cerre Centre on Regulation in Europe

# RESILIENCE IN DIGITAL SUPPLY CHAINS: OPPORTUNITIES FOR GLOBAL AND INTERNATIONAL GOVERNANCE

**September 2024**

**Paul Timmers**

GLOBAL GOVERNANCE FOR THE DIGITAL ECOSYSTEMS: PHASE TWO

cerre

Report

# Resilience in Digital Supply Chains: Opportunities for Global and International Governance

Paul Timmers

September 2024

*"The foundation for success is a Europe that controls its own destiny", Vincent Clerc, CEO AP Møller-Maersk, 2024*

As provided for in CERRE's bylaws and procedural rules from its "Transparency & Independence Policy", all CERRE research projects and reports are completed in accordance with the strictest academic independence.

The project, within the framework of which this report has been prepared, received the support and/or input of CERRE member organisations. However, they bear no responsibility for the contents of this report. The views expressed in this CERRE report are attributable only to the authors in a personal capacity and not to any institution with which they are associated. In addition, they do not necessarily correspond either to those of CERRE, or of any sponsor or of members of CERRE.

© Copyright 2024, Centre on Regulation in Europe (CERRE)

info@cerre.eu – www.cerre.eu

# Table of Contents

# About CERRE

Providing high quality studies and dissemination activities, the Centre on Regulation in Europe (CERRE) is a not-for-profit think tank. It promotes robust and consistent regulation in Europe's network, digital industry, and service sectors. CERRE's members are regulatory authorities and companies operating in these sectors, as well as universities.

CERRE's added value is based on:

- its original, multidisciplinary and cross-sector approach covering a variety of markets, e.g., energy, mobility, sustainability, tech, media, telecom, etc.;
- the widely acknowledged academic credentials and policy experience of its research team and associated staff members;
- its scientific independence and impartiality; and,
- the direct relevance and timeliness of its contributions to the policy and regulatory development process impacting network industry players and the markets for their goods and services.

CERRE's activities include contributions to the development of norms, standards, and policy recommendations related to the regulation of service providers, to the specification of market rules and to improvements in the management of infrastructure in a changing political, economic, technological, and social environment. CERRE's work also aims to clarify the respective roles of market operators, governments, and regulatory authorities, as well as contribute to the enhancement of those organisations' expertise in addressing regulatory issues of relevance to their activities.

# About the Author

Prof Dr Paul Timmers is a research associate at the University of Oxford, Oxford Internet Institute, professor at European University Cyprus, visiting professor at KU Leuven and the University of Rijeka, senior advisor EPC Brussels, President of the Supervisory Board Estonian eGovernance Academy and CEO of iivii. Previously, he was Director at the European Commission/DG CONNECT where has held responsibility for legislation and funding programmes for cybersecurity, eID, digital privacy, digital health, smart cities, and e-government. At the European Commission, he was also a cabinet member of European Commissioner Liikanen.

# Executive Summary

A supply chain is a network of suppliers and buyers, the related products and services, their flow, resources, information, people, and activities, with the purpose to deliver products and services efficiently, effectively, and sustainably. Digital supply chains concern digital products or services. Resilience in supply chain concerns the ability to recover quickly from unexpected events. The objective of this report is to: Deepen the understanding of resilience of digital supply chains and recommend actions on global/international governance to strengthen such resilience. The recommendations are for EU institutions and EU Member States as well as EU industry.

Supply chain resilience is threatened by geopolitical conflicts, breaches of cybersecurity, climate change, and by idiosyncratic shocks such as the COVID-19 pandemic and hazards such as fire and human error. Supply chain resilience is critical for economic progress and societal stability, safety and wellbeing, economic and national security. It has risen to the top of corporate and political agendas.

Companies and governments already take actions for supply chain resilience such as supplier diversification, re-shoring, investing in redundancy, 'just-in-case' next to 'just-in-time', monitoring, and international coordination. Actions, driven since 2017 by geostrategic rivalry of the USA and China, have been further stepped up due to the COVID-19 pandemic and Russia's war against Ukraine.

There can be difficult trade-offs between resilience and economic efficiency and supply chains can be extremely hard to disentangle or 'de-risk'. Profound de-globalisation risks causing unacceptable economic and welfare losses due to reduced global efficiencies. Yet, there are already significant shifts, concentrating trade relations on 'likeminded' countries, i.e., reducing geopolitical distance.

For the EU, going it alone is not an option. Despite its industrial and technological assets, the EU does not have enough strengths (such as in financing, natural resources, skilled people, and digital infrastructures) to ensure digital supply chain resilience through self-sufficiency. International and global collaboration and governance are necessary and appropriate. The EU already engages in concrete policies for resilience of (digital) supply chains and related international governance.

Yet, the hard reality is that the EU risks losing out to the US and China, geopolitically and geoeconomically. The USA and China invest massively in domestic capacity which is hard to match for the EU. For instance, the EU cannot reach a similar 2030 goal for semiconductors as the US with current levels of investment at one-third of US levels. The US is a digital, financial, and military powerhouse, acting fast with unabashedly America-First industrial policy. Of 8 key digital technologies the EU leads in only one, connectivity, and is lacking industrial capacity in several key digital technologies such as AI, cloud, and semiconductors. China *de facto* controls a wide range of supply chains as a result of its systematic, decades-long engagement with foreign suppliers and its strong China-Only internal policies for economic security.

Without further action, EU dependencies will worsen, jobs will be lost, social stability and the EU's industrial base will erode further. There is an **urgent need for speed,** and it is imperative to **mobilise all policy instruments** as global competition does**, be competitive with incentives such as public funding, tax incentives, and fast approvals,** and **reinforce strategic focus and policy/strategy staff**.

The root causes of the gap between the EU and US and China are political disagreement of EU Member States and risk aversion, at times exacerbated by delusional lack of realism about the size of challenges and the power of Europe. Not everything is bleak, however. Political will has grown to jointly address resilience, economic security, and strategic autonomy. The European Commission (EC) acted fast to counter crises. Old taboos are being overcome with more acceptance of EU action in industrial policy, national and economic security, and debt-sharing. Examples are joint COVID-19 vaccines procurement and recovery funding or sanctions against Russia. A hallmark of the EU is consistent, long-term policy engagement as in standardisation, international law, trade, and development. The EU has strong companies and knowledge institutes. The EU is a normative and regulatory frontrunner with a potential 'Brussels effect'. Above all, the EU has an attractive and large internal market.

With a prioritised 2024-2029 agenda, EU institutions, Member States and companies can secure and maintain a strong position in international governance for resilience of digital supply chains. However, EU policy for resilience of digital supply chains must be **realistic** about the EU's capabilities, capacities, and control, and about future disruptions such as an armed conflict over Taiwan, American isolationism, subsidy wars, post-colonial backlash, and supply chain transformation by AI, IoT, and 5G. Policy for resilience must have **flexibility** and increase **understanding** of the nature of digital supply chains resilience. This report aspires to make a small contribution in that respect.

The analysis of this report and the four case studies (semiconductors, critical raw materials, software, and finance/banking supply chains) lead to a set of policy principles and recommendations.

**Principles** – for EU involvement in global/international governance for digital supply chain resilience:

- ***Decisiveness and leadership*** answering the need for speed. Global rivals move fast. With a limited number of suppliers, first-comers win. At EU level there must be political leadership.
- ***Comprehensiveness and consistency*** mobilisation of all policy instruments, from market access regulation to investment, employment to trade, civil to defence, internal to external policies.
- ***Win-win and mutual interdependency*** with suppliers, co-developers, customers from across the world, enabling value for all from specialisation and deterring weaponisation.
- ***Realism and flexibility*** to not claim leadership in all technologies and supply chains and nurture like-mindedness yet accept trade-offs for EU resilience.
- ***Anticipation, proactiveness, and deepening***: policy must be able to respond and anticipate, be geopolitically aware, technology-aware, and society-aware.

**Recommendations -** summarised below with more detail in the last chapter of this report.

1. Consistently advance integrated, focused policy for digital supply chains resilience:
    a. EC/EEAS to put forward a comprehensive strategy for digital supply chains resilience, joining up digital, green, industrial (R&D, skills, investment, EU-internal supplier industries-user industries partnering e.g., in automotive, energy, medical devices, defence and space), market access, corporate due diligence, trade, and foreign policies.

   b. EC to provide a list of digital supply chains, prioritised on criticality and feasibility-to-act, using the EC open strategic autonomy assessment and list of key technologies in the EU economic security policy, focusing on emerging areas rather than catching up.

2. Promote win-win global/international cooperation for digital supply chains resilience:

   a. EC and European External Action Service (EEAS) to rapidly move forward with the EU-US led Minerals Security Partnership Forum of resource-rich and consuming countries for secure and sustainable supply of critical raw materials; and propose realistic win-win projects that fully mobilise EU Global Gateway funding.

   b. EC/EEAS to propose a similar approach in *digital* supply chains, both technological (AI, software, semiconductors, IoT, 5G/6G) and sectoral (logistics, manufacturing, health) to coordinate on supply shortages, enable specialisation, and pre-empt trade and subsidy wars.

3. Mobilise public procurement:

   a. EC to update the Public Procurement Directive to enable Europe-First and EU joint procurement for digital supply chains resilience where this promotes resilience and strategic autonomy (quantum, AI and cybersecurity, advanced semiconductors, drones, 6G, etc.) and issue a related Recommendation to unlock Cohesion Funds for economic security.

   b. Member States to include digital supply chains resilience in their public procurement and promote this by combining civil and military public procurement.

4. Lead in a global community approach to digital supply chains resilience:

   a. EC/EEAS to take the lead in cooperation for software supply chain resilience, leveraging cyber-cooperation of Member States and European open-source communities; and promote standards for open-source security and for digital supply chains resilience with the US and the OECD.

   b. EC and industry to set up an 'International Reserve' of experts on digital supply chains resilience to assist individual companies in their digital supply chains resilience.

   c. EEAS and EU Member States to promote norms and confidence-building measures for resilience of digital supply chains in the UN Global Digital Compact.

5. Advance monitoring of international governance in digital supply chains resilience:

   a. EC, EU Member States, and industry to form a resilience monitoring group to critically assess international governance of digital supply chains resilience on the basis of indicators and qualitative criteria such as policy synergies, or best practice learning in global governance.

b. EC to set up a Digital Supply Chains Resilience Lab for public-private-civil society partnerships among allies, fostering innovation and shared supply chain data infrastructures.

c. EEAS/EC to develop governance strategies for digital supply chain resilience and benchmark policymaking speed, supporting EU engagement in international governance and diplomacy.

6. Advance understanding and long-term strategic thinking:

   a. EC with OECD and industry to develop supply chain resilience metrics and supply chain modelling, and, where appropriate, propose these for international standardisation.

   b. EC/EEAS to set up a Digital Supply Chains Resilience Expertise Centre; exercise scenarios that consider both the cost of a break in resilience and the likelihood or risk of a break of resilience including geopolitical risks.

   c. Industry and academia to simulate the interplay of international governance and supply chain structure and dynamics to understand the limits of mutual interdependence such as in semiconductors, incentives for resilience in open-source communities, and systemic or cascading resilience risks in coupled supply chains such as energy and telecoms.

# 1. Introduction

**Chapter Summary**

We need to define basic terminology such as digital supply chain and resilience. The objective of the study is to better understand the linkage between digital supply chain resilience and global governance and provide recommendations on global governance to reinforce digital supply chain resilience. Case studies inform the analysis at supply chain level and global governance level.

**What are supply chains?**

A supply chain encompasses all the processes involved in the creation and delivery of a product from raw materials to the end customer. A supply chain is a network of suppliers and buyers, the related products and services, their flow, resources, information, people, and activities with the purpose to deliver products and services efficiently, effectively, and sustainably. The term value chain is also often used, to draw attention to value creation in these chains. When used here, we consider it in the sense of supply chain, focusing on value created by the flow of goods and services. The supply chain term 'downstream' means receivers (buyers) of inputs that are flowing to them from 'upstream' producers (suppliers).

**What are digital supply chains?**

Digital supply chains are supply chains that concern digital products or services. They therefore consist of the complete set of software, hardware, and services; companies and other organisations developing, producing, delivering, and maintaining these; combined with the flow of into the products and services that are put to real-life use by businesses, governments, and citizens. Table 1 gives some examples of digital supply chains.

**What is supply chain resilience?**

Supply chain resilience is the ability of supply chains to recover quickly from unexpected events. A resilient supply chain can easily adapt, rebound, or recover when faced with economic shocks that are either idiosyncratic or systemic (Ponomarov & Holcomb, 2009). The JRC has addressed resilience for several years in Strategic Foresight Reports (JRC, 2023b). According to the JRC, "Resilience is defined as the ability not only to withstand and cope with challenges but also to undergo transitions, in a sustainable, fair, and democratic manner."

**Why is it relevant to analyse the resilience of digital supply chains?**

Supply chains suffer from shocks, disruption, and degradation due to systemic and idiosyncratic causes such as climate change, geopolitical adversity technological change - especially cybersecurity threats- , pandemics, hazard, human error, and malice. Supply chains should be resilient to provide stability, safety, security, efficiency, effectiveness, sustainability, and innovation in the economy and society.

