

Breaking New Ground in the Assessment of Critical Risks

OECD Public Governance Directorate,
Infrastructure and Public Procurement Division
High Level Risk Forum Secretariat



High Level Risk Forum, 1 February 2024

ARTIFICIAL INTELLIGENCE – US UPDATE

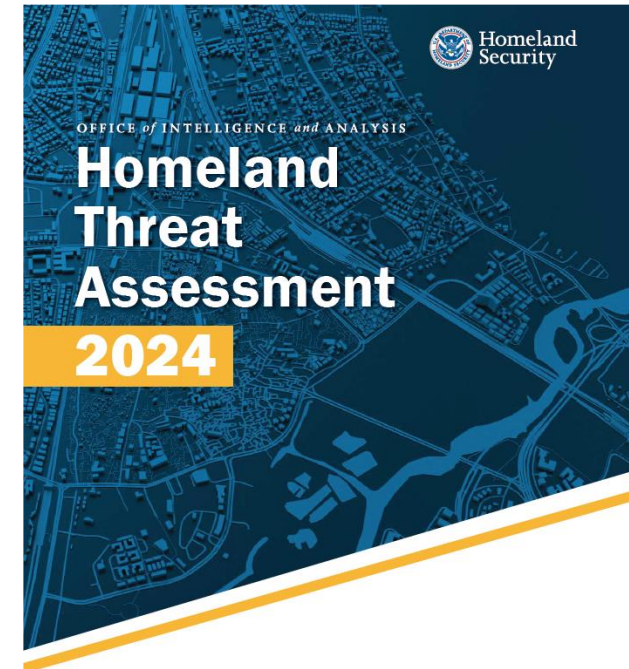
PRESENTATION FOR THE OECD - FEBRUARY 2024



2024 Homeland Security Threat Assessment

The 2024 Homeland Security Threat Assessment identified the following areas where AI is a significant risk factor:

- Countering Foreign Influence and Disinformation
- Chemical and Biological Weapons
- Cyber Attacks



Available at <https://www.dhs.gov/publication/homeland-threat-assessment>



A few recent developments



Executive Order 14110
October 2023



UK AI Safety Summit
November 2023



CISA AI Roadmap
November 2023

**Guidelines for secure AI
system development**



**Guidelines for
Secure AI System
Development**
November 2023



CISA's Lane

- Cyber defense
- Critical infrastructure protection
- Risk assessment and reduction



