of the world.

Elections will also drive gray zone political violence, with political actors seeking to influence outcomes through violence. In 2024, political violence rose 63%, on average, in countries where elections were held, compared with 21% in countries without elections.

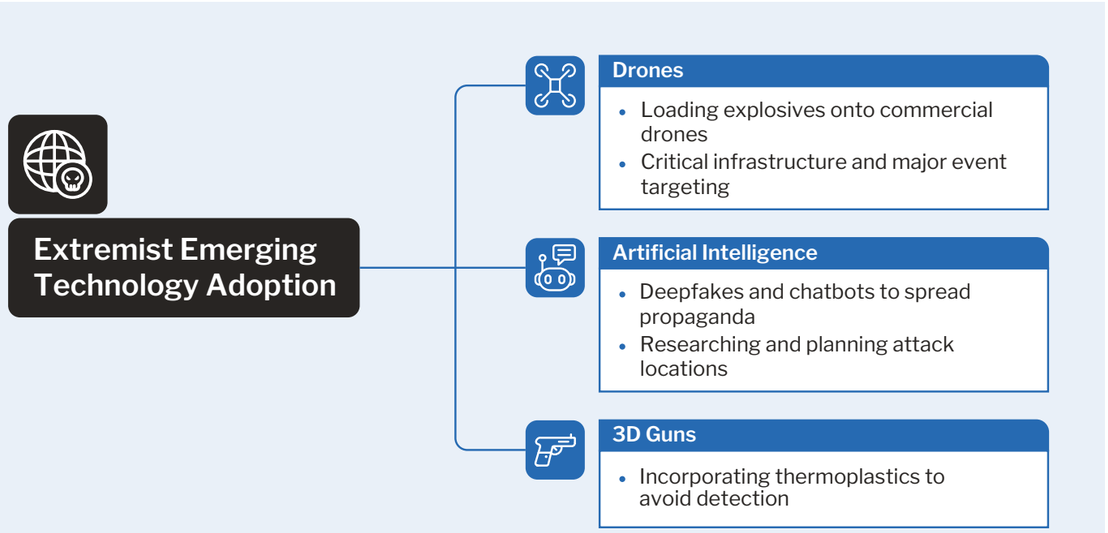
In 2026, multiple eastern European and Balkan elections will be at risk of Russian-driven political violence. Bangladesh's February election will see extensive political violence, as will Latin America, where gray zone political violence almost always rises during polls, such as in Colombia and Brazil. The US midterm elections will almost certainly see instances of political violence, primarily targeting election infrastructure, election workers and possibly candidates.

Businesses will face heightened threats to their employees and facilities, with governments, rebels and militant groups using violence outside conflict zones to advance their causes. State-linked and defense sector firms will be most at risk, though mass-casualty attacks will threaten any nearby business.

**The world's increasingly polarized media environment, disinformation campaigns, misuse of AI and threats to free speech and journalism expands the risks of political violence in 2026.**

The polarized global information space will be a gray zone battleground. Threat actors and nation states will harness traditional and social media, AI and disinformation to foment violence, stoke polarization and radicalize individuals. These efforts will be constant, intensifying during controversies, elections, and divisive moments to amplify protests and attacks and influence public opinion. These threat actors will also manipulate the information environment to drive violence against companies, transforming political risks into reputation and security crises.

> **Many of the most prominent recent incidents of political violence [...] were not motivated by a clear ideology nor emerged from a known violent group.**




Many governments – both autocratic and democratic – will block and suppress free speech. This includes encouraging violence against journalists, or attacking or arresting them directly. Such pressure on reporters and the broader media will damage the global information environment upon which businesses depend for data, situational awareness, and to communicate with the public. The US' 2025 fall in freedom press rankings underscores a global shift toward less media freedom, even in democracies.



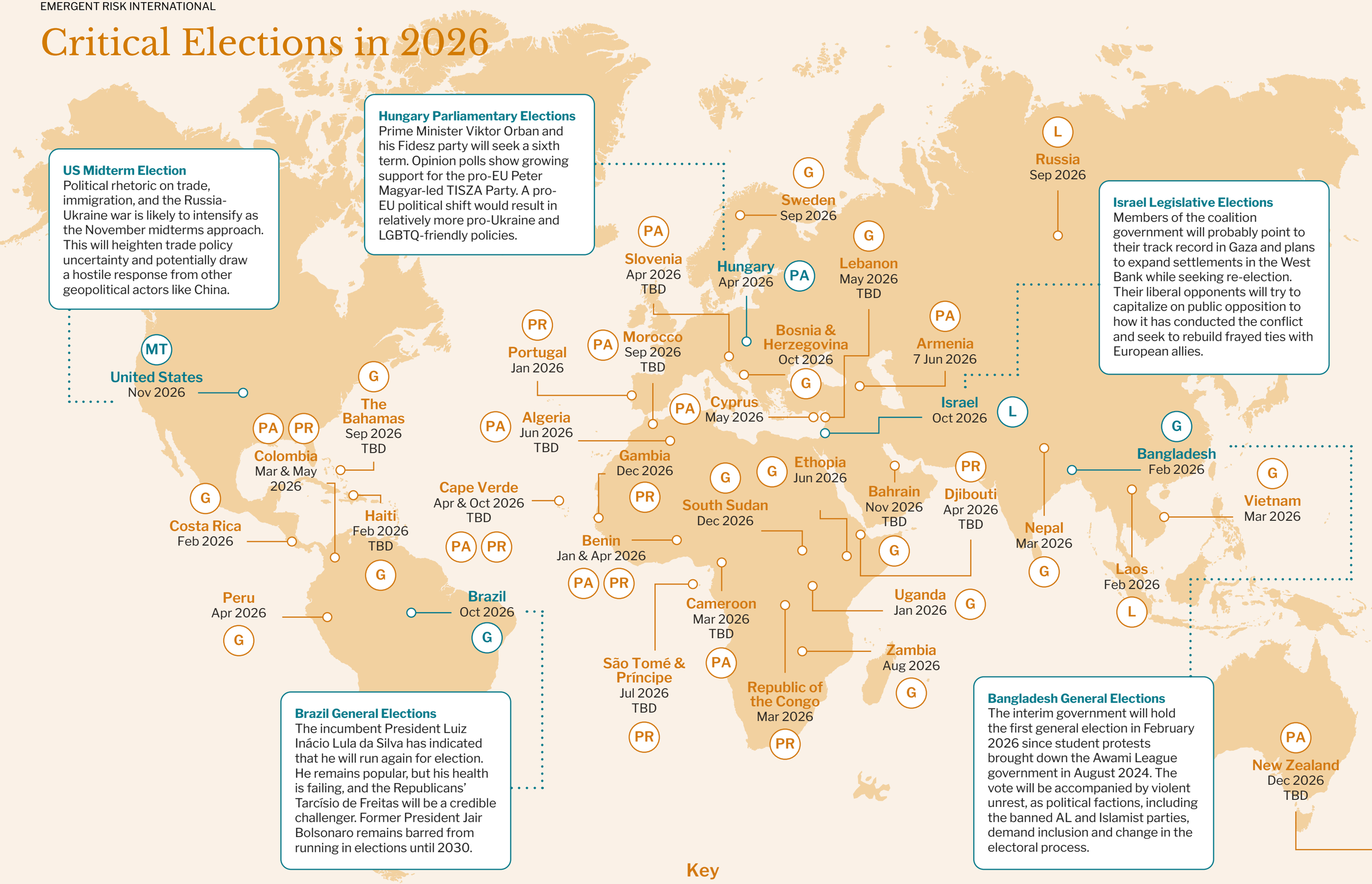
**Activist and extremist grievances will expand in 2026, driving political violence by non-state actors often targeting companies and occasionally prominent executives.**