**How serious are threats to the resilience of digital supply chains?**

In the recent past there have been serious disruptions from the COVID-19 pandemic, the war against Ukraine, attacks on ships in the Red Sea, cyber-attacks affecting many critical products and services such as raw materials for medicines, gases for production, petrol, semiconductors, medicines, blood-testing, etc. Natural disasters, weather/climate change-related events, mishap or human error have similarly led to massive disruptions at great and unanticipated cost (European Commission, 2023d), (The White House, Council of Economic Advisers, 2023), (Igan et al., 2022), (ISPI, 2024b), (Emily Benson, 2023; ISPI, 2024a), (Baldwin et al., 2023). Recently, concerns are rising that state-sponsored espionage and infiltration is intended to prepare for future disruption, also called pre-positioning (CISA, 2024), (Hmaidi, 2023). In the wider picture, it is alleged that China exercises state influence and provides unfair state support in order to take over whole industries (European Commission, 2023d, 2024b) as well as that there is massive human rights abuse in supply chains (US Senate Committee on Finance, 2024).

EC President von der Leyen said in her 2024-2029 Political Guidelines: “We have seen first-hand the dangers of dependencies or fraying supply chains – from medical products in the pandemic to Putin’s energy blackmail or China’s monopoly on raw materials essential for batteries or chips.” (Ursula von der Leyen, 2024b).

**How can we improve resilience of digital supply chains and is that effective?**

To some extent, ‘the market’ has been able to respond fast and adequately in a number of situations, to the extent that often supply recovered rather quickly and trade has continued to grow. However, this came at great cost, not only financially but also in human suffering. Moreover, the threats ahead are very worrying: ‘the market’ does not respond well to war, undermining sovereignty, climate change, or systemic cascading cyber-attacks. Companies are not intrinsically motivated to ensure supply chain resilience to contribute to public goods, in particular, strategic autonomy, economic security, and national security.

Increasingly – given the rising threats – public policies are being put in place to strengthen and increase supply chain resilience. China has a long-running programme to systematically reduce foreign supply chain dependencies. The US has embarked on massive investment for domestic capacity. Both the US and China are exercising control of supply chains through sanctions and export controls. The EU is putting in place an extensive economic security package. The impact of these on supply chains is certainly visible, but the jury is out as to whether they deliver the desired resilience.

In terms of public policy, resilience is part of economic security which in turn is part of strategic autonomy, see Figure 1. Economic security encompasses promoting resilience as well as protection of economic assets and trust in international economic relations. Strategic autonomy is the means to safeguard sovereignty. It consists of capabilities (knowledge, skills), capacities (production, manufacturing, services) and control over these capabilities and capacities to enable deciding and acting on one's own future in economy, society, and democracy. This report regularly refers to the wider context, given the critical importance of digital supply chain resilience for economic security and strategic autonomy. Resilience is a necessary but not sufficient condition for economic security and strategic autonomy.


*Figure 1 Resilience - Economic Security - Strategic Autonomy*

This study focuses on a specific contribution to strengthening digital supply chain resilience, namely global or international governance. Such governance can be by the private sector, governments, or by public-private partnerships. We will extensively use 'global governance' or 'global/international governance' as shorter expressions for 'global or international governance'.

The study's objective is to provide:

1. understanding of digital supply chain resilience and related governance;
2. recommendations to strength digital supply chain resilience with global/international governance.

**What is the outline of this report?**

The study is based on a number of case studies that provide insights into the challenges of and approaches to digital supply chain resilience. From these we can draw lessons for global governance.

**Chapter 2** explains the analysis framework to address the interplay of global governance with digital supply chains at meso-level (what does it mean for a supply chain) and macro-level (what does it means for economy as a whole). The cases also give examples of the micro-level (what does it mean for a company).

The short **Chapters 3-6** provide the case studies (semiconductors, critical raw materials, finance/banking, software). These cases have been chosen since they are important examples of digital supply chains; and illustrate the rich complexity of digital supply chains and related governance. Moreover, we can categorise digital supply chains in three types: digital technology supply chains, sectoral digital supply chains where a sector applies digital technologies, and cross-cutting supply chains. The three cases represent each one of these categories. See Table 1 below which also gives many more examples. We have added critical raw materials, as this is a key upstream supply chain for

most downstream digital supply chains and provides an insightful case with lessons for digital supply chains. To be clear, technology and application supply chains are often interlinked.

| Digital supply chain type | Examples (in bold the cases in this study) |
|---|---|
| Digital technology | **Semiconductors**<br>Quantum<br>5G/6G<br>Generative AI<br>Supercomputing |
| Sectoral (applied technology) | **Finance & Banking**<br>Automotive (esp. automated driving)<br>Smart industry / Industry 5.0<br>Smart logistics<br>Defence<br>Drones |
| Cross-cutting | **Software**<br>Cybersecurity<br>**Critical materials** |

*Table 1 Types of digital supply chains*

Each case is briefly presented and analysed in terms of resilience and current public policy and corporate strategies for resilience. For each we then focus on relations to global governance.

**Chapter 7** summarises the findings from these cases and generalises them into more broadly applicable conclusions on the relationship between global governance and digital supply chain resilience. Here the focus is on the meso-level answering how this global governance relates to the structure, dynamics, resilience, and other characteristics of individual supply chains. We also discuss the upsides but also the downsides of pursuing resilience policy within wider geopolitical or geoeconomic policy, i.e., as an element in strategic autonomy policy.

**Chapter 8** takes the macro-perspective, addressing the macro-level in terms of economic and political impact, aggregate material and immaterial costs, robustness, timescales, and longer-term perspectives.

**Chapter 9** provides recommendations and actions.

An extensive bibliography is added in annex.

# 2. Analysis Framework

**Chapter Summary**

The analysis is based on considering essential characteristics of supply chains and how these relate to governance within the supply chain and internationally.

The analysis logic is captured in Figure 2. Supply chains have a structure of entities and their relationships and are conditioned by factors such as natural resources or technology. We are interested in understanding the interplay of supply chains and global/international governance. Such governance has certain characteristics such as mandate and participants and is affected by forces such as geopolitics. Ultimately, we aim for recommendations on global governance that, through this interplay, have as an outcome the improvement of resilience of (digital) supply chains, albeit that there may be a trade-off with other outcomes such as impact on GDP.

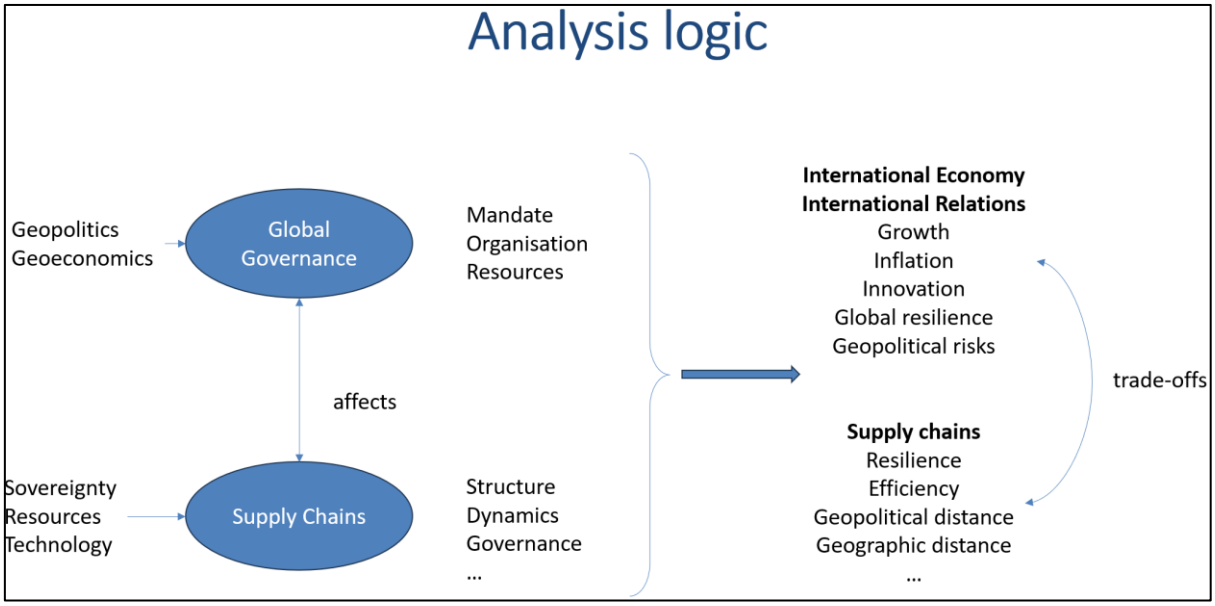



*Figure 2 Analysis logic*

## 2.1 Supply Chains: Structure, Strategy, Governance, Resilience

Supply chains are characterised by their structure, dynamics, and governance, influenced by external factors, and deliver economic efficiency, resilience. Some of their characteristics may be measurable. Companies will pursue strategic approaches to improve resilience, e.g., supplier diversification, stockpiling, etc. They may also take ad-hoc tactical measures such a spot-purchasing. Supply chain

actors and governments may work together for resilience, thereby creating a layer of supply chain governance. Spelling this out we have:[1]

1. the **structure** and **dynamics** of a supply chain and its wider industrial ecosystem: who are the actors in the system (fabs, raw material processors, etc.), what are their relations (supplier, buyers, etc.), what is the structure of the supply chain (as, e.g., captured in a graph), how dense or diversified or geographically concentrated is the supply chain, what are specific supply chain structures (e.g., chokepoints, mutual dependencies), and consequently what are the degrees of freedom are(e.g., are there alternative suppliers), and finally, how do actors and their relations map to international relations (e.g., are they in a partnership of likeminded countries). Extensive literature exists to characterise structure and dynamics as a system of actors and relationships.

2. **strategies** to address resilience, economic security, strategic autonomy: a systematic and goal-oriented approach to resilience, such as preferential procurement from national or likeminded suppliers, export controls for advanced technologies or friendshoring. Strategic control is exercised onto specific actors in the industrial ecosystem who in turn control specific assets (e.g., IP[2], raw materials, fabs[3]). A supply chain resilience strategy likely needs tools to understand and control supply chains such as product labelling (e.g., of country-of-origin) and quality or security certificates. Such information may be supported by a distributed ledger ('blockchain') to guarantee quality of information, bill of materials and related standards.

3. supply chain **governance** seeks to organise, affect, or control supply chains, such as a collaboration on ICT supply chain security, a standardisation organisation, trans-Atlantic cooperation e.g., in the Trade and Technology Council (TTC), international agreements such as the Wassenaar agreement for export controls, etc.

Such supply chain / governance analysis is ambitious as it seeks to answer tough questions about a complex set of actors, products, use cases, business models and political intentions in a complex context and partially with under-defined terminology. For lack of an integrated analytical framework, this study combines insights and models from international relations, business ecosystems dynamics and business management.[4]

## 2.2 Micro-Meso-Macro

As in the CERRE Digital Industrial Policy report, we consider the three levels of companies, industrial ecosystem, and the geopolitical system, see Figure 3 based on Timmers (2022a). At the top level, we want to understand how global governance for resilience of digital supply chains affects overall functioning of the global economy, e.g., patterns of global trade and Foreign Direct Investment (FDI). We also want to understand how this international level relates to the characteristics of supply chains themselves such as their structure and geographic locations. Supply chains are part of larger 'industrial ecosystem', in the sense of Michael E. Porter (1990) and illustrated in Figure 4. Ultimately – though

[1] (1) and (2) correspond to network structure, network dynamics, and network strategies as in Network Analysis of Supply Chain Systems by (Bellamy & Basole, 2013).
[2] IP = intellectual property.
[3] A fab is a plant that produces semiconductors.
[4] A similar approach was followed in Timmers (2022a).

that is not addressed *in extenso* in this study -, we also want to know how this relates to companies such as for their economic performance or their individual influence on strategic decision-making. In economic terms these three levels correspond to respectively macro-, meso-, and micro-economics.

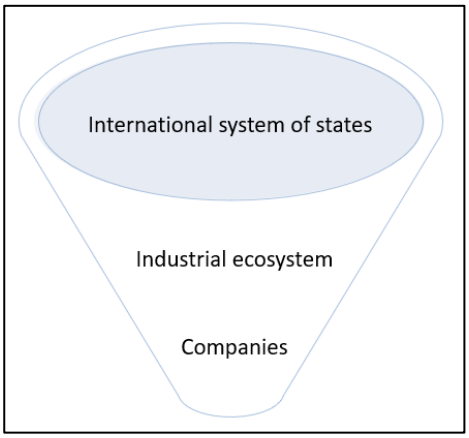



*Figure 4 Three levels*

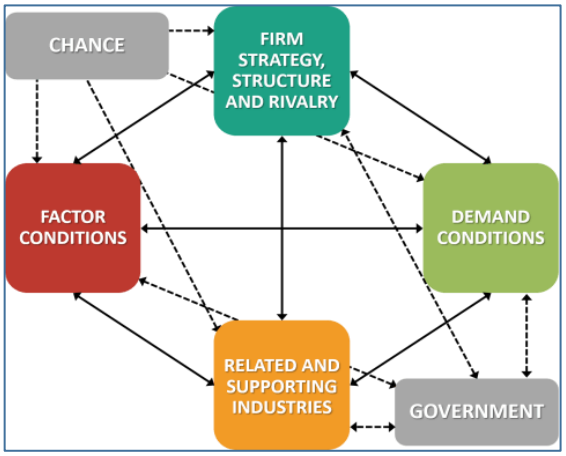



*Figure 3 Industry ecosystem (after Porter)*

Recently, meso-economics gets increasing attention, as argued by Tett (2024). This is understandable given the increased political focus on economic security which in turn concentrates a great deal of attention on supply chains and their resilience.