See all CISA materials on AI at www.cisa.gov/ai



President Biden issues Executive Order on AI

OCTOBER 30, 2023

Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence



▶ BRIEFING ROOM ▶ PRESIDENTIAL ACTIONS



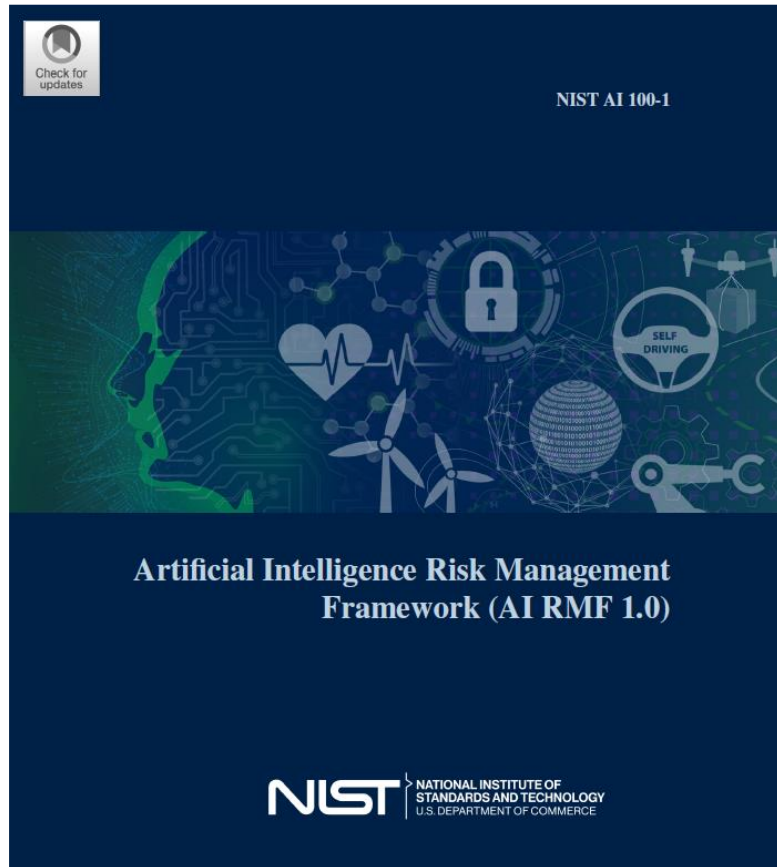
1-2 February, 2024

CISA's Role under Executive Order 14110

- **Protect critical infrastructure:**
 - Coordinate AI risk assessment for each critical infrastructure sector (Jan 2024)
 - Incorporate the National Institute of Standards and Technology's (NIST) AI Risk Management framework into critical infrastructure risk guidance (April 2024)
- **Cyber defense**
 - Launch operational AI-enabled vulnerability discovery and remediation pilot for federal civilian government systems (April 2024)
 - Share summary report of pilot results (July 2024)
- **Assure AI systems**
 - Coordinate with interagency on AI security red teaming guidance (March 2024)



AI Risk Management Framework



- CISA is incorporating the National Institute of Standards and Technology's (NIST) AI Risk Management framework into critical infrastructure risk guidance.
- Enhancing AI trustworthiness can reduce negative AI risk.
- CISA guidance underscores the characteristics of AI trustworthy systems (pictured below).



Fig. 4. Characteristics of trustworthy AI systems. Valid & Reliable is a necessary condition of trustworthiness and is shown as the base for other trustworthiness characteristics. Accountable & Transparent is shown as a vertical box because it relates to all other characteristics.



CISA Roadmap for AI

Purpose

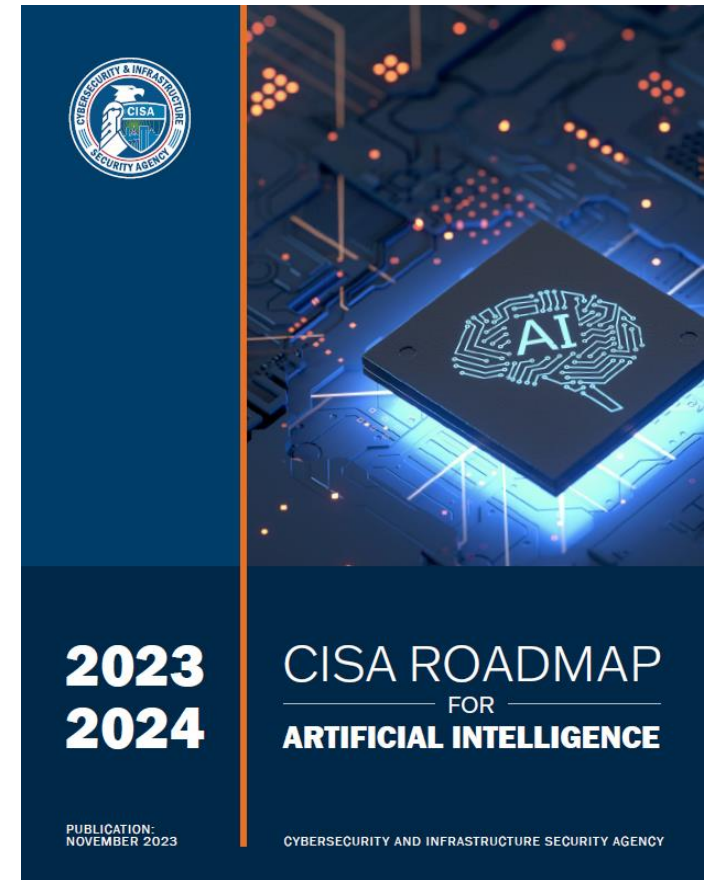
CISA's AI Roadmap is a whole-of-agency plan aligned with national AI strategy to align our cross-agency efforts and communicate our role in AI safety and security.

Areas of Focus

1. Promote the beneficial uses of AI to **enhance cybersecurity capabilities.**
2. Ensure **AI systems are protected from cyber-based threats.**
3. **Deter the malicious use of AI capabilities** to threaten the critical infrastructure Americans rely on every day.



<https://www.cisa.gov/resources-tools/resources/roadmap-ai>



Secure AI Guidelines

- Co-authored with international partners and co-sealed with 21 additional international agencies from 18 countries
- Developed in collaboration with industry
- Broken into four key areas:
 - Secure design
 - Secure development
 - Secure deployment
 - Secure operation and maintenance

Guidelines for secure AI system development



Where is AI being used at FEMA?