Political causes are becoming more diffuse. With groups blurring ideologies and lone actors revealing few signs of their plans before an attack, law enforcement and corporate security teams face a challenge to detect threats ahead of time. Many of the most prominent recent incidents of political violence – multiple US assassinations and attempted assassinations, the killings of UnitedHealthcare CEO Brian Thompson and political commentator Charlie Kirk – were not motivated by a clear ideology nor emerged from a known violent group.

New alliances between groups, such as some environmental activists and pro-Palestine movements, compound their reach and disruptive capacity. While this partnership may abate while the Gaza ceasefire holds, other unusual activist partnerships are likely to emerge in 2026. Intensifying anti-migrant sentiment in many parts of the world will motivate political violence and draw its proponents into previously mainstream political spaces, further expanding the potential for violence.

At the same time, militants and extremists are adopting new technologies. They are using AI to recruit members and to research and plan attack targets. Non-state violent actors increasingly use 3D-printed "ghost guns." No longer the domain of just explosives experts, traditional cyber analysts, and weapons designers, understanding political violence trends now demands the understanding of technological trends and defense, such as counter-drone measures, counter-AI cyber approaches, and understanding new trends in 3D weapon creation.

# Critical Elections in 2026




**US Midterm Election**
Political rhetoric on trade, immigration, and the Russia-Ukraine war is likely to intensify as the November midterms approach. This will heighten trade policy uncertainty and potentially draw a hostile response from other geopolitical actors like China.

**Hungary Parliamentary Elections**
Prime Minister Viktor Orban and his Fidesz party will seek a sixth term. Opinion polls show growing support for the pro-EU Peter Magyar-led TISZA Party. A pro-EU political shift would result in relatively more pro-Ukraine and LGBTQ-friendly policies.

**Israel Legislative Elections**
Members of the coalition government will probably point to their track record in Gaza and plans to expand settlements in the West Bank while seeking re-election. Their liberal opponents will try to capitalize on public opposition to how it has conducted the conflict and seek to rebuild frayed ties with European allies.

**Brazil General Elections**
The incumbent President Luiz Inácio Lula da Silva has indicated that he will run again for election. He remains popular, but his health is failing, and the Republicans' Tarcísio de Freitas will be a credible challenger. Former President Jair Bolsonaro remains barred from running in elections until 2030.

**Bangladesh General Elections**
The interim government will hold the first general election in February 2026 since student protests brought down the Awami League government in August 2024. The vote will be accompanied by violent unrest, as political factions, including the banned AL and Islamist parties, demand inclusion and change in the electoral process.

## Key

G General | L Legislative | MT Mid-Term | PA Parliamentary | PR Presidential

EMERGENT RISK INTERNATIONAL

# Technology Powering the Gray Zone

**Threat actors will exploit dual-use technologies to expand the scope, scale, and impact of gray zone activities for espionage, sabotage, and influence operations.**

### Indicators of change:

- Novel AI-powered malicious information operations
- Attributable attacks on critical infrastructure outside of Europe
- Increased rates of remotely operated vehicle attacks or electromagnetic systems disruption
- Emergence of robust public-private partnerships to counter technological threats

**State and non-state actors will ingeniously repurpose existing technologies to advance cyber operations, information warfare, and critical infrastructure sabotage.**

Global business faces a complex technological threat landscape — spanning GPS interference, location tracking via digital wearables and 3D-printed weapons — raising the stakes for executive protection and workforce security. Repurposing of dual-use technologies for malign ends will be a defining threat trend in 2026. The scope of such repurposing is limited only by human creativity and could range from manipulating commercial satellites for surveillance to using networked vehicles or IoT devices for sabotage.

Malicious exploitation of social media and other platforms to conduct cognitive warfare, information campaigns and erode trust in institutions is set to expand rapidly. AI advances open avenues for its misuse, powering innovative and sophisticated cyberattacks on businesses and critical infrastructure, while lowering the entry barriers to non-state actors conducting disinformation, exploitation of large language models for malicious purposes, astroturfing campaigns and interference in democratic processes. Such campaigns will be aggressively directed at business ecosystems, clouding companies' ability to monitor their environment and driving reputation risks.

Unmanned systems will be co-opted for gray zone operations in civilian and military domains. Governments and non-state actors alike will use drones to threaten ports, energy facilities, and transport hubs. The development of dual-purpose software and technology that can be used for military or criminal purposes will raise concerns about proliferation and misuse within technology companies, driving staff resistance and insider threats. The race to develop defense systems against drones and swarming will also accelerate.

Space militarization is a growing gray zone arena with consequences for global business and industry. Anti-satellite weapons and co-orbital attacks, such as laser dazzling or proximity operations pose significant gray zone threats to the Western space infrastructure underpinning global communications and navigation. The expansion of commercial space services, including satellite imagery and communications, will introduce new risks for industries relying on these services, such as agribusiness, shipping, and others. This may include space-based position spoofing, denial of satellite communications or orbital access.

**Business-as-battlefield will become more mainstream next year, prompting tighter partnerships among like-minded nations and the private sector to counter emerging gray-zone technologies.**

Companies will be viewed as both targets and players in gray zone operations — they will be victims, vectors and enablers. In response, governments will likely intensify technology export controls, licensing, and sanctions, as well as national security screening of dual-use critical technologies and materials.

This gray technological competition will become more visible next year, with governments and the private sector enhancing intelligence sharing, resilience frameworks, and threat indicators.

Regulatory lag will challenge governments and businesses in 2026 as advancements outpace legislative processes. Governments' reliance on guidelines and standards in the absence of binding statutes and regulations will leave companies navigating a global patchwork of uncertain rules for data privacy, artificial intelligence, autonomous weapon systems and new technologies.