Supply chain is a meso-economic concept that can be analysed with graph theory. Some academic references that make use of graph theory or related economic or international political economy theories for supply chain analysis include:

- Janeway, (2024) who argues convincingly the rise in importance of meso-economics, and contends that graph theoretical analysis is especially useful today because much more data is available on companies and their relations.
- Aguila & ElMaraghy, (2019) who show a theoretical model that defines a supply chain resilience index and calculates it for some examples based on metrics of density, scale, and centralisation. They consider the geographic location of nodes (supply chain entities) in the network topology. Such modelling allows for examining scenarios and strategies to modify the supply chain.
- Meso-macro studies of supply chains show that micro disruptions can turn into macro-level effects, even extending across the economy, e.g., (Acemoglu & Tahbaz-Salehi, 2024).
- Jiang et al., (2021) discuss the robustness of supply chains comparing efficiency-optimising Just-In-Time to resilience-driven Just-In-Case and to Just-In-Worst-Case; for practical cases see also (Masters & Edgecliffe-Johnson, 2021).
- Farrell & Newman, (2019) who argue weaponisation of techno-economic network structures, identifying bottlenecks, chokepoints, and centralisation points, such as

At macro-level we certainly want to know whether and how resilience changes and preferably measure this economy-wide (we return to this in section **Error! Reference source not found.**). One macro-level indicator is the World Bank supply chain stress index (World Bank, 2024), which is a

logistics-based indicator. Figure 5 shows the rise of stress due to the Red Sea shipping disruptions in September 2023.

However, we also need to consider other macro-economic indicators and be aware of possible trade-offs such as with economic efficiency, GDP growth, financial stability (Tett, 2023), inflation (Giovanni et al., 2022; Tett, 2024), (Rubbo, 2024), innovation and R&D allocation (Liu, E. & Ma, Song, 2023).


*Figure 5 Supply Chain Stress Index, World Bank Trade Watch, 2024*

Another important indicator is trade and, more generally, aggregate indicators of the 'realignment of global value chains' expressed in levels of trade, geographic concentration of trade, regional economic integration, the length of supply chains or geographic distance (Qiu et al., 2023a), as well as geopolitical distance of trading partners (McKinsey, 2024a).

To summarise: supply chains are networked and dynamic structures of entities, their relationships, and governance by means of technological constructs such as supply chain management software and social constructs such as regulations, standards, monitoring, contracts, organisations, etc. From this - in theory - economic performance, resilience, and other metrics can be derived and critical control points in the structure can be identified such as bottlenecks. We are interested in global or international governance that can affect or be affected by any of these aspects of a supply chain.

# 3. Case: Semiconductors

**Chapter Summary**

Semiconductor supply chains are extraordinarily complex. Around the world, significant public policy initiatives and corporate strategies aim to increase semiconductor supply chain resilience, but full resilience is extremely hard to achieve. Global/international governance is bipolarizing.

## 3.1 Description

Semiconductors supply chains involve a huge number of companies and research centres, with a large variety of functions, from chip design to fabs, from materials research and engineering to the chip packaging and testing, etc. see Figure 6. Some of the thousands of companies are shown in Figure 7 from (Flaningam, 2023).

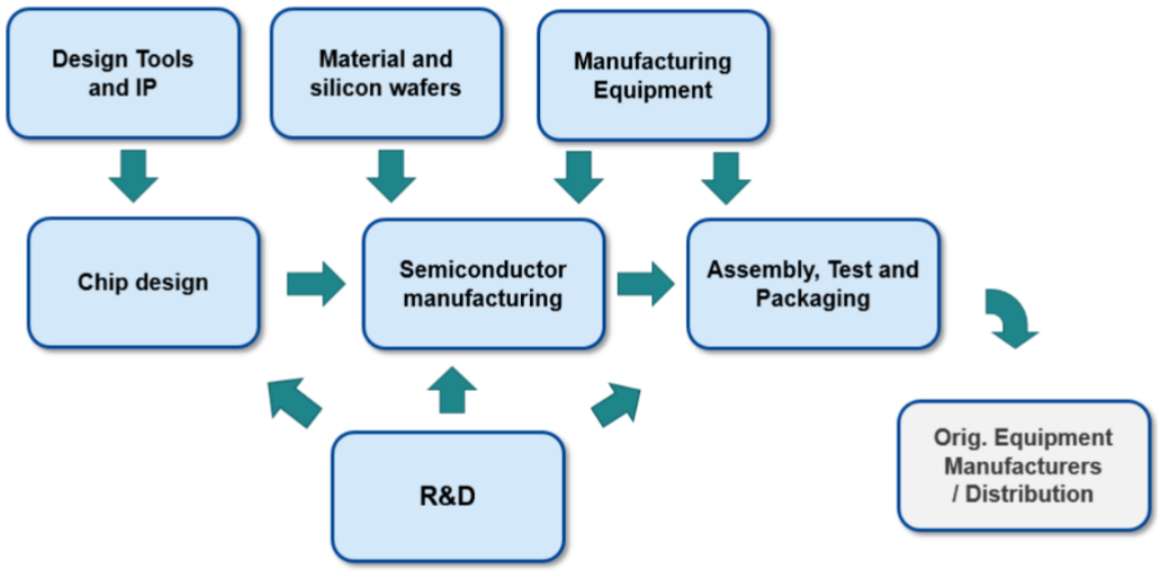



*Figure 6 Semiconductor value chain, source EC (2022), SWD Chips Act*

Excellent descriptions of the semiconductors industrial ecosystems are in Boston Consulting Group & Semiconductor Industry Association (2021), and European Commission (2022a, pp. 7–12), as well as in highly readable accounts of the chips industry such as Hijink (2023) and Miller (2022). The weaponisation of semiconductor supply chains as part of geopolitical competition and conflict is described in Farrell & Newman (2023a). None of these accounts can be all-comprehensive, though, as the semiconductor ecosystem is so vast and complex.

What such literature shows is that, beyond traditional supplier-buyer relationships, there are also extensive and mutual relationships between the entities such as equipment manufacturers that share

knowledge, research, investment, and financial risk with their specialised suppliers[5] or equipment manufacturers that must be constantly in-house and on-the-floor in the fabs. Hundreds of ASML engineers are on the floor in TSCM's fabs (Hijink, 2023). Yet another example is the fabless chip company NVIDIA being a risk-capital funder of startups who subsequently as customers are expected to generate a significant part of NVIDIA's turnover (Elder, 2024).

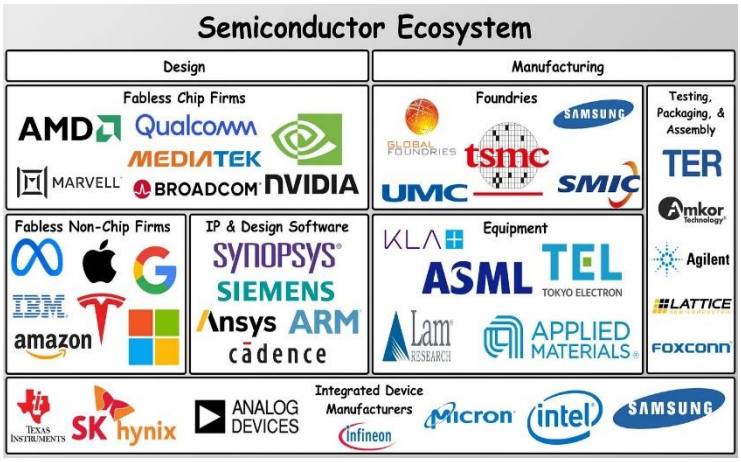



*Figure 7 Selection of companies in the semiconductor ecosystem*

Managing these relationships properly is a source of competitive advantage. ASML has over 5,000 suppliers globally. ASML invested heavily in developing these supplier-buyer relationships over many years. The company claims that this enabled it to take a lead and even establish a monopoly in EUV (Extreme Ultraviolet) lithography to produce below-3 nm semiconductors.

In the wider industrial ecosystem view (referring to Figure 4), governments play a special role. They can condition the market through regulation, provide factor inputs like skilled people, and can be both launch and end-customer. For instance, they ensure education to create and maintain a pool of specialist skills. They define and oversee export controls and may impose buying from local or 'friendly' suppliers.[6] They are a customer for military semiconductors. They are international negotiator of industrial cooperation with likeminded partner countries. They set environmental rules. They provide state aid for 'friendshoring,' etc.

## 3.2 Public Policies, Company Strategies

Semiconductors has rapidly become the focus of public policy of many developed and of developing economies. Company strategies have evolved from a supply chain perspective. Sometimes this has been in response to public policy but also often internally driven by seeking efficiency and complementarity. Let's discuss some of them here and relate them to supply chain resilience.

**Governmental policies:**

1. **USA**: the US Chips and Science Act made $53 billion investment available for R&D, design, and manufacturing through direct state aid, tax incentives, and favourable loans (Mui, 2024) (Figure 8 gives a breakdown in which $52.7 billion is for semiconductor manufacturing). The Act includes monitoring for shortages and critical dependencies to address risks for supply chain resilience. It promotes domestic manufacturing capacity, i.e., fabs, as well as human resource capacity building through skills training and STEM education. Domestic and foreign

[5] Such as ASML's investment in Zeiss (Miller, 2022).
[6] This is not limited to the cases described here. To overcome medicines shortages this is also happening in the pharmaceutical field, see e.g., (Thieu Vaessen, 2024).

(Taiwanese, Korean, Japanese) companies have been responding favourably by increasing their investment in the USA in fabs.

The USA has imposed export controls to China of advanced semiconductors end-products

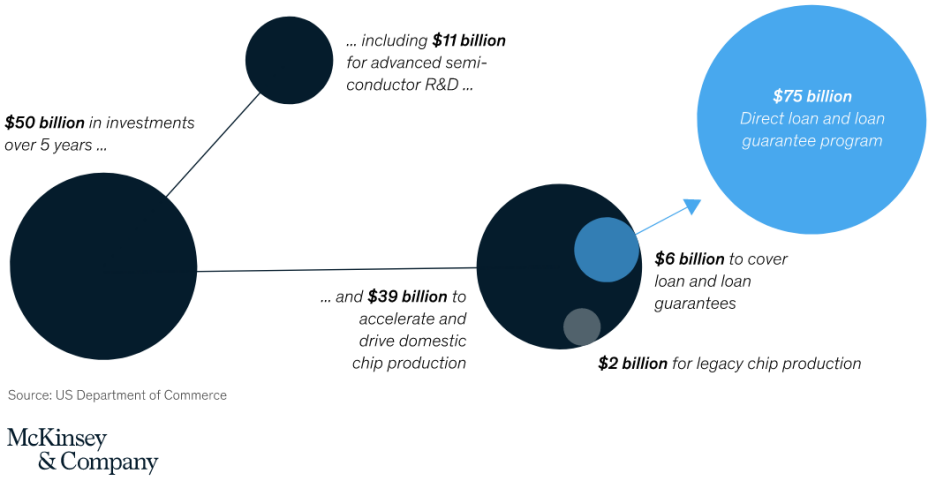



*Figure 8 US Chips and Science Act budgets, source: McKinsey (2024)*

(such as high-end AI chips), as well as production equipment and design capacity of advanced semiconductors. This affects not only US firms but also Dutch and Japanese companies that provide high-end lithography machines (ASML, Tokyo Electron and Nikon). This goes beyond today's resilience, namely, the US hopes to pre-empt or delay progress of China in the most advanced semiconductors (7 nm and smaller node sizes). This would then deteriorate China's resilience (read: self-sufficiency) in advanced military equipment. For an assessment of whether this would actually work see the 'risk of failure' discussion on page 71.

The US Chips Act also includes international partnerships, such as with Japan, South Korea, and Taiwan in the CHIPS-4 initiative and with the EU in the trans-Atlantic Trade and Technology Council. These seek to improve resilience in the supply chains by shared monitoring and common supply chain standards and mutual information to avoid subsidy wars. At the same time, US Secretary of Commerce Gina M. Raimondo expressed confidence that the US can house the entire supply chain for leading-edge chips (Center for Strategic and International Studies (CSIS), 2024). Pursuing an autarkic semiconductor strategic autonomy approach may, however, reduce the appetite for such international cooperation.

The US does not have in the semiconductors non-military market a 'buy America' policy (contrary to China) but does pursue a 'supply America' policy. The US also does not create strong supplier-buyer partnerships in semiconductors (again contrary to what China does), except for military procurement.