The Federal Emergency Management Agency (FEMA) has several existing AI use cases at various levels of complexity and maturity. Examples include:

- 1 Geospatial Damage Assessments:** FEMA's Response Geospatial Office leveraged a custom model built using deep learning capabilities to quickly assess damage severity following Hurricane Ian.
- 2 Office of the Chief Financial Officer GPT:** FEMA's Office of the Chief Financial Officer is building a Generative AI model to automate the generation of draft responses to budget questions, seeking to improve quality, decrease time to respond, and free up staff resources.
- 3 Planning Assistance for Resilience Communities (PARC):** FEMA Resilience is leading a DHS-sponsored Generative AI pilot to create efficiencies for the hazard mitigation planning process (e.g., documenting and plan writing) for local governments and focus on increasing the quality and impact of their planning.
- 4 Individual and Public Assistance:** FEMA's Recovery Directorate uses linear regression and ARIMA time series techniques to predict demand for Individual Assistance Program Registration Intake & Inspections and Public Assistance Program Workload.
- 5 Workforce Deployment:** FEMA's Field Operations Directorate built a custom model to predict staffing demand for an incident, and the degree to which available responders can meet demand.
- 6 Security Tools:** AI is in several FEMA security products. For example, Zero Trust exchange platform for FEMA Cloud based Network Access Security.



FEMA's U.S. Fire Administration

- The National Emergency Response Information System (NERIS) will serve as the platform for safely integrating the best available, vetted, and validated machine learning (ML) and deep learning (DL) models for predictive local fire analytics and post-fire impact assessments that both U.S. Fire Administration and the American fire service will rely on to inform mission critical decisions both pre- and post-incident.




Empowering Effective Emergency Response

The U.S. Fire Administration (USFA) has partnered with U.S. Department of Homeland Security's (DHS) Science and Technology Directorate (S&T), and the Fire Safety Research Institute (FSRI) to develop and launch a new interoperable fire information and analytics platform, known as the National Emergency Response Information System (NERIS).

The goal of NERIS is to empower the local fire and emergency services community by equipping them with near real-time information and analytic tools that support data informed decision-making for enhanced preparedness and response to incidents involving all hazards.

NERIS will be tailored to meet the evolving needs of today's fire and emergency responders. It will provide reliable analytics to help understand the complex fire and public safety challenges we face today, such as:

- ★ Changing Climate
- ★ Aging Infrastructure
- ★ Future Pandemic Response
- ★ Wildland Urban Interface Fires
- ★ Electrification and Stored Energy Hazards
- ★ Emergency Medical Incident Scope Growth



The Future of Incident Reporting

Enhance Data Quality and Effectiveness with NERIS

Features	Benefits
 User-Friendly Design Responsive data input and retrieval on mobile phones, tablets, and desktops	Reduced barriers to accurate and timely data for local fire departments
 Revamped Data Framework Data structures and processes modernized, tested, and enhanced	Streamlined incident reporting, enabling responders to document in less time
 Easy Integration Seamless connectivity with trusted third-party systems like CAD and RMS	Simplified data management using your preferred vendors
 Free of Charge Interface access for verified essential services, even if they don't use an RMS	First responders can connect without facing financial barriers
 Advanced Analytics Turnkey tools and enhanced analysis and dashboard capabilities	More efficient trendspotting and mission critical information for your teams
 Robust Security Cloud-based data protection is a top priority	Safeguarded data and reliable access to incident information
 Near Real-time Data Offering dynamic and timely incident updates	Increased visibility in decision-making, minimizing mission-critical blind spots

"Once launched, the new NERIS platform will provide capabilities for documenting and introducing community risk reduction efforts, associated resilience and mitigation efforts into the overall preparedness and resilience equation — providing greater insights into vulnerability gaps where resources can be used to harden communities and minimize future emergency and disaster events."

- U.S. Fire Administrator Dr. Lori Moore-Merrell

CONNECT WITH US

- ★ Visit the NERIS site
- ★ NERIS@u.l.org



COMING SOON - STAY INFORMED

- ★ NERIS Data Framework Release: December 2023
- ★ NERIS Platform v1 Release: Fall 2024

The USFA is dedicated to the continuous improvement of the system, incorporating feedback from our users.

© 2023 Underwriters Laboratories Inc. All rights reserved.