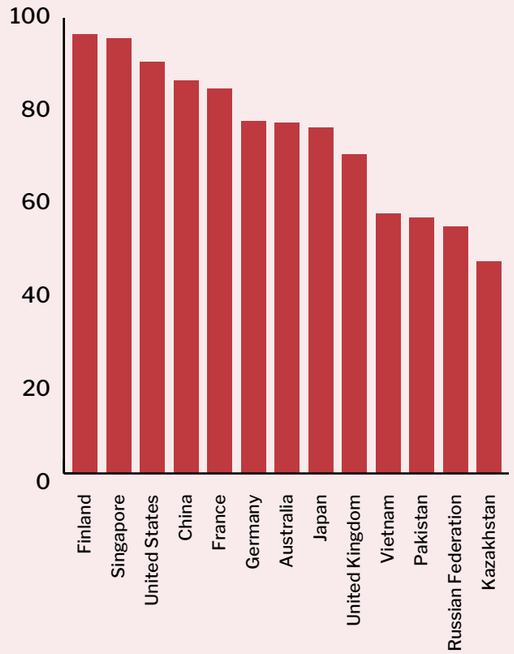
> **Companies will be viewed as both targets and players in gray zone operations — they will be victims, vectors and enablers.**

**Energy will be a significant business and competitive risk for digital infrastructure and technology companies, driving a stronger emphasis on alternative energy sources to satisfy demand.**

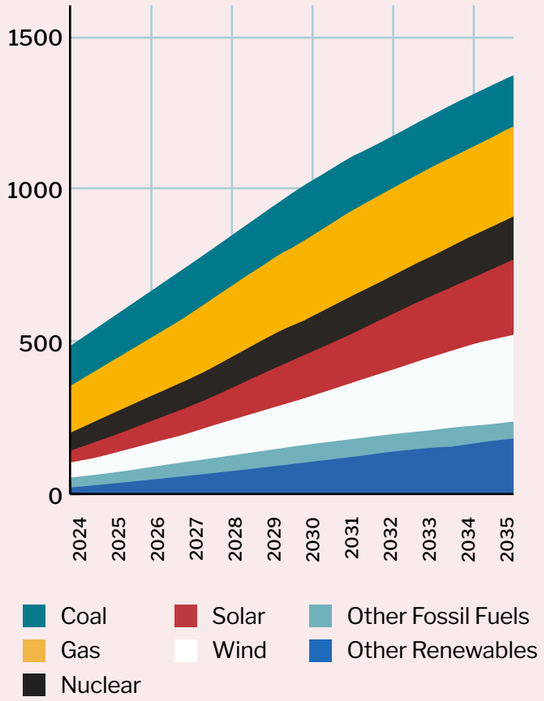
Energy will be a new gray zone battlefield at the intersection of digital systems, physical grids, and geopolitical competition. For businesses, energy cost volatility, supply reliability, and exposure to grid stress or infrastructure bottlenecks all drive operational, financial, and strategic resilience risks. Global electricity demand from data centers is projected to more than double by 2030, constraining digital expansion and exposing other businesses to energy shortages and cost volatility.

Energy will be both a target and a lever. Threat actors will use innovative tactics to shape the energy sector, including cyberattacks on energy infrastructure, manipulation of energy markets, disinformation about energy policies, weaponization of the renewable energy supply chain, and influence through energy financing. The global economy's growing energy vulnerability will spur companies, especially technology developers and digital infrastructure operators, to counter such gray zone threats with sustainable energy sources and efficient design.

Quality of Regulation of Emerging Technologies (2024)




Electricity Sources for Data Centers (2024-2035) Terrawatt Hour (TWh)



# Crime as a Gray Zone Tool

**Countries, particularly China, India, Russia, and Iran, will intensify their use of criminal organizations as proxies, primarily to target dissidents but also to conduct espionage and sabotage.**

### Indicators of change:

- Indictments of criminals and crime groups mention explicit state links
- NGOs report transnational repression of activists using anti-crime laws
- New anti-money laundering laws passed OR old laws repealed or loosened

**More governments will employ criminal groups as deniable proxies for gray zone operations, amplifying compliance risk for exposed sectors and elevating criminal threats to multinational businesses.**

Criminal groups are effective conduits for gray zone activity, excelling at smuggling, law enforcement evasion, and making profit in illicit markets. States provide them with resources, protection, a veneer of legitimacy, and financing to further expand. As governments increasingly rely on these actors to undermine adversaries, criminal networks will gain further power to broaden their operations and pose escalating risks to global business.

State-criminal partnerships will empower illicit networks and expand their penetration of legitimate sectors. Beijing collaborates with transnational organized crime groups to advance strategic objectives abroad. It shields Chinese criminal networks in exchange for their service as local enforcers and agents of influence. This arrangement enhances these criminal groups' operational capacity and complicates due diligence in China-linked supply chains.

This dynamic is especially acute in the pharmaceutical sector, although risks bleed into adjacent sectors such as logistics and finance.

The Chinese government subsidizes companies trafficking fentanyl precursors while obstructing US law enforcement. Other governments, including Russia and Turkey, leverage criminal groups to evade sanctions — particularly for semiconductors — and to supply arms to aligned rebel organizations.

**Russia, Iran and others will leverage criminal proxies to surveil, intimidate, and assassinate dissidents abroad and to sabotage critical infrastructure, heightening corporate security risks — especially for politically engaged firms and those integral to Western countries' national security.**

Businesses supporting Ukraine's war effort and European rearmament face the greatest direct exposure to violence from state-criminal collaboration. The Russian government recruits criminals and disaffected youth to conduct sabotage. Critical infrastructure and transport across Europe will remain the most common targets. Moscow has also plotted assassinations of European defense executives, and the risk of targeted attacks against that sector endures.

Other governments, including India and Iran, have also contracted criminal organizations to carry out politically motivated assassinations and attacks, emboldening their other illicit activities. Neither government is likely to deliberately target businesses; the high-profile suspension of a Canada-India free-trade agreement in 2023 following one such assassination attempt will discourage India and others from commissioning similar operations. Nonetheless, when these state-criminal gray zone tactics emerge from the shadows, they can trigger unexpected business and trade disruptions.



> **"State-criminal partnerships will empower illicit networks and expand their penetration of legitimate sectors."**

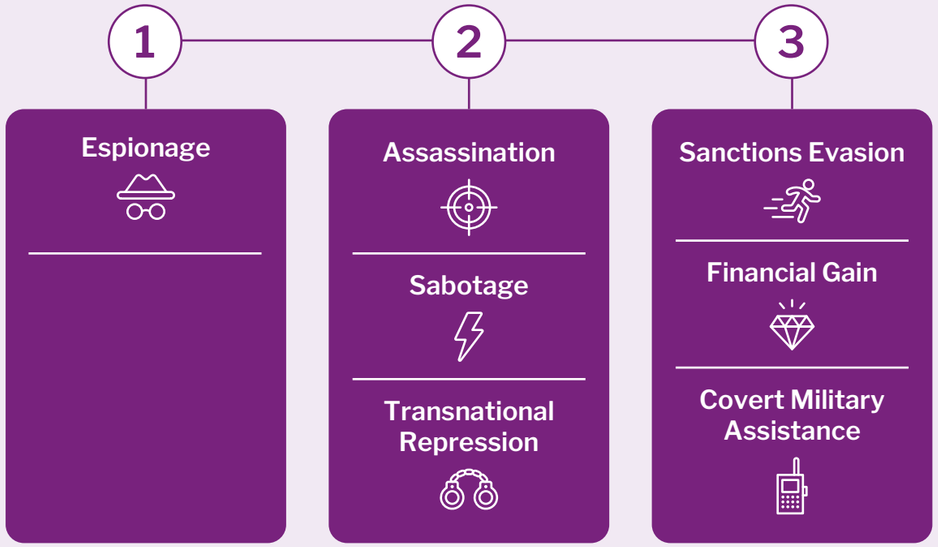
**Collaboration between intelligence services and organized crime will accelerate state-directed corporate intellectual property theft and heighten pressure on industries targeted by these networks.**

Criminal groups are inherently well-equipped for economic and corporate intelligence collection, with transnational logistics, covert communication channels, and technical capabilities that can be repurposed to steal data, infiltrate supply chains, or compromise companies. The organized crime-state espionage nexus will drive intensified law-enforcement action and regulatory scrutiny of the businesses and financial institutions that these networks exploit, increasing legal and compliance risks for multinational.