The USA is also developing partnerships with other Asian countries (e.g., India, Philippines) with the objective to further diversify suppliers. These countries, however, also want to move up from low value-added packaging, testing, and assembly to higher value-added manufacturing and design. They have their own aspirations to increase their strategic autonomy. A case in point is India. These countries are, however, also courted by China.

2. China: Semiconductors is one of 30 critical technologies identified already well before 2018 by the Chinese government. For each of these, approaches were developed to eliminate foreign dependencies. These are being implemented by companies themselves, with government support (Murphy, 2022). They include finding alternative suppliers, developing domestic production capacity, investing in domestic R&D, acquiring foreign companies and/or IP, and even theft of IP. Entrepreneurships, fierce domestic competition, and smart business strategies were driving such approaches as well. In the field of semiconductors examples include theft of IP from ASML in 2022 by a Chinese employee who reportedly later went on to work for Huawei.[7] China invests heavily to the tune of most recently $48 billion, within a longer-term plan (Naughton, 2021) and earlier investments of $22 billion in 2014, and $28-$42 billion in 2019. China clearly pursues strategic autonomy within which resides resilience.

   China seeks to overcome US export controls on most advanced EUV equipment by upgrading the previous DUV generation to produce chips with smaller node sizes and by an ambitious programme in advanced chips manufacturing. According to industry experts, China may not be able to readily move to the most advanced chips but may conquer the market for less-advanced chips with over-supply given its massive investment in fabs. If so, the automotive industry as a big buyer would run into yet another supply chain resilience risk (Smith, 2024). However, opinions are divided in this regard. Some experts argue that this capacity is largely to serve the Chinese market and, moreover, China would not have a cost advantage as these are capital-intensive rather than labour-intensive activities (The Economist, 2024a). Moreover, these chips largely go into so-called concentrated products, that is, products that are produced in a small number of countries only. These originate mostly from the USA and the EU, who can threaten with trade restrictions. However, the rapid rise of Chinese e-vehicle production (an important concentrated product) speaks against this. Summarising, the verdict is out on whether 1) China will catch up in advanced in semiconductors and 2) whether China will be able to control the supply of less-advanced semiconductors.

   China combines buy-side and supply-side through policy interventions. Being able and willing to do so gives it a big advantage, in particular relative to the EU where this appears to be far more difficult and there is more hesitation for such EU-level industrial policy. Recently, for instance, the Chinese government has asked carmakers to increase the local procurement of automotive-related chips to 25% by 2025 with the goal to eventually go fully local. China has also similar local procurement goals for car components. The shift to electrical vehicles brings a big opportunity to ‘go local’. Moreover, several car manufacturers such as BYD have their own semiconductors capabilities (Li et al., 2024). Chinese semiconductor manufacturers in turn are pushing their suppliers to go local such as for wafers, chemicals, and gases, which is also supported by government subsidies. This also holds for downstream activities such as packaging and testing services. Already foreign companies get outcompeted and leave the Chinese market (Tabeta & Ting-Fang, 2024).

   In response to US export restrictions, China retaliated in August 2023 by imposing export restrictions on germanium and gallium. In these two materials, both of high importance for

[7] As reported by (Diederik Toet - Computable, 2023). China did not contest this specific case but generally rejects accusations of theft of IP.

certain types of semiconductors, China controls respectively 60% and 90% of global supply. These restrictions threaten supply chain resilience for other countries. This is a form of retaliation within the same sector though there can be a spillover to other sectors if China would retaliate on other rare earths that have wider application such as neodymium which is widely used for magnets.

3. **EU**: the EU Chips Act is a comprehensive investment and policy program with three pillars: technological capacity building, production capacity investments, and semiconductor supply crisis management. The first pillar focuses on cutting-edge chip research, pilot production, standards, skills, and networking through the 'EU Chips Joint Undertaking', involving EU states, partner countries, and industry. It targets advanced chip design (sub-2 nm), quantum chips, and new production methods, aiming to strengthen the EU's pre-production phase and provide venture funding for startups. The second pillar supports establishing vertically integrated production facilities and 'Open EU Foundries', focusing on "first-of-a-kind" technologies that are not present in the EU. Companies can access State aid, direct funding for new fabs, and fast-tracked administrative permits. The third pillar aims to ensure chip supply continuity by monitoring early warning indicators for shortages and activating crisis mechanisms. In case of shortages, coordinated procurement can be conducted by the European Commission (mandated by EU Member States), and Pillar 2 companies may be asked to shift production towards critical semiconductors (Timmers, 2022a). The third pillar is therefore closest to resilience, whereas the other pillars are rather about strategic autonomy.

   GMF keeps an EU Chips Act Investment Tracker which shows 33 investments as per June 2024 (and over 100 in the US) – most of them announced rather than already implemented (GMF, 2024), see Table 2. The total of these semiconductor investments in the EU adds up to €110-150 billion which can be compared to €43 billion available from the EU Chips Act and investments in the US estimated to over $500 billion. All these figures must be taken with a fair amount of salt as often these are soft intentions for investment, there is likely some double counting and timescales for investment vary. Another projection, by BCG (2024) is $154 billion in Europe and $646 billion in the USA in Capex during over the next decade. Consistent in these numbers is that investment in the US is about 3 times larger than in Europe. According to the same source, Taiwan would outspend any other country with over $700 billion.

*Table 2 Semiconductor investments under the EU Chips Act (source: GMF)*

| **Country** | **Investments** |
|---|---|
| AT - Austria | 1 |
| CZ - Czech Republic | 2 |
| DE - Germany | 7 |
| ES - Spain | 2 |
| FR – France | 6 |
| IT – Italy | 9 |

| | |
|---|---|
| LT – Lithuania | 1 |
| NL – The Netherlands | 2 |
| PL – Poland | 1 |
| PT – Portugal | 1 |
| RO - Romania | 1 |
| **Total** | **33** |

The EU also coordinates in the TTC with the USA and has established partnerships that include joint work on semiconductors with other countries such as India, S. Korea, Japan, and Singapore. Additionally, the EU included in 2023 advanced semiconductors as one of four priority critical technologies (next to quantum tech, AI, and biotech) in its economic security risk assessment (European Commission, 2023b). The results of this assessment still must be announced. It may have consequences for outbound investments to counter the risk of technology leakage (European Commission, 2024a).

The European Commission has also approved two IPCEIs - Important Project of Common European Interest – on semiconductors and microelectronics, one in 2018[8] and a second one in 2023.[9] These are investment and R&D focused and indirectly address resilience through building technological capabilities and capacity in the EU. The second IPCEI explicitly mentioned in its objectives to contribute to 'Europe's ambition for a greener, digital, more secure, resilient, and sovereign society'. This IPCEI is therefore about both resilience and strategic autonomy.

4. **Other countries**: a range of other countries next to the US, EU, and China, have very significant public policy in this field such as S. Korea, Japan, Taiwan (see Figure 9, (BCG, 2024). Other countries in countries in Southeast Asia, Latin America, and Eastern Europe are expected to step up capacity in assembly, test, and packaging (ATP). This enables further supplier diversification and increase of resilience.

5. **Internationally**: the G7, presided in 2024 by Italy, has raised EU-US collaboration on exchange of information on semiconductor supply chains to the G7 level, stating "we welcome the establishment of a semiconductors Point of Contact (PoC) Group dedicated to facilitating information exchange and sharing best practises among G7 members. The PoC Group plans to exchange information on issues impacting the semiconductor industry, including but not limited to pre-competitive industrial research & development priorities, sustainable manufacturing, the effect of non-market policies and practices, and crisis coordination channels, leveraging the work of and in collaboration with the OECD Semiconductor Informal Exchange Network. The PoC Group intends to work throughout Italy's G7 Presidency and engage key stakeholders from industry, academia, and others." (G7, 2024; G7 Italia, 2024).

[8] https://www.ipcei-me.eu/.
[9] https://ipcei-me-ct.eu/.

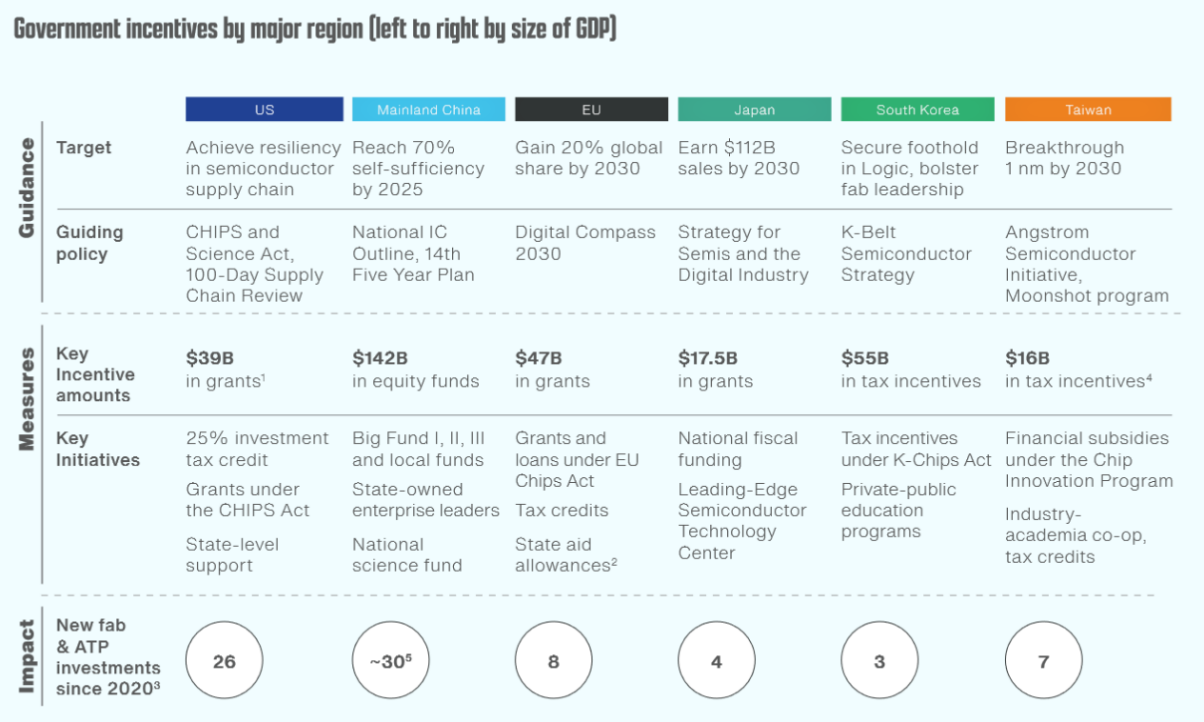



*Figure 9 Government incentives by major region, source BCG/SIA (2024)*

**Company strategies:**

1. *Expansion*: Major fab companies, TSMC, Intel, Samsung, SK Hynix, Global Foundries, Micron, STM and others, are constructing production facilities outside their country of origin, such as in the USA, Germany, Poland, France, Italy, India, Vietnam, and Singapore. They are enticed by government subsidies that seek economic growth, stronger national resilience, and even strategic autonomy in semiconductors. The are banking on the projected doubling of the market to about $1000 billion by 2030. They also must find new locations given limits in their home country in terms of engineers, water, electricity, or land.

2. *Diversifying suppliers or multi-sourcing*: Major producers are also opening new facilities in South-Asia and relocate facilities to have China+1, that is, be no longer solely dependent on production facilities in China.

3. *Vertical integration or co-investment*: semiconductor companies seek to take control of suppliers through co-investment or mergers and acquisitions (M&A) or develop their own in-house capacity. This is an old practice, e.g., ASML secured access to advanced Zeiss technology through co-investment.

4. *Contracting:* supplier-buyer contracts can stipulate resilience. This can also diffuse towards upstream contracts. Masters & Edgecliffe-Johnson (2021) report that a big German industrial group was confronted by the COVID-19 semiconductor shortage and was forced to shift from three-month non-binding arrangements with suppliers to 24-month commitments and payment in advance of receiving its chips.

5. *Scarce resource acquisition:* semiconductor companies seek to bind scarce talent, for instance, US companies seek chip design, R&D, and manufacturing talent in Europe and India and remarkably, also in China. The US firm KLA opened an R&D centre in Wales (BCG, 2024).

6. *Innovation*:

    a. Chinese companies seek to squeeze out the maximum from less-advanced equipment: following EUV export restrictions, ASML saw a marked uptick of purchases from China of its less-advanced DUV machines.

    b. Chinese companies manage, despite the export restrictions, to produce 7 nm and possibly also 5nm chips, probably by finetuning existing DUV equipment (intended for larger node sizes) and, in doing so, learning important skills for improving and refining production. This to some extent erodes the effectiveness of current export restrictions, but also, and possibly more importantly, nibbles away at the competitive advantage of companies such as ASML.[10]

7. *Stockpiling*: Chinese buyers are also buying at scale gaming PCs to strip them from their high-end NVIDA graphics cards that can be used for AI. In the past Huawei reportedly stockpiled 7nm chips ahead of export restrictions (News, 2019) although that may not have reassured customers as regards long-lasting maintenance of their telecoms equipment. Increasing inventory may be the most easily implemented strategy as reported by McKinsey.