Dr. Mikael Wigell

Research Director, The Finnish Institute of International Affairs

Geopolitical Advisor, Hill + Knowlton Strategies

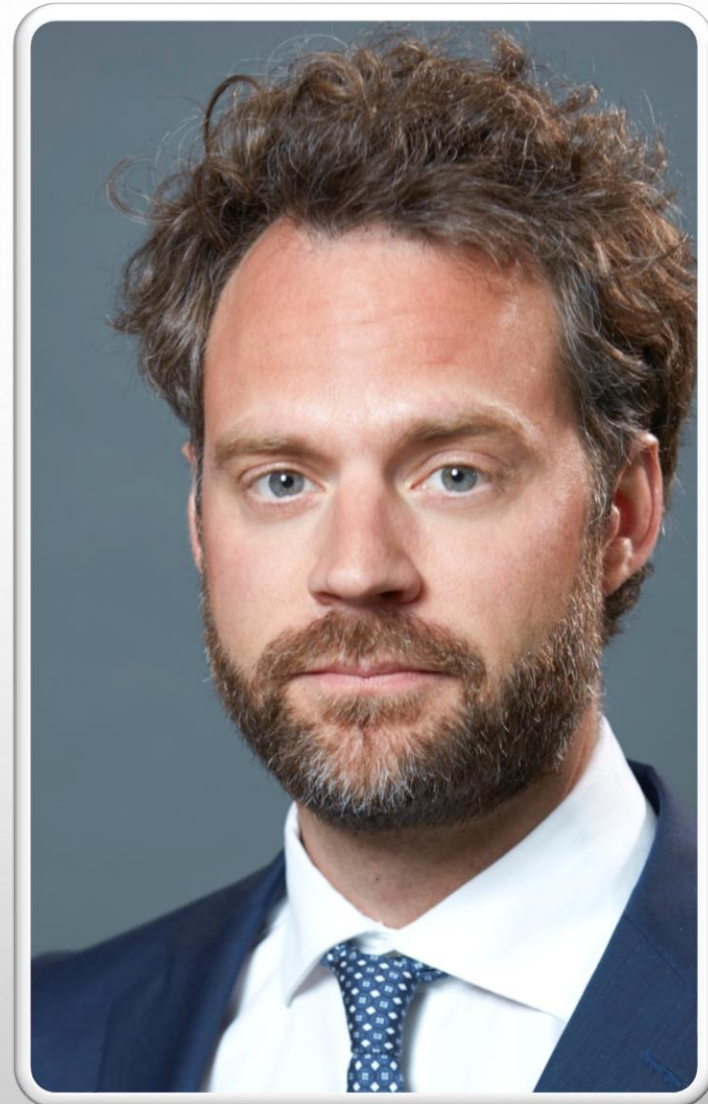
Expert Member, World Economic Forum

Senior Advisor, Geostrategic Intelligence Group

Visiting Professor, Oxford University

*Editor, Geo-economics and Power Politics in the 21st Century
(Routledge 2018; 2020)*

PhD, London School of Economics



The logo for the Finnish Institute of International Affairs (FIIA) is located in the top left corner. It consists of the letters 'FIIA' in a bold, dark red, sans-serif font. The background of the slide features a light gray gradient with several realistic water droplets of various sizes scattered across it, some in the top left and others in the bottom right.

FINNISH INSTITUTE
OF INTERNATIONAL AFFAIRS

The Emergence of Geoeconomic Risk

The Logic of Global Economic Relations Is Changing



- From interdependence to autonomy
- From efficiency to resilience
- *De-risking*
- *Economic security as national security*

How to Make Sense of It?

- Market economics a poor guide to the transformation underway
- Need for a new analytical framework → *Geoeconomics*



The Rise of Geoeconomics

- The use of economics to advance political goals
- Economics and security thinking becoming intertwined
- The norms and rules governing the international economy uprooted



Using a Geoeconomic Framework to Understand...

- How international politics is changing
- How international economics is changing
- How international business is changing