Taiwan has warned that Beijing is leveraging major triad groups to conduct espionage and influence operations, such as recruiting military personnel to obtain classified information. China will also task these groups with stealing intellectual property, particularly from Taiwan's world-leading semiconductor firms. Other governments seeking commercial and military advantages, such as Iran, North Korea and Russia will likewise deepen their reliance on organized crime for espionage.



## How States Can Leverage Criminal Groups



EMERGENT RISK INTERNATIONAL

# Resources, Supply Chains and Coercion

**Government and nonstate actors' competition over gray zone resources will make them leverage in international disputes, drawing multinational organizations into geopolitical competition.**

### Indicators of change:

- China's coastguard and fishing fleet numbers rapidly increase
- States other than China use commercial vessels for gray zone activities
- Morocco announces a referendum date for Western Sahara
- South China Sea hydrocarbon reserves projections revised upwards

**Geopolitical actors will compete for control of contested resources, creating uncertain operating environments for multinational businesses and complicating supply chain management.**

Culminating with the capture of Venezuelan President Nicolas Maduro on criminal charges, over the past year the US has used gray zone tactics to pressure Venezuela to yield access to its energy resources and infrastructure to US firms. Such firms now face a complex set of choices in balancing political pressure to exploit those resources against the commercial realities of difficult extraction and poor infrastructure, likely security threats and potential regional and global brand harm from perceived complicity in controversial US policies and gray zone strategies.

Meanwhile, non-US firms with interests in Venezuela confront an uncertain regulatory environment for their existing legal claims, alongside a risky and confused political landscape in the US, Venezuela and wider Latin America.

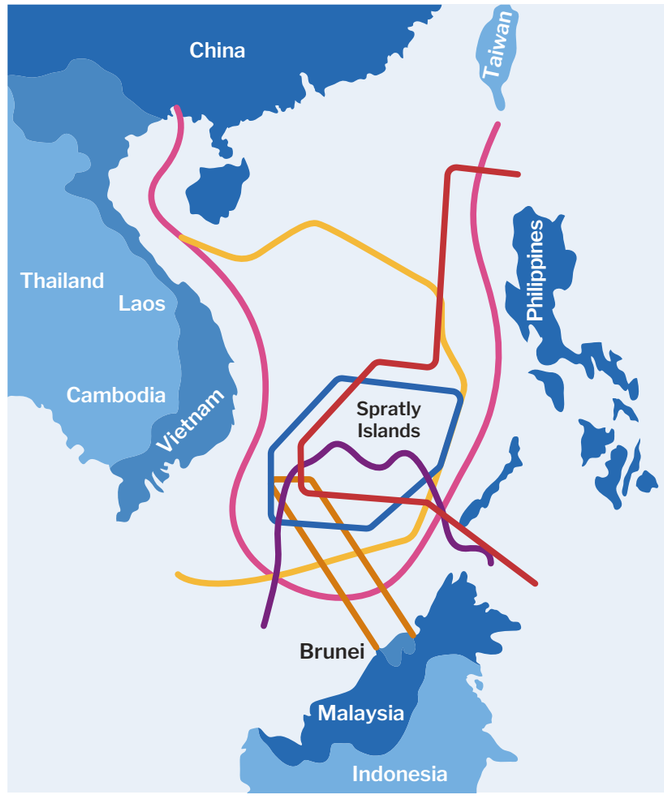
Resources originating in areas affected by gray zone conflicts and disputed territory like the South China Sea or Western Sahara include minerals, oil and gas, agricultural products, and seafood. The legal status of these resources is contested, yet it is difficult for businesses to prevent them from leaking into global supply chains when governments assert sovereign ownership.

In 2024, China issued rules allowing its coastguard to detain foreign nationals in its South China Sea claims. Subsequent arrests of foreign fishermen for allegedly operating in Chinese-claimed waters reinforce Chinese control of the region's $100 billion fishing sector.

China will conduct gray zone operations against companies exploring the South China Sea in other states' territories, including harassment, intimidation and legal action. China, Taiwan, Vietnam, the Philippines, Malaysia, and Brunei all claim parts of the South China Sea, which holds an estimated 40 trillion cubic feet of natural gas and 3.6 billion barrels of oil. Regional push back against China's actions raises tensions, drawing companies unwillingly into disputes.

**Non-state actors will adopt similar gray zone tactics to controlling resources, including legal threats to deter firms from investing in extractive industry projects.**

By their nature, gray zone conflicts in disputed territories include rebels, militias, political activists and disaffected communities, all of whom will lay claim to resources to support their causes. While some groups will leverage force to control exploitation of resources, others will adopt international political or legal approaches, deepening uncertainty and political risk for firms. West Saharan independence activists will challenge the EU's October 2025 draft effort to amend the bloc's free trade deal with Morocco in court in 2026, exposing firms that source agricultural products or phosphate from the region to negative publicity and potential future legal harm, despite Morocco's claims of sovereignty.




| Country | Fishing Fleet Size |
|---|---|
| China | 564,000 (as of 2020) |
| Vietnam | 110,000 inshore & offshore boats (2016) / 34,919,000 offshore vessels (2022) |
| Indonesia | 893,258 (2022) |
| Philippines | 407,215 municipal fishing vessels, 4,560 commercial vessels (total of 411,775) |
| Malaysia | 48,605 (2022) |
| Brunei | 6,466 (2022) |

**Countries engaged in geopolitical struggles will manipulate control of access to resources to gain strategic advantages, attempting to use firms as tools of geopolitical competition and pressuring companies to lobby their home governments.**

Governments engaged in strategic competition and territorial conflicts will threaten to disrupt firms' operations in gray zone regions, seeking to use pressure on firms to influence their home governments. Beijing has used this tactic against developed economies to counter US-led technology restrictions on Chinese firms and US tariffs, such as imposing strict export controls on rare earth minerals to disrupt Western supply chains. This tactic is questionably legal but hard to counter – a classic gray zone strategy - and exposes businesses in the electric vehicle, semiconductor, renewable energy and consumer electronics sectors to severe supply chain disruptions if US-China relations worsen.