8. *Information management and monitoring*: companies themselves also benefit from better data on the supply chain. An upstream automotive collaboration, Catena-X, was set up in 2020 to create an 'open data ecosystem' and 'data chains', involving major German car companies and their largest suppliers like Bosch, or Siemens. In the EU and the US companies participate in supply chain monitoring (as required by the respective Chips Acts).

9. *Protection*: Companies are raising their cyber-defences for both short-term resilience (business continuity) and long-term protection against IP theft and espionage. ASML works closely with its supplier base to also raise their level of cyber-capabilities and -capacities.

10. *Standardisation*: Information standards are required to enable sharing under monitoring obligations such as under the EU Chips Act and US Executive Orders. Cybersecurity standards are needed where semiconductors are in turn the upstream component that go into downstream products and where increasingly obligation exists such as under the EU Cyber Resilience Act and US Executive Orders.

11. *Collaboration*: national and international industry organisations provide data and strategic analysis on resilience and lobby governments, such as SIA (US), ESIA (EU), and SEMI (global).

12. *Retracting*: USA export controls spill-over into services and investment. The Abu Dhabi G24 investment fund decided to cull its Chinese customer base to appease the US and keep access to the US market (Cornish & Wiggins, 2024).

[10] Opinions are divided not about whether but about when China will manage to achieve 2-5 nm node sizes, see e.g., (Triolo, 2024) and (Mat Honan & James O'Donnell, 2024).

13. *Bypassing*: Russia has managed to bypass export restrictions by parallel and illegal imports via third countries.

## 3.3 Observations

**Structure and dynamics, policies and strategies**

Public policies for semiconductor supply chain resilience are using a language of control, protecting assets, chokepoints, de-risking, mutual dependencies, critical suppliers, diversification, nearshoring, friendshoring, self-sufficiency, concentration, monitoring, permissions, export restrictions, etc. This is a language of economic security and strategic autonomy, going well beyond resilience. It is also a language of structures, dynamics, governance, and strategy, that is, the key aspects we identified for supply chain analysis.

Though the semiconductor industrial system is very complex and a full overview of its structure and dynamics is not yet (publicly) available, focused and forceful policy interventions are already underway. Interventions range from investment programmes of many tens of billions of dollars, as mentioned before, to targeted export restrictions. It is generally recognised that semiconductor supply chain resilience necessitates a wide scope of integrated interventions. Indeed, governmental policies generally combine industrial, resilience, economic security, and national security aspects, but the mix is different across the world. For instance, the EU Chips Act is clear about the intention to build up industrial capabilities and capacity to be competitive in advanced semiconductors by 2030, while it also has a full resilience pillar with monitoring and production allocation in case of critical supply shortages. The USA Chips & Science Act, in addition, imposes national security restrictions on involvement in China as a condition for companies to benefit from that Act.

International dynamics are equally complex and intriguing. Likeminded partners are also competitors. Governments aspire for the suppliers in their country to become global competitors (the same aspiration is held by the EU). Global companies push back against governmental economic nationalism. One country's interventions incite other countries to react, if not to retaliate. Military concerns override economics. There is a mix of collaboration, competition, geoeconomic, and geopolitical warfare. The field is rife with political risks. It is important for actors to understand such political risks. This starts by having timely and detailed intelligence.[11]

The semiconductor case shows a wide range of company strategies (we will see some other additional ones and variations in the other cases). Some very large companies, near-monopolies, such as TSMC, Samsung, Intel, ASML, and Nvidia are in a special position as they can both afford to invest into expansion or M&A as well as impose discipline amongst their suppliers. However, even these, being further downstream and having dependencies on upstream companies, have their limits in what they can realise in terms of resilience.

Established industry organisations such as SIA and ESIA are highly active in studying and lobbying on semiconductor supply chain resilience. New user-industry collaboration such as Catena-X in

[11] In semiconductors for 6G, in the Netherlands considerable financial support under the IPCEI scheme went to a consortium of which one of the partners, Ampleon, turned out have a Chinese owner. It was subsequently felt necessary to wall-off the participation of Ampleon.

automotive seek to express their resilience requirements to upstream supply chains including semiconductors (Masters & Edgecliffe-Johnson, 2021).

**Global governance**

In the past, globally broad semiconductor governance was mostly based in industrial organisations such as the World Semiconductor Council (WSC) and SEMI (Semiconductor Equipment and Materials International). These, being of a global nature, may be less suited to address the geopolitically contentious aspects, notably when resilience gets close to economic security or strategic autonomy. WSC indeed does not address resilience. SEMI – which has a global membership and presence - does address resilience in its supply chain management workstream and does mention geopolitical conflicts as a risk. However, it focuses on pre-competitive work. Moreover, the supply chain management workstream, as the cybersecurity workstream, appears to have no Chinese participation. The regional industry organisations, such as SIA (US) and ESIA (Europe), are highly active on resilience but also promote national interests that may bring them in competition or even in conflict with other national organisations.

International private-public or public governance links to work across sectors on resilience-related issues (see section **Error! Reference source not found.**). New forms of cooperation, initiated by governments, are being put in place such as CHIP-4 (Kaur, 2023; Wu & Wu, 2022). and the EU-US trans-Atlantic Trade and Technology Council (TTC). In addition, bilateral agreements are numerous. China is less into pursuing international partnerships in semiconductors but rather pursues increasing one-sided foreign dependencies (Antonia Hmaidi, 2024).

The case of semiconductors suggests a full range of areas that could be considered for global cooperation: monitoring, supply chain data, standards, and even supply crisis management. The least sensitive may be standardisation. However, even in that area governments want to be strongly involved such as for information standards to perform supply chain monitoring (cf. work in TTC). The important domain of cybersecurity standards is obviously sensitive in itself (cf. SEMI). Industry may wish to keep governments at bay, as these standards can strongly impact design and production and indeed, international business relations throughout their supply chains. Yet, given the link to national security, several government departments with strong capabilities pursue strong involvement (e.g., BSI, ANSSI, NIST resp. in Germany, France, USA). Even standardisation, then, is increasingly a hard nut to crack for truly global cooperation.

Yet, companies do push back: they express concern about government involvement as they see a risk for global fragmentation and obstacles to trade. They oppose mandating country-unique standards and rather want governments to commit to using industry standards. As ESIA & SIA (2022) states: “The semiconductor industry is to a large degree based on industry standards. Industry standards are developed by private organisations. Such organisations typically adhere to respected practices regarding their openness and rules of procedure. There can be advantages in an industry standard approach over a (formal) international standards approach, specifically in fields requiring flexibility and adaptation to changing requirements in the industry. Some examples are JEDEC, SAE, IEEE, and AEC. The EU-U.S. cooperation should safeguard the position and nature of industry standards as part of the collaborative effort.”

The assessment of the effectiveness of policies and strategies for resilience of this digital supply chain and what this has as a consequence for global or international governance is deferred to Chapter **Error! Reference source not found.**.

# 4. Case: Critical Raw Materials

**Chapter Summary**

Critical raw materials (CRM) supply chains are generally linear and much less complex than for instance semiconductors. Public policy for CRM supply chain resilience mobilises and integrates a complete set of policy instruments. Global/international governance for critical raw materials resilience involves a wide range of countries.

Critical raw materials is an instructive case as it shows integrated and an international-by-design EU resilience policy. Moreover, though it is not a digital supply chain, it is an input to downstream digital and, importantly, to 'green economy' supply chains. The EU is relatively resource-poor and has, today, little mining and refining capacity and therefore hugely dependent on third countries for critical raw materials.

## 4.1 Description

Critical raw materials are materials of high economic importance and high supply risks (European Commission, 2023c). Supply risks come mainly from concentration of supply in a few countries. The EC has identified 35 critical raw materials, as given in Figure 10. The supply risk is considered critical if it is above 1.

| | | | | | |
|---|---|---|---|---|---|
| Gallium (4.8) | Bismuth (1.9) | Tungsten (1.2) | LREE (rest) (3.5) | Beryllium (1.8) | Aluminium (1.2) |
| Magnesium (4.1) | Germanium (1.8) | Manganese (1.2) | Phosphorus (3.3) | Arsenic (1.6) | Helium (1.2) |
| REE (magnets) (4.0) | Natural graphite (1.8) | Nickel (.5) | Strontium (2.6) | Feldspar (1.5) | Fluorspar (1.1) |
| Boron (3.8) | Cobalt (1.7) | Copper (.1) | Scandium (2.4) | Hafnium (1.5) | Phosphate rock (1.0) |
| PGM (2.7) | Titanium metal (1.6) | HREE (rest) (5.3) | Vanadium (2.3) | Baryte (1.3) | |
| Lithium (1.9) | Silicon metal (1.4) | Niobium (4.4) | Antimony (1.8) | Tantalum (1.3) | |

*Figure 10 Critical raw materials with supply risk (source: JRC(2023))*

Critical raw materials supply chains are largely linear, running from miners (extraction) to processing to component assemblers to larger system assemblers to manufacturers who integrate these in their products. Buyers then use the products, which may get collected after use and possibly recycled. Market-makers, aggregators, and centralised commodity exchanges also play a significant role as do critical raw material markets/trading platforms.

Critical raw materials and their upstream processing deliver an intermediate product which is input to a potentially much more complex industrial ecosystem, such as semiconductors, or into a relatively simply one such as solar photovoltaics, see Figure 11. There are many digital products that depend on these critical materials as analysed by the JRC and reproduced from Carrara et al. (2023). Given the supply chain linearity (i.e. large dependency of downstream buyers on upstream suppliers), any of these are potential concentration points or bottlenecks that can be weaponised.

Limited technological innovation, large, fixed investment, and long-running exploitation contracts mean that critical raw material networks are relatively static.

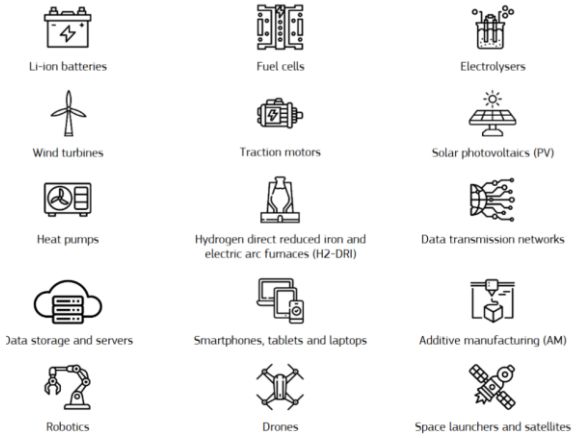



*Figure 11 Digital products depending on critical raw materials (JRC - Carrara et al (20223))*

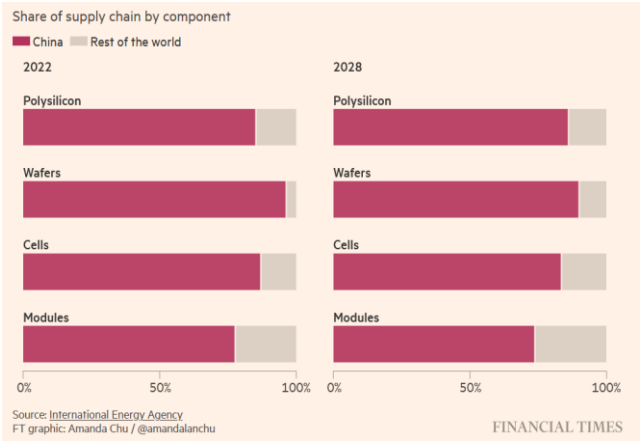



*Figure 12 Share of supply in the photovoltaic supply chain and final product (source: FT/IAE, 203/2022)*

## 4.2 Public Policies, Company Strategies

**Governmental policies:**

1. **EU**: the European Commission has, for several years, been worried about foreign dependencies given the role of critical raw materials for resilient supply chains in general and has been stepping up CRM initiatives. These are a combination of resilience, economic security[12], industrial policy, and international cooperation (European Commission, 2024b). This means that EU CRM policy is a leading example of integrated policy. However, demand side linkages – for instance to the automotive sector – are not fully addressed. The main policy is the 2023 Critical Raw Materials Strategy European Commission, 2023a) and Critical Raw Materials Act, a Regulation on secure and sustainable supply of critical raw materials.[13] The policy includes:

    a. Monitoring and Raw Material System Analysis to understand the supply chains and resilience risks. This started already in 2015. It includes a list of critical and strategic raw materials.

    b. Strategic investment projects with favourable permitting such as for mining.

    c. Coordinated strategic stockpiling and joint purchasing by the EC at the request of two or more Member States[14].