How International Politics Is Changing: *Geoeconomic Statecraft*

- Coercion
- Binding
- Wedging
- Hedging



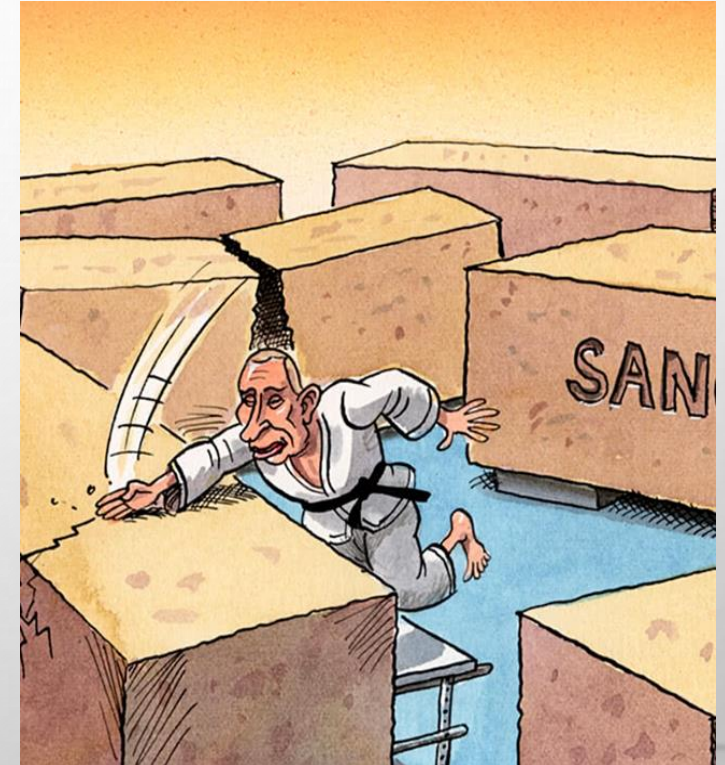
Geoeconomic Strategies - Coercion

Instruments

- Trade sanctions – export-, import controls
- Financial sanctions – debt-, investment restrictions, financial embargoes (eg. de-swiftization)
- Currency warfare
- Asset seizures

Effects

- Extra-territorial/secondary effects
- Decoupling effects



Geoeconomic Strategies - Binding

- Economic alliances (EU, EEU)
- Economic aid (Marshall Plan, development aid)
- Trade agreements (NAFTA, EU-Mercosur)
- Investment agreements (ACIA, bilateral)
- Loan programs (World Bank, IMF, BRICS Bank)
- Infrastructure alliances and projects (BRI)



Geoeconomic strategies - **Wedging**

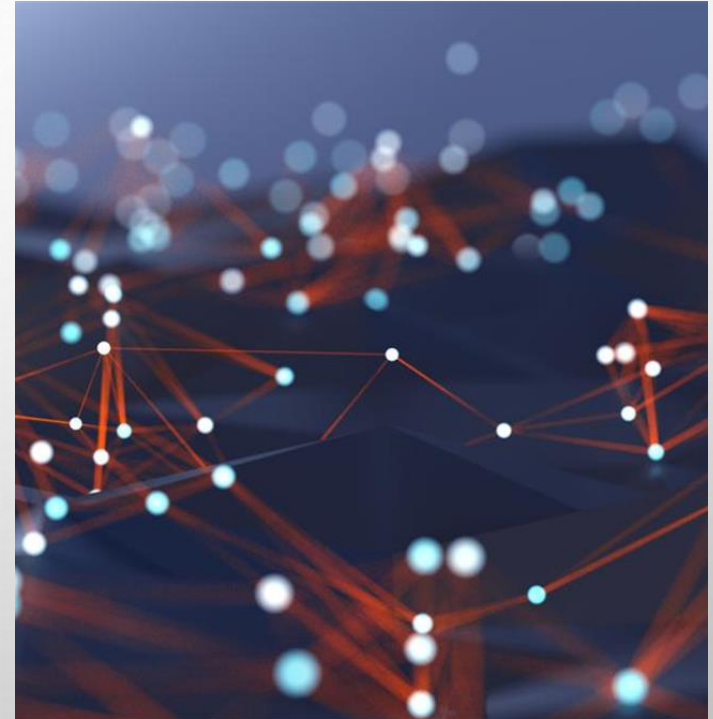
Economic sticks and carrots

- Manipulating export prices
(GASPROM)
- Selective economic accomodation
(NORD Stream)
- Corruption networks (Laundromat)



Geoeconomic strategies - **Hedging**

- Resilience (CER directive)
- Diversification (Critical Raw Materials act)
- Supply security (LNG)
- Self-sufficiency (Chips Act)



How International Economics Is Changing: Geoeconomic Trends



- Weaponization
- Securitization
- Balkanization

Geoeconomic Trends - Weaponization

Economic policy used as a strategic weapon

- New financial sanctions with extraterritorial effects
- Sanctions against companies and individuals
- Companies used for espionage
- Strategic corruption

➤ Vulnerability to sanctions, corruption and espionage increasing



Geoeconomic Trends - **Securitization**

Security-sensitiveness increasing

- Investment screening (inbound and outbound)
- Export controls
- Science and technology cooperation restrictions
- Data localization regulations
- Critical infrastructure protection regulations
- Reshoring subsidies
- New industrial policy



➤ Broader state intervention in strategic sectors

Geoeconomic Trends - **Balkanization**



Disintegration of global economic networks into smaller ecosystems

- Decoupling of global value and supply chains
- Competition over technical standards and norms
- Competing economic and technological "spheres of interest"

➤ 'Gated globalization'...?