> **"While some groups will leverage force to control exploitation of resources, others will adopt international political or legal approaches, deepening uncertainty and political risk for firms."**



EMERGENT RISK INTERNATIONAL

# Weaponizing Trade

**More governments will weaponize trade and control over strategic supply chain chokepoints as tools of geopolitical leverage, increasing challenges for multinational supply chains and procurement.**

### Indicators of change:

- New or expanded export controls on critical minerals, AI tech or bio-tech
- Increased national security framing of trade for extraterritorial enforcement and leverage maximization
- European states initialize digital sovereignty initiatives

## Expanding use of tariffs and critical technology export controls as coercive tools will spur governments worldwide to tighten control over strategic industries and reduce dependencies on external supply chains.

The US and China's use of tariffs and export controls will prompt governments to reconsider their dependence on both economies for critical supply chains and to increase their use of these tools to protect their own economic and national security interests. This shift is already particularly visible in Europe's support for "digital sovereignty" to reduce reliance on US technology; a trend likely to accelerate if Washington continues to use such dependencies as leverage.

In 2025, Washington used tariffs to pressure both partners and rivals during negotiations and will almost certainly continue doing so in the year ahead. The US also retains substantial leverage through export controls, including restricting access to aircraft engines and components, chip-making equipment, and products developed with US software. Washington's control over key global financial infrastructure provides an additional coercive instrument, enabling it to enforce extraterritorial sanctions against its rivals.

## China will expand and enforce its export controls as a form of geopolitical coercion when tensions with the US, Europe and other rivals arise, constraining access to critical minerals, magnets and potentially pharmaceuticals, among other chokepoints.

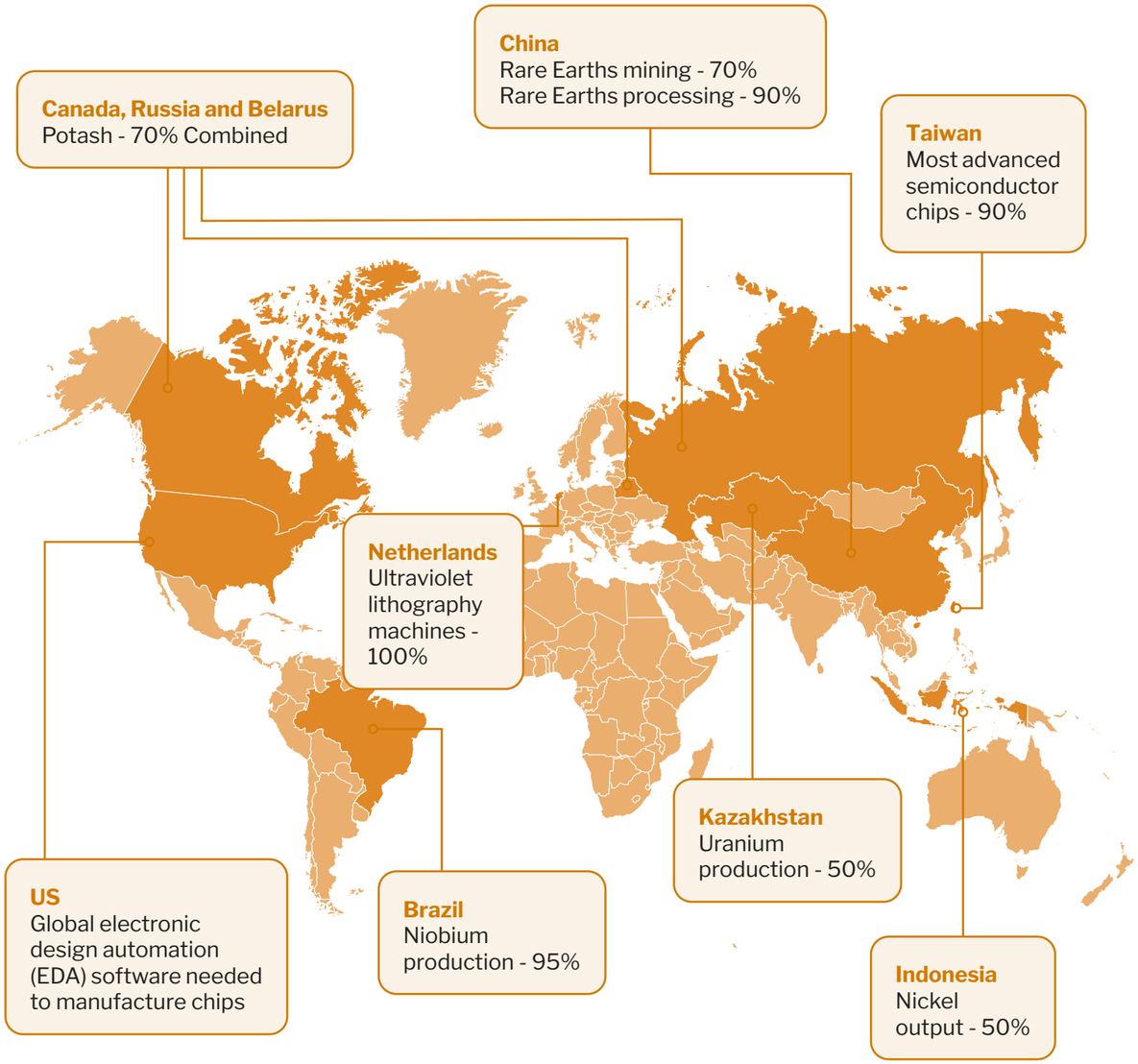
While export controls are a legitimate exercise of state power, their use as a tool of selective and coercive lawfare against adversaries makes them firmly a gray zone tool. China has built a sophisticated export control regime which it will keep in reserve, regardless of whether the global trade war eases. The Chinese government will use any lessening of trade tensions with the US to strengthen its enforcement capabilities to increase leverage in moments of geopolitical tension.

China is expanding its export control bureaucracy and is determined to institutionalize its export control regime as a long-term strategic tool. That suggests it neither expects the trade truce with the US to endure nor intends to fully adhere to it.

Beyond rare earths and critical minerals, Beijing has further coercive options. Global pharmaceutical manufacturing remains heavily dependent on Chinese-sourced active pharmaceutical ingredients, raising the risk that China could weaponize pharmaceutical supply chains against the US, EU, and other rivals. Such a move would be highly provocative, so the Chinese government would likely reserve it for only the most severe geopolitical tension.

## As the US and China weaponize supply chains and trade, other governments will seek to exploit control over their critical resources to maintain leverage, threatening to snare companies in geopolitical gray zone trade warfare.

The politicization of trade and supply chains suggests that economic interdependence is no longer a stabilizing force but an emerging arena of competition. Governments have observed the US and China's successful use of gray zone trade pressure to force others to change behavior or negotiate. They will examine their own economies to identify their critical points of leverage over others.




There are already a handful of illustrative cases. Taiwan threatened to restrict exports of its world-leading semiconductor technology to South Africa after Pretoria downgraded Taipei's diplomatic status. In Canada, federal and provincial leaders have weighed using the country's dominant position in US potash supplies and electricity exports to gain leverage over the US in trade disputes.

As this trend accelerates, multinational firms will be both a tool for governments to enforce these restrictions and the unwilling victims, suffering short-notice supply disruptions when geopolitical disputes arise. Firms will need to adapt to a world in which supply chain chokepoints are not merely logistics vulnerabilities, but instruments of state power and gray zone weapons.