[12] For the relationship between resilience and economic security see Figure 1 and related text above.
[13] (Regulation (EU) 2024/1252 of the European Parliament and of the Council of 11 April 2024 Establishing a Framework for Ensuring a Secure and Sustainable Supply of Critical Raw Materials and Amending Regulations (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1724 and (EU) 2019/1020Text with EEA Relevance., 2024). See also (Council of the European Union, 2024)
[14] Joint purchasing may be much more difficult for CRMs than for vaccines or gas, and the experience should be carefully monitored to avoid undue optimism, see (Hancock & Wilson, 2024).

d. R&D and industrial cooperation. This includes R&D financing under Horizon Europe including for recycling and an Advanced Materials initiative (European Commission, 2024e). It also includes the European Raw Materials Alliance (ERMA), set up in 2020, a mostly industrial alliance with wide participation from Europe, Australia, Brazil, Chile, Cameroon, South Africa, India, Türkiye, Canada, and the USA. Not involved are China, Iran, and Russia and Congo (not yet). This also includes standardisation on a broad range of topic (exploration, extraction, refining and recycling) (European Commission, 2024b) as well as skills development.

e. Trade and international intergovernmental (multilateral) cooperation which includes trade facilitation through trade agreements and export credits, and possibly invoking WTO compliance but also possibly trade defence; as well as the 2022 Minerals Security Partnership of likeminded resource-seeking countries (initiated by the US). The European Commission also announced the intention to set up international collaboration in a Critical Raw Materials Club. This would have a membership of both supply-side resource-rich countries and demand-side resource-consuming countries. It would provide security of supply and allow supply-side countries to move up the value chain.[15] This Club as well as (presumably related) Global Gateway projects should be win-win by also paying particular attention to local value addition. The CRM Club proposal has been absorbed in the Minerals Security Partnership Forum (MSP Forum) which is a joint undertaking of the EU and the US.[16] Further bilateral agreements are Strategic Raw Materials Partnerships with Australia, Canada, Ukraine, Kazakhstan, Namibia, Argentina, Chile, the Democratic Republic of Congo, Zambia, and Greenland (European Commission, 2024d), (Platform Africa, 2023).

f. EU critical raw materials policy interplays with environmental, social, and human rights policies.

2. **EU Member States**: several EU countries have national policies in the area of CRM. An example is France, which amongst others has an *Observatoire français des ressources minérales pour les filières industrielles* (OFREMI), set up in 2022 and a private-public investment vehicle, to the amount of 2B€ (Mathieu Duchâtel, 2024). Other examples are the substantial investments in mining in Sweden and Germany.

3. **US**: the US approach is also instructive. The US Government has taken forceful initiatives such as the 2022 Inflation Reduction Act (IRA), which includes tax incentives designed to foster critical materials supply chains within the US. The US has also imposed tariffs such as on graphite anodes from China to stimulate its domestic battery industry and its suppliers – despite China accounting for 97% of global anode output (Davies, 2024). The US-Japan critical

[15] "The EU should […] establish a Critical Raw Materials Club […] to promote the secure and sustainable supply of CRMs. The EU should join partners in promoting the reliable, commercially based, transparent and environmentally friendly supply of CRMs. In particular, the CRM Club should foster sustainable investment in producing countries and allowing them to move up the value chain.", see (European Commission, 2023a).

[16] See European Commission Press Release at https://ec.europa.eu/commission/presscorner/detail/fen/ip_24_1807.

minerals agreement has commitments on non-imposition of export duties, cooperation on trade defence, FDI, circularity, but also labour rights (USTR, 2023a).

Lobby groups such as ITIF are making the strong case that the USA is losing leadership in several key technologies (telecommunications equipment, semiconductors, television, solar panels, and chemicals) and stress that the resilience and security of critical materials supply that underpin all of these is essential (ITIF, 2021). They argue for strong R&D and IP protection and limited or no constraints on profit-making. However, others argue that investing in basic materials and technologies will pull resources away from the advanced work which is essential for long-term competitiveness and national security (the so-called resource curse argument).

4. **China**: an extensive description of China's CRM policy can be found in John Seaman, Florian Vidal and Raphaël Danino-Perraud (2024). China's most recent official policy on 24 strategic minerals is the National Mineral Resources Plan, 2016–2020. At the time, in 2016, the plan prioritised economic importance over supply risks. Generally, China pursues a strategy of domination. This includes controls on production and export of 17 rare earth minerals and beyond geoeconomic dominance. China has also weaponised these in the battle for advanced semiconductors (the export controls on germanium and gallium in response to US export restrictions on advanced semiconductor manufacturing equipment). Recently China issued a regulation which specifies that rare earth minerals belong to the state. The stated aim of the regulation is to "ensure national resource security and industrial security". The rules apply to the entire supply chain, from mining to smelting and separation, processing, distribution and export (Shunsuke Tabeta, 2024).

5. **Others**: Australia, Chile, Canada, and others provide billions in governmental support for new mining.

6. **International cooperation**: the Hiroshima G7 meeting in 2023 asked the International Energy Agency (IEA) to make recommendations on options how to diversify the supplies of critical minerals (the context being clean energy transitions) which include co-ordination across supply chains to determine risks, strategic partnerships both within G7 and beyond, investment facilitation in emerging market and developing economies, an information platform, and resource efficiency (IEA, 2023). IEA also produces an annual Global Critical Minerals Outlook. The G20, having many of the key countries for critical minerals as members, has agreed under Indian Presidency to voluntary high-level principles for critical minerals supply.

**Company strategies:**

Company strategies are less documented. Generally, public policy is implemented through companies in which case corporate strategies are driven by public policy requirements. Some documented strategies for CRM resilience are:

1. *Vertical integration or collaboration*: upstream or downstream integration or shareholding such as buyers acquiring stakes in with upstream mining companies and refiners or downstream recyclers. An example is the strategy that Northvolt pursues as a battery

manufacturer (Northvolt, 2023). Car manufacturers cooperate with battery recyclers to create a closed loop system.

2. *Stockpiling*: buyers create a strategic stockpile. This can potentially go relatively fast but is difficult if there is a very high degree of upstream concentration. Reports are scarce and anecdotal.

3. *Long-term contracts*: buyers can establish long-running contracts with upstream suppliers (Northvolt, 2023). Tesla buys directly from nine miners, e.g., cobalt, and states to also require compliance with environmental and social standards.

4. *New CRM activities as a business*: such as opening new rare earth mines; even if, domestically, permits and commencement of sizable exploration can take 10-15 years, environmental opposition may be significant and, in foreign locations, regimes may be problematic (Foroohar, 2023).

5. *Diversification*: Downstream companies that use the raw materials as inputs, such as battery manufacturers, can diversify suppliers (Davies, 2024). This also eases the threat of China's curbs on germanium and gallium exports.

6. *R&D*: for instance, into alternative materials or into the reduced use or recycling of materials. Umicore is developing technologies based on "thin film" germanium to reduce use of the material. The EIT Raw Materials, an EU Horizon Europe-funded R&I platform lists tens success stories.

7. *Import substitution (setting up domestic businesses)*: in the US companies are being set up to produce anodes with as input US-supplied precursor material of graphite (Davies, 2024). European aluminium producers such as Mytilineos Energy & Metals have been asked to explore gallium production as a byproduct. Nyrstar may build a $150 million germanium and gallium recovery and processing facility at its zinc smelter in Tennessee.

8. *Cooperation*: companies can cooperate if this is not collusive to better control suppliers, pick up early signals of shortages, jointly invest, and possibly assist each other in case of shocks. The ERMA platform for rare earth magnets and motors, batteries, and fuel cells can in principle play such a role, but the current status is not clear.

9. *Consumption efficiency and recycling*: Companies may also reduce material consumption by increasing efficiency and recovery and minimizing waste. Some of this may go fast.[17]

10. *Monitoring and planning*: AI and blockchain may be deployed to help optimizing and tracking the supply chain such as for supply planning, although this appears to be still in pilot stage.

## 4.3 Observations

**Structure and dynamics, policies and strategies**

[17] The 80-20 rule, or Pareto Principle, is widely applicable in production and manufacturing processes to seek efficiencies (see general manufacturing/production quality management literature).

CRM supply chains pose a challenge for EU and US policy. This is not so much because of their complexity as they are – relatively – straightforward and mostly linear. Rather this is because, firstly, for a large number of materials, mining and processing is to a large extent controlled by foreign companies and countries. Secondly, finding alternatives generally takes years whereas the need for resilience is more acute. Thirdly, building alternatives is generally costly, requiring investments of many billions while capital is not readily available from public funds nor from private capital markets as these hesitate because of geopolitical and demand uncertainties.

Still, the nature of CRM supply chains makes it easier to systematically build up comprehensive and enduring policy. Moreover, by linking the supply resilience policy with a buy-side industrial policy (e.g., solar panels, electrical vehicles) this may become a self-reinforcing system, where the paybacks in the long run make such policy more affordable and acceptable. This reduces investor uncertainty, puts in place structural change, and gives more resilience to respond to shocks. Moreover, by creating a win-win with resource-rich countries this creates geopolitical closeness that likely also pays off in other areas.

Here lessons can be learned from China's international strategy which has been remarkably successful – viz. China's control of many CRM supply chains. China has built up an extraordinarily strong, perhaps unassailable position in a range of critical raw materials. For instance, it holds 91% of the supply of magnesium, 85% of neodymium, and 100% of heavy rare earths. Moreover, China often has significant shareholding in mines in other countries such as Congo.

China also combines the intention to achieve dominance in the supply side with the intention for dominance or a strong position at the demand side. The EC cites photovoltaics as an example of this phenomenon. China's share in all the manufacturing stages of solar panels (such as polysilicon, ingots, wafers, cells and modules) exceeded 80% in 2022 and this is expected to last for years (Chu, 2024; International Energy Agency, 2022), see Figure 12. The EU solar panel industry states that it is, as a consequence, in mortal danger.

Yet, it is still possible for the Western liberal democracies and likeminded partners (such as US, EU, Japan, S. Korea, Taiwan, and others) to pursue such a policy. China has not locked in everything. Firstly, there are alternative suppliers, domestic ones or from likeminded countries such as Canada or Australia or 'neutral' countries such as Indonesia, Congo, etc. Secondly, substitution by new materials may be possible in certain cases. Thirdly, a degree of demand reduction is feasible by recycling and perhaps also by technological innovation, though the latter can take a long time and may run into trade-offs of increased resilience versus reduced product performance.[18] Fourthly, the West can also take trade counter measures. The EC has opened an investigation under the Foreign Subsidies Regulation in the solar photovoltaic sector to find out about the potentially market distortive role of Chinese state subsidies (European Commission, 2024g). More generally, the EC has extensively documented state-induced distortions of competition and trade in a wide range of sectors (European Commission, 2024h) in order to prepare for trade defence measures.

All these actions change the structure and dynamics of the supply chains by creating more choice, less tight coupling or even decoupling, etc. and thereby resilience risks are reduced. The goals are clear in

[18] For a telling example in replacing critical magnetic minerals for electrical vehicle motors, see (IEEE Spectrum, 2024).

EU policy such as that, by 2030, EU extraction, processing, and recycling must cover at least respectively 10%, 40%, and 15%, of EU annual consumption. However, these targets, which are all far below 100%, show that significant foreign dependency will remain, and it is reasonable to expect that this implies a significant continued dependence on China. Moreover, it remains to be seen whether the goals are attainable and sufficient. There are several reasons to question this as will be discussed in chapter **Error! Reference source not found.**. In addition, timeliness matters, viz. the case of Northvolt the European battery manufacturer who experienced supply shocks due to the war against Ukraine, which necessitates a response on a much shorter timescale than the ten years to 2030 (the years quoted in EU policy).

The situation of dependencies in critical raw materials supply chains illustrate past failure or absence of geopolitically aware industrial policy. This holds for both the EU and the USA. The USA seeks to repair this with massive instruments such as the IRA but remains dependent on China's CRM processing knowledge, for now.

One would think that EU Member State policies would strategically seek to exclude China as regards international collaboration on CRMs, if alternative sourcing is possible (such as for batteries), but reality shows a more complex interplay of strategic and tactical considerations. For instance, there are several recent instances of French companies teaming up with Chinese counterparts. Moreover, some of these French companies can also receive state aid under the IPCEI scheme (i.c., for the IPCEI for batteries). Mathieu Duchâtel (2024) concludes that "This means that even if France's investment in its battery industry reflects a desire to diversify its partnerships and a commitment to industrial localization and employment, for the time being, it is tantamount to increasing France's dependence on China for critical materials essential to the energy transition."

However, China has also dependencies, such as for copper, iron ore, as well as for several unprocessed rare earths (John Seaman, Florian Vidal and Raphaël Danino-Perraud, 2024). Consequently, China is highly active in 'mining diplomacy' to achieve greater control and reduce such dependencies.

A critical issue that comes up over and over again, and more so in CRM than in other areas, is that long timescales are to be taken into account, 10-15 years, to (re-)build critical materials supply chains. Building and sustaining resilience is a marathon. In principle, the European Commission may have an edge in this respect, being used to pursue long-running policies.[19] China has a similar advantage. Academics have argued that the US still needs to adapt its governmental machinery in this respect towards a 'new economic security state' (Farrell & Newman, 2023b).

[19] There are after all some advantages to a 'technocratic bureaucracy'...