From Market Capitalism to **Strategic Capitalism**

		Market Capitalism	Strategic Capitalism	State Capitalism
State Intervention	<i>Scope</i>	Limited	Selective	Broad
	<i>Driver</i>	Economic	Security	Political
State-Corporate Relations		Distant	Varied	Close

Impact on Supply Chains

- Market access
- Technology development and transfer
- Sourcing of raw material
- Access to talents
- Supply chain reorganization



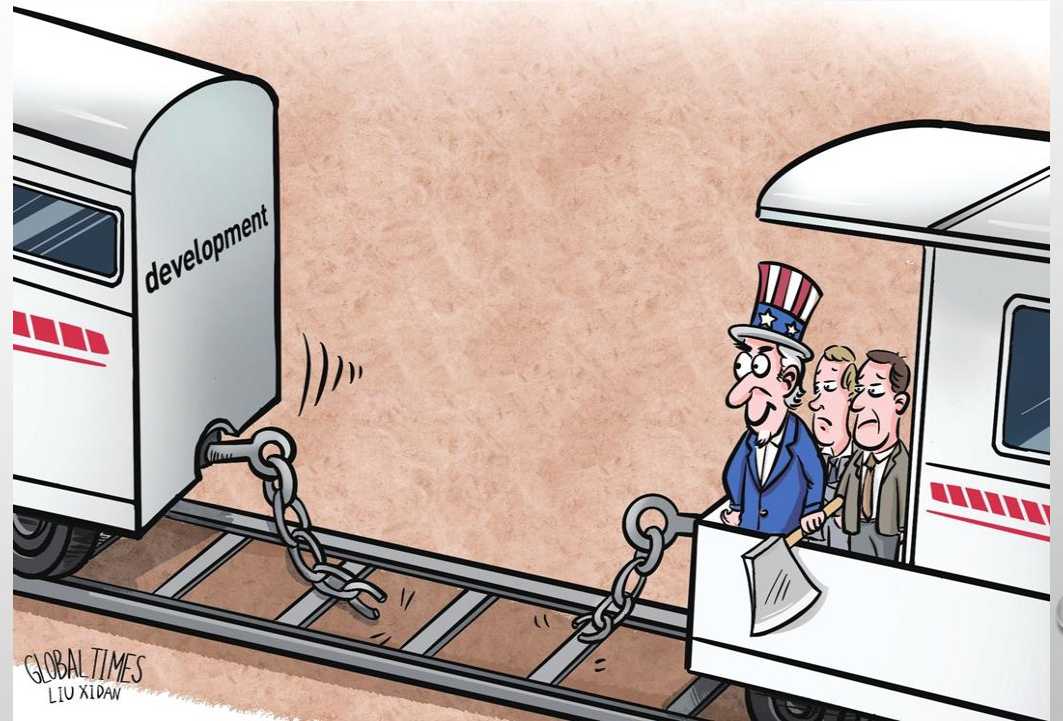
Market Access



- "No go markets" limit strategic options
- Risk of stranded assets
- Crowding-out effect due to "made in" policies

Technology Development and Transfer

- Loss of critical technology partners
- Risk of being caught in "digital/data traps"
- Outbound investment screening to limit technology cooperation with third parties



Sourcing of Raw Materials

- Significantly increasing price fluctuations
- Loss of access to critical raw materials
- Risk of increasing dependence on few suppliers



Access to Talents

- Loss of access to critical expertise
- Growing risk of espionage
- Risk of C-level "gloeconomic decapitation" due to export license requirements



Supply Chain Reorganization

- Public policies risk offsetting market signals
- Friend-shoring risk undermining diversification
- Corporate capacities risk becoming overstretched



The background is a light gray gradient with several realistic water droplets of various sizes scattered in the corners. The droplets have highlights and shadows, giving them a three-dimensional appearance.

Thank You!

mikael.wigell@fiia.fi