> **Firms will need to adapt to a world in which supply chain chokepoints are not merely logistics vulnerabilities, but instruments of state power and gray zone weapons.**

EMERGENT RISK INTERNATIONAL

# Weaponizing Finance

**New sanctions, currency competition and predatory lending will shift the global financial system from being the bedrock of international commerce to a new front in gray zone competition.**

### Indicators of change:

- Western sanctions targets shifting from deterrence to behavioral coercion
- Compliance evolves from legal obligation to a political loyalty test
- Sanctioned states increasingly retaliate, leading to financial warfare

**Financial sanctions will remain a key tool for the US and Europe to pressure Russia, China, Iran and others, but their application and scope will likely become more creative and ruthless.**

The US and Europe will continue to dominate the world's financial transactions. Nearly 90% of all foreign exchange transactions involve the US dollar and about 30% involve the Euro, while nearly 85% of global trade transactions are conducted in one of those two currencies. Financial transactions involving these currencies go through US or European banks, giving those governments the ability to implement sanctions – a longstanding international response to war and poor behavior.

Despite that dominance and the widespread use of sanctions by the US and EU, these have not been particularly effective in recent years. Russia's economy has not collapsed, and it is still waging war in Ukraine; the North Korean regime still exists; the Iranian regime still has a nuclear program; and the Myanmar junta is still in power. These governments have found creative workarounds and ways to evade sanctions.

So the US, Europe and their allies and partners will try to be more creative in leveraging their control of the global financial system into pressure that changes behavior. That will involve scrutinizing the pressure points that keep these regimes afloat and targeting them, regardless of the human and economic costs, and demanding compliance from Western companies to enforce sanctions.

However, governments targeted with sanctions will not just evade them; they will also find ways to retaliate with their own financial weapons. That will likely involve penalizing multinational or domestic companies that enforce or comply with foreign sanctions.

**Control of global currencies will become a new battleground for countries to pressure each other and to pressure companies to trade where and with whom governments want.**

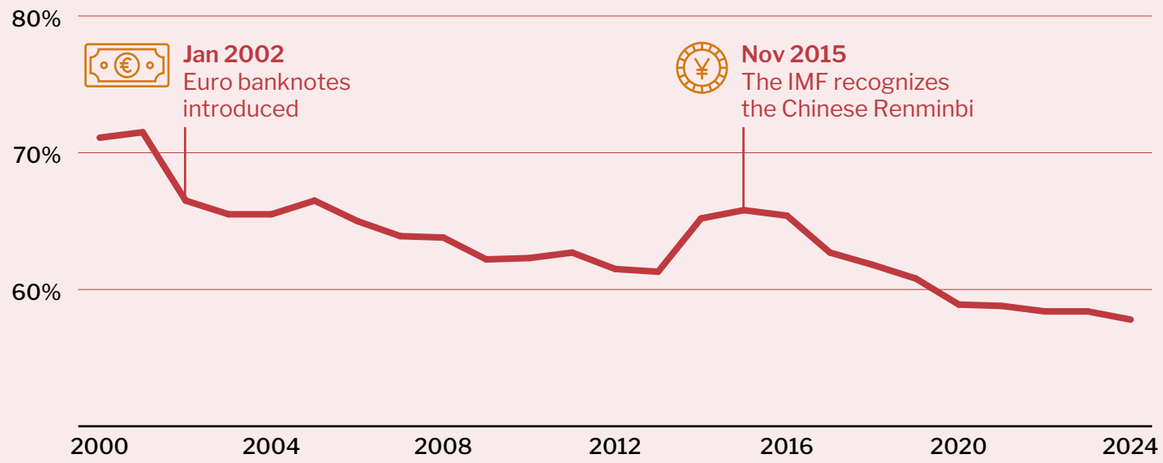
The dominance of the US dollar and Euro is a powerful tool for Western governments to control trade, apply pressure and support their own companies, so it is a key target for rivals and autocracies to weaken. Russia and China are already cooperating on increasing the use of their currencies in global trade, leaning on the expanded BRICS grouping to take up the cause, and this will be a high priority in 2026, albeit a subtle effort.

Neither the US nor Europe will stand idly by, with the US in particular pressing its partners to increase their use of the dollar, in some cases to dollarize their economies, and retaliating against countries that shift to other currencies. Companies trading

> **...governments targeted with sanctions will not just evade them; they will also find ways to retaliate with their own financial weapons.**



Percentage of Global FX Reserves held in US Dollars $



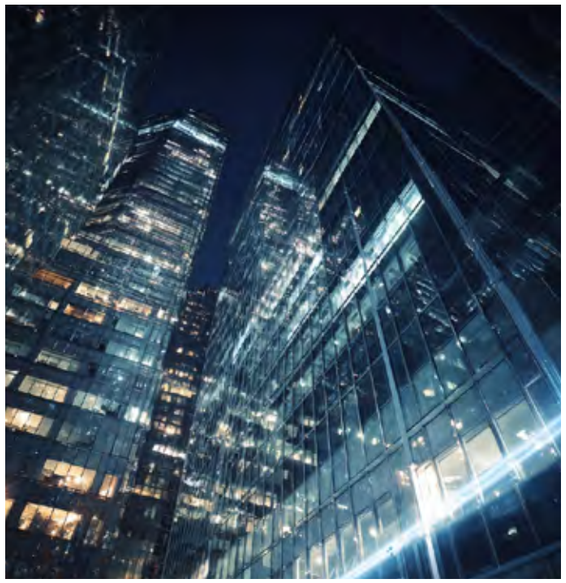

with China or others in their domestic currencies will increasingly find themselves under US pressure to only trade in dollars, or face consequences.

Cryptocurrencies, sovereign digital currencies and stablecoins will be another area of gray zone competition, as major economies – and some companies and non-state actors – strive to set the rules and norms for how these financial technologies will be used. The US will seek to have these currencies structurally tied to the US dollar, leveraging its financial and regulatory heft to get its way, while China, Russia and cryptocurrency advocates will seek to link them to alternative currencies or to remain independent.

**International financial assistance – lending, development aid – will be more explicitly transactional to build influence, control access to resources and exclude companies from rival countries from doing business in donor countries.**

China has long used its extensive fiscal reserves to lend to developing nations for infrastructure construction under its Belt and Road program. Beijing ramped up its B&R engagement in 2025 to establish itself as a counterpoint to the US trade war, claiming its assistance was free of political strings, a trend Beijing will intensify in 2026. But China's assistance is not without strings, and China will insist that its companies displace Western firms or demand exclusive access to resources in exchange for assistance.

Lending and development assistance is not inherently ill-intentioned, but it is China's use of the practice to exclude rivals, control resources and coerce recipients that takes it into the gray zone – and provides a model for other international actors to follow. The West is not immune to leveraging its financial strength in gray ways. Washington and others will shape financial bailouts, lending and development assistance to their own political ends – supporting governments with whom they are politically aligned, while denying assistance to even allies with whom they differ.