**Global or International governance**

Raw materials supply chains have very much been left to the market and industry, to the extent that international governance hardly existed until recently. However, CRMs have become ever more geopoliticised.[20] Given the current geopolitical climate, recent international governance tends to be organised around camps of likeminded partners or is limited to bilateral agreements. Examples are agreements of the EU with third countries and "coordination on the availability of critical raw materials crucial for semiconductor production" in the US-EU TTC. The US, China and others are likewise mostly pursuing country-to-country approaches (despite G20 and G7).

A question is then, however, whether the EU would be wise and able to internationalise its approach. An example is the proposal for a Critical Raw Materials Club which is building on the EU's bilateral partnerships and is an integral part of the EU's raw materials resilience and economic security policy. The benefits could be to fill a gap left by rising geopolitical adversity, raise credibility with neutral countries, and develop an agenda in areas of common and global interest such as critical raw materials and climate change.

In that respect, more than other cases, the critical materials case illustrates that international governance must be:

- Win-win
- Sustained over a very long time
- Consistent in respecting environmental and human rights principles
- Robust against political changes in a participating country.

The international relations theories of neofunctionalism and trans-governmentalism tell us that such approaches can evolve from public administrations and experts that have established informal cooperation, share technical and professional similarities, are involved in governmental networks, and progress incrementally. In a sense they are emerging from collaboration of expert and technocratic elites. These elites, however, must also pay attention to democratic accountability.

This could lead to combined government-based, industry-based, and NGO-based international governance. For the industry participants this can readily be mapped on supply chain structure and dynamics. Parties such as mining companies, processors, and financiers will likely be in this for the long run. They expect stable relations and contracts. Many will have an understanding about working with governments.

Finally, one may wonder what role the WTO should play. For instance, can export controls in this area be challenged by international arbitration in the WTO? However, where the bazooka of national security is used, as is currently the case, such arbitration is a non-starter. Moreover, the WTO has been weakened over recent years, a position that may deteriorate even further should Trump win re-election.

[20] Ironic is that the EU was founded on for common management of two raw materials: steel and coal… and this to avoid war…

# 5. Case: Software Supply Chains

**Chapter Summary**

Software supply chains are part of any other digital supply chain and therefore one of the most important to analyse. While there are important public policies for software supply chain resilience, much work on resilience (i.e. on cybersecurity) is driven by concentrated corporate presence and by open-source community with its own global/international governance.

A software supply chain can be defined as a network of actors, processes, and software components for delivering software products to end-users.[21] We focus here on the resilience of software supply chains, or ICT security (cybersecurity) of software supply chains. We pay special attention to open-source software supply chains. Open-source software is software released under a license that allows users to use, study, change, and distribute the source code for any purpose.[22] Software is present in every other digital supply chain. Therefore, software supply chains can also be seen as a sub-supply chain of other digital supply chains.

## 5.1 What are Software Supply Chains?

As software is purely digital, software supply chains are quite different from physical goods supply chains. Software can be fully online and remotely distributed, upgraded, and altered. Software can be integrated into other software without physical intervention (except a programmer or software engineer at a keyboard). Software can be altered during its transmission, as well as during its development and deployment, which is a manifestation of cybersecurity.[23] Software supply chains rely on digital communications which can be interrupted, intercepted, or altered by cyber intrusion (e.g., man in the middle attack) as well as physical incidents (cutting an undersea cable, tapping a phone line).

Software is being distributed, upgraded, maintained, and supported from originator to end-user such as a company, public administration, or citizen in several ways:

1. Direct distribution from software producer to user
2. Indirect distribution:
    a. from software producer via a software hub to integrator or larger provider

[21] Definition based on https://en.wikipedia.org/wiki/Software_supply_chain.
[22] There is a range of open-source licensing schemes, see https://en.wikipedia.org/wiki/The_Open_Source_Definition.
[23] Cybersecurity challenges can be broken down into the C-I-A of confidentiality, integrity, and availability. The example mentioned here is an integrity breach.

b. from software producer to an integrator[24] or a larger software/cloud provider (Figure 13[25]).

An example of (1) is the updates we all receive on our laptops or smartphones, such as directly from Microsoft, Apple, or Samsung and others. In these supply chains there are a few companies ('big tech') that are extremely large, next to many smaller ones. An example of (2)(a) is GitHub, a software collaboration and repository hub. Many cases fit in (2)(b). The original software producer as well as

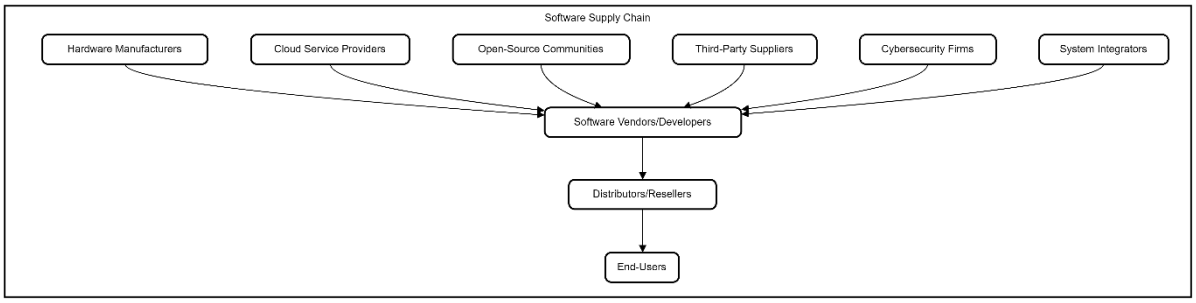



*Figure 13 Example software Supply Chain*

downstream integrators may use open-source components and likely are doing so. Open-source software producers range from commercial software companies to non-commercial individuals who do software development in their spare time without formal quality control process.

Increasingly, open source has been embraced, at least partially, by large software companies such as IBM/RedHat, Canonical/Ubuntu, Microsoft, and Google. Because of the significant voluntary and/or not-for-profit activities of open-source software (OSS), often involving driven but unpaid individuals, it is very delicate to intervene as government, let alone as regulator. It would be easy to destroy motivation by imposing bureaucracy on self-motivated and highly capable individuals. It is even delicate to introduce financial incentives, as in these common goods market the supply-price (payment) curve may partially be inverted, meaning that financially rewarding works – such as for better security - reduces motivation until it is raised to more normal hourly wage levels for software development (Le Grand, 2003).

This supply chain structure can be vulnerable to cybersecurity incidents and attacks. For instance, in the case of supply chain along the direct route (point (1) above) an infamous incident was the SolarWinds intrusion in 2020. The eponymous company performed remote updates in a trusted direct relationship of vendor and customer. SolarWinds was the target of state-sponsored intrusion thereby widely opening the door to its customers who were the ultimate target.

In supply chains taking the shape of (2)(a), a recent example is the introduction of the xz backdoor in much used open-source software in a sophisticated human stealth operation (Claburn, 2024). This attack was, probably by accident, stopped in its tracks but it could have been devastating. An older example is the 2014 HeartBleed bug, which got widely spread. The software originated from one single

[24] An integrator can be an IT services and consultancy company but in the situations here it can also be a hardware vendor integrating third-party and own software such as a provider of routers.
[25] Diagram generated with Claude.ai, Mermaid and Draw.io.

programmer. Updating servers across the internet took many months during which the vulnerability persisted.

In supply chain (2)(b), an example of a vulnerability is Mirai; a DDOS attack that mobilised thousands of routers and other internet-connected devices that all had the same backdoor vulnerability, with the Mirai software spreading from router to router. In cybersecurity terms, these examples show breaches of confidentiality, integrity, and availability. They all deteriorate software supply chain resilience.

## 5.2 Public Policies, Company Strategies

**Governmental policies**

1. **EU**: resilience of software supply chains is not subject of one single specific policy as such but rather addressed indirectly through several policies such as the Network and Information Security (NIS) Directive for cybersecurity of critical service and infrastructure providers or the Digital Operational Resilience Act (DORA) for cybersecurity in the finance/banking sector. In addition, there is the important case of products (hardware, software) with digital elements and direct or indirect logical or physical data connection to a device or network. This is the subject of the Cyber Resilience Act (CRA) which imposes internal market-based requirements for design, development and production, vulnerability handling, and market surveillance while the product is in use. Where such products are to be certified the certification scheme and its organisation such as inspection is arranged for under the Cybersecurity Act (CSA). The CSA also specifies cybersecurity certification based on risk-based assurance, addresses secure development lifecycle, and foresees the composability of certifications – the latter being of specific importance for software supply chains where several certifications must be put on top of each other or be sequences.

   As is often the case with internal market legislation, supervision is by market surveillance authorities at Member State level. In case of non-compliance, these authorities can go as far as removing the product from the market and/or imposing fines that can be as large as 2.5% of worldwide turnover. The CRA has the potential to be quite strict. Depending on how critical products are, they must have third-party assessment and EU certification. Depending on how rigorous supervision is fines can be as substantial as for serious GDPR personal data breaches.

   It is important to understand the (limited) extent of CRA obligations as this affects software supply chain resilience. In particular, as regards the relevance of the CRA for open source, an excellent explanation is provided by Bert Hubert (2023), summarised as follows: the CRA is only applicable to products with digital elements (read: open-source software) where related to a commercial activity. The law makes it explicit that it “does not apply to natural or legal persons who contribute source code to free and open-source products that are not under their responsibility.” From a resilience point of view, this means that vulnerabilities may be present in OSS that is maintained by, say, a single volunteer. Also, commercial open-source software (OSS) providers are exempted from obligations except when the original manufacturer monetises it (which may be possible depending on the licensing scheme). Even in this case, package OSS providers, for instance of a Linux distribution, are exempt.

However, the commercial users of such OSS do have cybersecurity obligations. Namely, "When integrating components sourced from third parties […] manufacturers should exercise due diligence with regard to those components, including free and open-source software components that have not been made available on the market." In addition, security attestation, also by such integrators downstream in the supply chain ('manufacturers') is being promoted. Moreover, these integrators should also report vulnerabilities.

In the OSS supply chain, there are also 'OSS stewards' who provide sustained support for the viability of OSS. They could, for instance, do systematic software inspection and vetting. They are to be subject to a light-touch and tailor-made regulator regime, for instance voluntary reporting of vulnerabilities.

Altogether then, the CRA will improve resilience for proprietary software but puts the onus of OSS resilience largely on the manufacturers or integrators. The CRA encourages an enhanced governance in the supply chain, with OSS stewards and clearer, common approaches to cybersecurity. Potentially, this opens avenues for international governance, as the EU's CRA rules could be taken up by international OSS foundations as well as by commercial undertakings that wish to have one set of rules for global markets and would take the CRA rules as a reference given the large EU market – this is what is called the 'Brussels Effect' (Bradford, 2020).

The relevant EU laws (CRA, CSA, NIS2, DORA) also make reference to European standardisation. The EC's 2024 standardisation plan promises work on (i) security specifications relating to the properties of products with digital elements and vulnerability handling specifications (ii) methodologies concerning assurance levels relating to products with digital elements as referred to above; and (iii) evaluation methodologies for evaluating cybersecurity risks associated with products with digital elements (European Commission, 2024c).

Council conclusions also address ICT supply chain security, (Council of the European Union, 2022), as related to NIS2, CER, CRA, and Cyber Solidarity Act for Managed Security Service Providers, as well as for FDI screening, and the economic security risk assessment. They also invite "the Commission to develop methodological guidelines by the third quarter of 2023 in order to encourage the contracting authorities to put appropriate focus on the cybersecurity practices of tenderers and their subcontractors, and to assess and, if needed, make proposals to revise or complement relevant public procurement legislation."

The intention of the Council is to link to global governance, recognizing "the need for close cooperation within the EU and internationally in sharing knowledge and expertise among relevant stakeholders". Indeed, the Council recommends EU-level led digital partnerships, cyber dialogues, UN norms processes and where appropriate, free-trade agreements, TTC, Global Gateway for the promotion of risk-based evaluations of ICT product suppliers and ICT services providers, the use of trustworthy suppliers and for the employment of a secure and innovative digital ecosystem based on open, interoperable and transparent standards. The EU and the US are indeed cooperating in the TTC on ICT supply chain security (see below).

2. **USA**: the US, as the largest software producer and one of the largest software markets in the world, and very concerned about economic and national security, has a number of initiatives for software supply chain security. Following the Executive Order (EO) on Improving the Nation's Cybersecurity of 2021 (Executive Office of the President, 2021), triggered by the 2020 SolarWinds cyber-attack, the US standardisation agency NIST issued in 2022 guidance on Software Security in Supply Chains (NIST, 2022). This informs the acquisition, use, and maintenance of third-party software and services for agencies' information technology, Cybersecurity Supply Chain Risk Management, Program Management Office, acquisition/procurement, and other functions. The EO is therefore applicable to US agencies, in the expectation that these requirements will 'bubble up' into the upstream software supply chain and thereby raise cybersecurity with the software suppliers. From that time onward the US also started to coordinate with the EU in these matters.