# Weaponizing Regulation

**To punish and weaken adversaries – and bolster domestic economies – states will weaponize regulations, couching their actions in the language of national security and bringing more multinational firms into the firing line.**

### Indicators of change:

- Regulatory scrutiny of M&A deals increases on national security grounds
- Introduction of new or expansion of existing foreign ownership laws
- EU introduces list of hostile foreign entities

**More states will use regulation to protect national security and limit foreign involvement, notably in technology, critical infrastructure and investment, altering organizations' international footprint and increasing their regulatory burden.**

Governments seeking to weaponize regulation against their adversaries are quickly repurposing old rules. National security and foreign ownership restrictions are particularly adaptable in this regard. The US banned TikTok, Chinese-owned social media app, citing national security threats and emergency powers. The US, China and other governments are also likely to issue politically-motivated travel and overflight warnings, making it harder for firms to objectively assess risk.

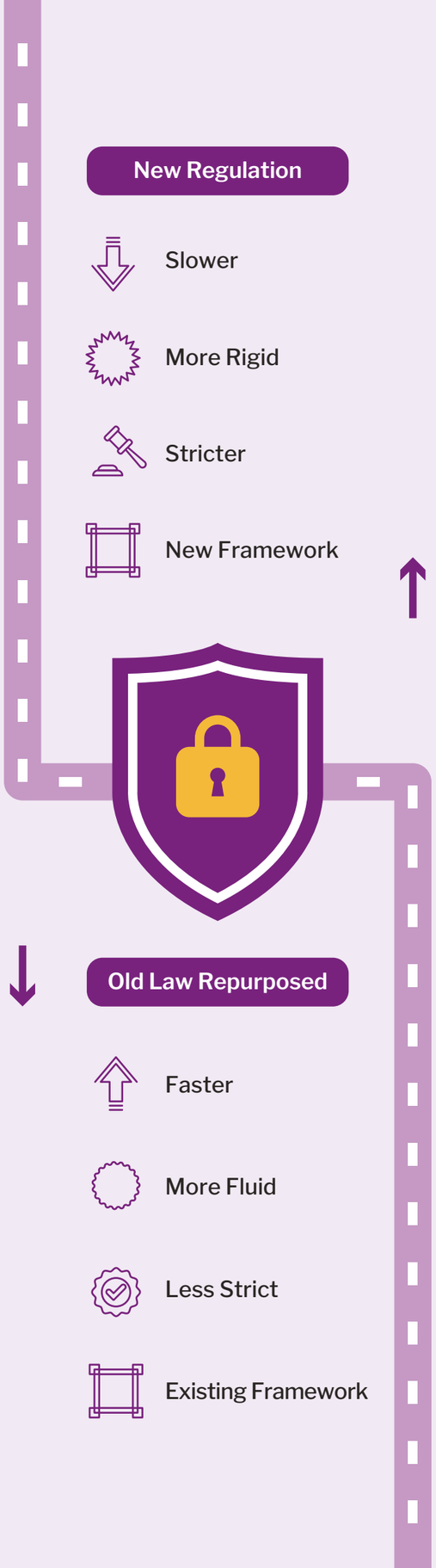
Authoritarian-leaning states where laws are vague and punitive, like China, Russia, Saudi Arabia and the UAE, are most likely to deploy this tactic. It turns domestic agencies into their gray zone enforcers; Sahel governments like Niger have sent tax inspectors to shake down mining firms. Agencies can increase inspections on facilities, enact stricter product safety measures or adapt an existing framework like China's negative list to exclude sectors or products.

The EU and India are becoming more willing to adopt this approach too, focusing on the likes of China, and such normalization opens the road for smaller economies, like Ethiopia, the DRC and Colombia, to follow suit. Sensitive sectors, such as technology, data, and critical infrastructure, will be the most common target of weaponized regulation; Taiwan enhanced its control over the semiconductor sector via 2022 amendments to the National Security Act. Still, the scope can expand to virtually any sector.

**Countries that are economically weaker – or shy away from overt confrontation – will adopt new rules that indirectly harm their adversaries, a more deniable gray zone approach, which is particularly challenging for firms to track.**

Countries will introduce new tax breaks or subsidies as well as other regulations that purport to boost domestic industries. However, these rules may instead be intended to create additional hurdles for foreign firms. In June, the Canadian government passed the Building Canada Act to fast-track approvals for national interest infrastructure projects. The Act does not explicitly identify the US but was passed in part to reduce reliance on it, amid worsening bilateral relations. States like India, Germany, and South Korea, under pressure to protect their industrial base, will be particularly motivated to do so.

> **"Trade rules and tariffs were a major gray zone weapon in 2025 [...] in 2026, this tactic will proliferate."**






Trade rules and tariffs were a major gray zone weapon in 2025, mainly for the US and China; in 2026, this tactic will proliferate. Leading exporters of a critical resource or good will also use regulation to limit foreign actors' involvement while protecting their economies. Sectors dominated by singular countries like Australia (lithium), Chile (copper), Indonesia (nickel), and Brazil (soybeans) will be subject to greater regulatory uncertainty. Those include energy and EVs, batteries, automobiles and agrifoods.

**Regulation by executive action – particularly by the US – will grow, meaning that compliance and supply chain teams that previously depended on legislative trackers will instead be called on to horizon scan for geopolitical trends and the moods of leaders.**

The US will continue to alter regulations by executive order, rather than congressional action. With the US issuing over 200 such orders in 2025 alone, there is little to suggest that the pace will slow. Examples in the last year have ranged from tariffs to energy subsidies and federal reporting rules. Many have met campaign promises or have been discussed in advance, providing a degree of predictability, but the pace of regulation and deregulation remains a challenge to US-exposed firms seeking to plan anything from trade to labor and finance.

Unlike normal legislative processes, executive orders are much faster and not subject to industry consultation or moderation, although rarely carry the full force of law. This makes them appealing to leaders under pressure to produce political results. Other major economies that will likely lean towards ruling by executive decree this year include Turkey, Argentina, Brazil and Mexico. Such orders enter the gray zone when they are harnessed as quasi-legal means of pressuring rival governments. For companies, their continued use also means uncertainty, since they can also be repealed or lifted at legal challenges.

# The Regulatory Uncertainty Trap

**Fragmented global and domestic rules on emerging technology, ESG, and other politically charged issues will create costly regulatory uncertainty for multinationals in 2026.**

### Indicators of change:

- EU, China, Canada, UK further tighten AI rules
- Domestic fragmentation mirrors global regulatory divides
- ESG evolves from disclosure to extraterritorial regulatory leverage

**Differences in the scope and standards of emerging technology regulations between major economies will make compliance more challenging and costly for multinational companies.**

Multiple regulatory blocs with differing approaches to regulating technological innovations will consolidate in 2026, illustrating how companies are forced to operate in the gray uncertainty of competing regulations. One bloc values comprehensive regulations for new technologies and greater legal certainty. Another bloc prefers to be more permissive when it comes to technology, favoring greater innovation – particularly in areas considered high-risk like data-heavy advanced technology.

The EU, China, Canada, UK and Japan fall in the first bloc. To prevent misuse of new technology, they will continue to place guardrails, sometimes even before technology and its applications are fully formed. China and the EU are already enforcing strict generative AI rules and, by 2026, hope to expand controls over autonomous systems, biotechnology applications, and quantum technologies. Bigger firms will likely find it easier to adhere to legislation in this bloc.

The US falls into the second bloc, favoring an innovation-focused approach, less constrained by regulation. As a result, US state laws – such as the Colorado AI Act and California's Frontier AI Act – have taken stricter regulatory measures as a counter. Multinational companies will have to navigate the regulatory uncertainty between blocs: complying with stringent legislation in some countries through geo-fencing, but taking advantage of regulatory space in the second bloc to develop innovative or riskier features.

**The EU and others will attempt to use Environmental, Social and Governance (ESG) rules to regulate beyond their borders, with counter-regulations complicating due diligence and supply chain management through 2026.**

Countries' contrasting approaches to ESG-related rules will muddy the regulatory environment for firms. Nations will prefer to trade with other countries that have a similar ESG standards and underlying values and some major economies will pressure their trading partners to adjust accordingly. The most notable example of this is the EU's phased rollout of its Corporate Sustainability Due Diligence Directive (CSDDD), the Corporate Sustainability Reporting Directive (CSRD) and the EU Deforestation Regulation (EUDR). All are aimed at upholding ESG standards throughout the EU's supply chains.

The EU will meet resistance from its trade partners, notably the US, Brazil, Indonesia and India. EU firms' inability to monitor labor rights or environmental safety compliance in countries with opaque supply chains will force them to shift sourcing to more transparent vendors and countries – even if at a higher cost – to pre-empt compliance risks.

In contrast, the US is actively rolling back ESG regulations, complicating compliance for firms that work in both the EU and US. Additionally, strict ESG rules for Western companies operating abroad will continue to leave them at a competitive disadvantage compared with Russian, Chinese and Indian firms that face lesser regulatory scrutiny from their home countries when operating in regions where human or labor rights records are poor.

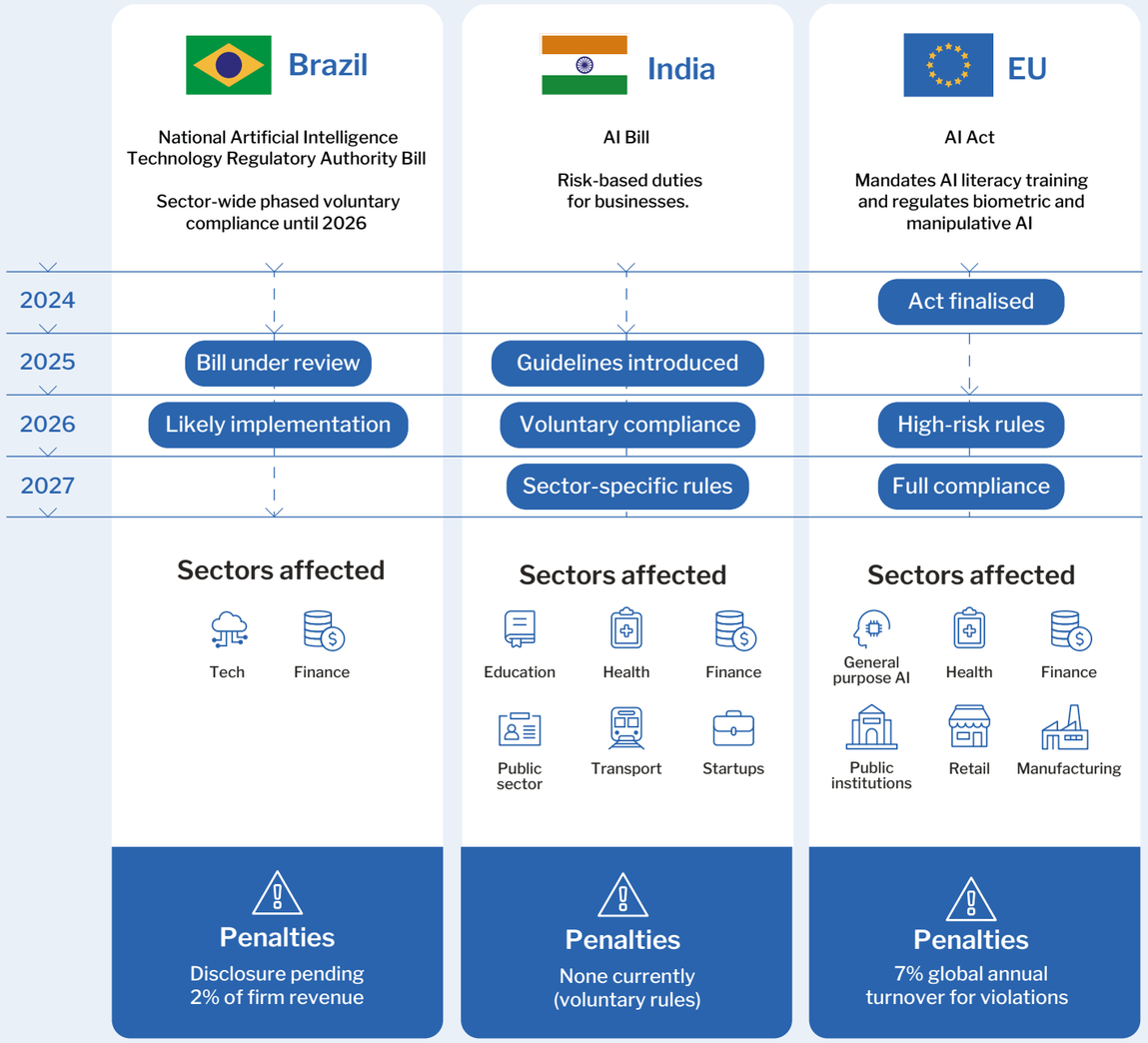


**Disputes between national and sub-national regulation of politically-charged issues such as immigration, climate change and diversity, equity and inclusion (DEI) will generate legal uncertainty and reputational harm for firms.**

In some countries with a federal system, companies will be caught between national and state, provincial or local regulations. This regulatory uncertainty will especially play out in ideologically polarized nations, where the federal ruling government is in political opposition to many state governments. India, Brazil, Canada and most notably the US, are where this is most likely to occur.

In the US, scrutiny over companies' DEI-related programs – or the absence of such programs – will be a major source of intra-national regulatory muddiness. US federal contractors and firms in Republican-governed states have faced moves to reduce or ban DEI requirements in 2025. Conversely, other states expect companies to demonstrate commitment to DEI values, forcing large companies operating nationally to balance competing pressures. Private sector handling of DEI is a litmus test for other cultural and legal battleground issues, pointing to challenges for firms on divisive issues such as immigration policy, gun rights, reproductive and other public health issues.

## Implementation Timeline





## Follow Us

/emergent-risk-international

/emergentriskinternational

@ERIriskfeed

@emergentrisk

@emergentrisk

## Contact Us

commercial@emergentriskinternational.com

emergentriskinternational.com

EMERGENT RISK INTERNATIONAL

© 2026 Emergent Risk International. All Rights Reserved.