   However, the EO was apparently not felt to be enough. Concerns about open-source software led the US Cybersecurity and Infrastructure Security Agency (CISA) to issue in 2023 an Open Source Software Security Roadmap based on voluntary efforts (Jen Easterly, 2024), (CISA, 2024b). This addresses secure package management, provenance, software bill of materials (SBOM), multi-factor authentication (i.e., secure distribution of software), with collaboration of major package manager initiatives (e.g., those maintaining the Rust and Python programming languages); information sharing of OSS developers and government; and tabletop exercises. In these matters, CISA coordinates with the US Office of the National Cyber Director (ONCD)'s Open-Source Software Security Initiative which promotes open-source software security and the adoption of memory-safe programming languages. The US OSS initiatives are remarkable as a first example of how to tackle this important supply of software where, as argued, it is delicate to intervene.

3. **China**: as (MERICS, 2021) explains, opensource is an important industrial policy tool in its push for strategic autonomy. An example is that Huawei appears to have been recovering from the ban on licensing Google's Android by a.o. by making HarmonyOS open source and thereby enabling a viable software ecosystem to develop (The Economist, 2024b). Two out of five GitHub accounts are Chinese, although in terms of actual open-source contributions this is 1 in 10 (Figure 14). Chinese companies participate in and/or sponsor important open-source foundations such as Apache. China also open-sources top-ranking generative AI.

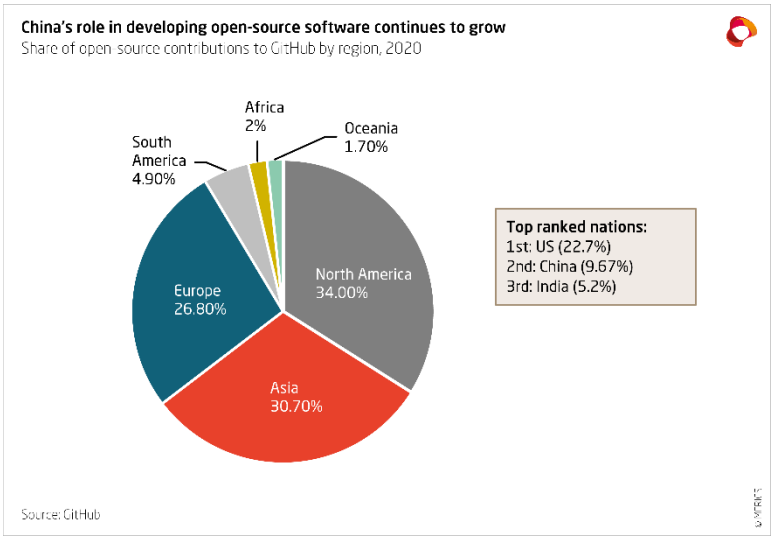



*Figure 14 GitHub open-source contributors by region*

Open-source companies are shored up by private risk capital from China. Nevertheless, concerns about security risks are also entering the world of open source, creating a pushback to involvement of Chinese contributors and universities. Often reference is made to the obligation in the National Intelligence Law of 2017 (People's Republic of China, 2017) which compels any Chinese subject to conduct espionage on behalf of the government (article 7 "All organizations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with law, and shall protect national intelligence work secrets they are aware of."). There are reports that China is censoring open-source developers (Zeyi Yang, 2022). Moreover, open source can be used for surveillance and suppressive purposes that go against the values of the original software developers and against the interests of their democratic governments. Geopolitical fragmentation of the open-source world is already starting to become a fact, for instance Gitee is a state-backed Chinese competitor to GitHub. Concerns are that code review in China is no longer independent and will be influenced by political motives – which could include weakening resilience.

4. International initiatives:

    a. The US and EU have been working together since 2021 on cybersecurity in software supply chains. The various US agencies such as NIST, ONCD and CISA have ENISA and the EC (DG CONNECT) as counterparts. One topic has been SBOM, although a harmonised scheme still remains to be published. In 2024 the scope was extended to also include connected products (IoT, consumer products) in the form of a Joint CyberSafe Products Action Plan (European Commission & U.S. National Security Agency, 2024). The overall framing is either bilateral cybersecurity cooperation or the TTC. This is clearly related to the CRA and a similar security labelling of connected devices, by the FCC's Cyber Trustmark, a voluntary scheme (FCC, 2023).

    b. The world of open source and open standards has a very rich set of international and often open initiatives, from IETF for internet specifications and de facto standards, to the Open Group promoting open standards in software, to open-source foundations around specific products such as the Linux Foundation (operating system) or Apache Foundation (webserver) to a very large international informal community of committed open-source developers, that have their own informal but powerful leaders such as Linus Torvalds.

**Company strategies**

Several software supply chain incidents such as SolarWinds, xz, and HeartBleed, show how companies react. Usually, for proprietary software the first port to call is in-house patching (bug fixing) and distributing updates to customers. Many of the company strategies for resilience as found in other supply chains such as diversification of suppliers or relocation are not or hardly known in software supply chains[26]. However, there are other fairly unique approaches in resilience of software supply chains:

[26] Quantity of supply does not play a role for software as reproduction is zero-cost. Place of supply until recently did not play much of a role as there are few delivery restrictions. Supplier quality could be an issue and even more so in the future if certification kicks in. This would especially hold for critical products. However, if these

1. *Extending the supply chain*: a more systematic action has been taken by large IT companies to incentivise finding bugs (bug bounty programmes). This is an interesting extension of the supply chain, bringing in independent 'inspectors' or as they are called in software 'white hackers'. This, of course, works with the lowest barriers when it concerns freely available open-source software, but it is also applied for proprietary software. Other supply chains might learn from this.

2. *Cooperation*: in software supply chains – or more generally in cybersecurity - extensive collaboration and joint information management is quite common. Not only in OSS but also in registering vulnerabilities in the freely accessible Common Vulnerabilities and Exposures CVE system, maintained by the US Department of Homeland Security and the MITRE Corporation. Anti-virus companies, even if competitors, share bug information. Cooperation also happens to repair OSS bugs. For instance, many websites of national cybersecurity centres but also of foundations, and companies spread the word about the urgency and the method to fix the 2014 HeartBleed bug. Yet another form of cooperation is in industry standards: Tech Accord, a coalition of over 150 global technology companies committed to improving the security, stability, and resilience of cyberspace (but none from China) advises putting third-party risk management procedures in supplier contracts, standardizing risk management in procurement and security strategies, and checking through audits, diversification of supply chains with zero-trust policies, though much of this remains to be done (Martins, 2023).

3. *Partnering with suppliers*: ASML partners with its thousands of suppliers that are often relatively small to enhance through training their inhouse security programs.

4. *Technology for resilience*: several companies are providing solutions for secure distribution and updating of software using technologies like blockchain (De Filippi & Wright, 2020).

5. *Moving to open-source:* companies can decide to move their proprietary software into the open-source domain. The thinking is that this increases the number of providers of updates and bug-fixing. In practice, however, companies have little control over the open-source community. Incentive programs (bug bounties) can be thrown in. Some academic research suggests that they can be effective, at least initially, when bugs are still easily found (Maillart et al., 2017).

## 5.3 Observations

**Structure and dynamics, policies and strategies**

Software supply chains show that what matters for resilience, economic security, and strategic autonomy is whether 'key positions' in the supply chain can be 'critically affected' or not. For instance, it is not necessary for a foreign nation to own a specifically important software component supplier if it can infiltrate a supplier by cyber or physical means. The supplier does not need to be owned but

are also export-restricted, most buyers would not want to risk bypassing such export restrictions. Other constraints are lock-in by dominant suppliers and additional integration/interoperability/learning costs when switching suppliers. Legislation such as the EU's Digital Markets Act may reduce such constraints in the future. Software also needs maintenance and update. In theory, for open source it is easier to find alternative providers for maintenance and updates.

must be 'pwned' in the jargon in cyber-land.[27] This sharpens our understanding of intrusion or infiltration as a supply chain risk. Of course, it is less likely for purely physical supply chains to suffer intrusion, contrary to the purely digital supply chains. If it happens, it is rather the classical area of espionage (industrial, military). In any event, a very high level of cyber-protection of entities in the supply chain is necessary.

What is a key position in the software supply chain? It is the extent of downstream dependency on the provider in that key position, meaning, the criticality (for economic, societal, or democratic resilience) of the customers of the software. This criticality can be mitigated if there is the possibility to switch to alternative software providers, that is, avoiding that the provider constitutes a Single Point of Failure (SPOF). However, such diversification is not a strategy that is much pursued in software supply chains, as we have seen. The narrative, then, is: establish a Software Bill of Materials (SBOM); use the SBOM to identify software companies in the software supply chain and to establish whether these are a Single Point of Failure (SPOF) or an Essential Third Party Vendor (ETPV)[28]; also use the SBOM to identify actual or potential vulnerabilities in the software provided by that company using a methodology such as MITRE ATT&CK®; assess the severity of exploitation of a vulnerability in product or company using a methodology such as Common Vulnerability Scoring System (CVSS) and multiply that with the value of SPOF and of ETPV and assign that to the company-product combination as the Software Supply Chain Criticality (SSCC). This is shown in Figure 15.[29]

What does 'critically affected', mentioned above, mean? This can be assessed with actual or hypothetical assessment of the severity of a cyber incident or vulnerability. In the field of cyber the Traffic Light Protocol (TLP)[30] was created to indicate such severity. It is one of the elements designed to enable sharing of potentially sensitive information and more effective collaboration. In addition, MITRE ATT&CK® provides a globally accessible knowledge base with information on adversary tactics and techniques based on real-world observations.[31]

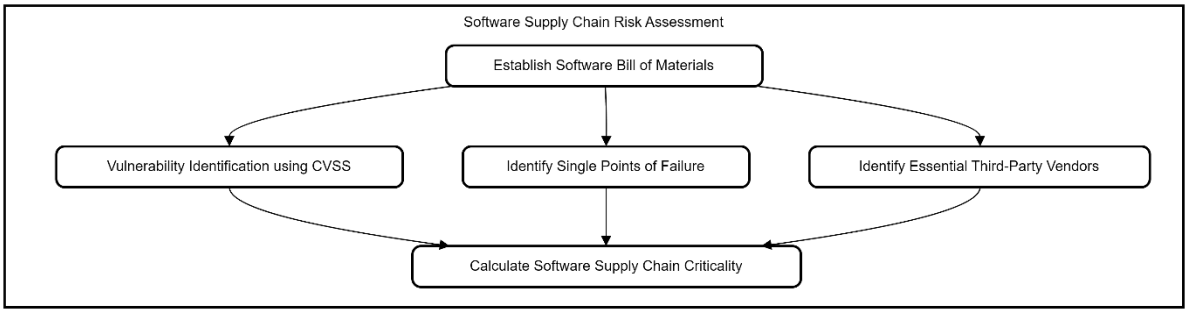



*Figure 15 Software Supply Chain Risk Assessment*

[27] Readers who want to know whether they themselves run the risk of infiltration due to exposure of their credentials (email, password, etc) can look up https://haveibeenpwned.com/.
[28] An ETPV can be defined as an external company or service provider that supplies products, services, or support that is critical or essential for an organization's operations, products, or services. The term used in DORA is critical ICT third-party service provider, while in NIS2 these are providers in a critical supply chain.
[29] Figure generated from narrative by Claude.ai, drawing with Mermaid and Draw.io.
[30] https://www.first.org/tlp/.
[31] https://attack.mitre.org/.

**Global or International governance**

In software supply chains we can then observe several global governance approaches such as:

- Proprietary:
    - Constellations of a big tech company with many affiliated developers and companies.
- Open source:
    - Global technical cooperation such as IETF, IANA for internet architecture and specifications.
    - International sharing of vulnerabilities, based on the CVE de facto standard.
    - Global cooperation of CERTs in FIRST, with joint work on standards such as TLP.
    - Software repositories such as GitHub.
    - Open-source software foundations.

The open-source approaches have weathered the test of time. They generally fit with a view in the coding community that sharing is a win-win and technical cooperation – including, importantly, on resilience and security – should not get fragmented due to geopolitical or corporate interests. Of course, this is an idealistic view. As noted, fragmentation is starting to happen, in the internet itself and in such governance of software supply chains.

However, global sharing and cooperation is still strong. New initiatives can benefit from this and build on it for global approaches, creating global common goods such as standards and best practices. An example could be to take to the global level bilateral cooperation such as of the EU and US in the TTC on Software Bill of Materials.

Such an approach for software might also be supported at UN level as it is fitting with the 2030 vision of global involvement in the digital world, the UN Global Digital Compact (GDC). The GDC is expected to "outline shared principles for an open, free and secure digital future for all" (UN, 2024). The GDC stresses common standards and data commons for the public good and considers open source a digital public good. It commits, for instance, to "Develop and decide on a set of safeguards for safe, inclusive, secure and responsible digital public infrastructure that can be adopted by and tailored to the specific needs of each society". The GDC in its current version does not yet, however, explicitly make commitments for resilience of software supply chains, not even for open-source ones, and could be enhanced in that respect. Likewise the Declaration for the Future of the Internet, if further internationalised, could support such an approach (EU and USA, 2023).

# 6. Case: Finance and Banking

**Chapter Summary**

Finance/banking is an important example of a sector that has both a long tradition in global/international governance and a high level of awareness about systemic risks. Addressing digital supply chain resilience can be an extension of both. However, combined finance/banking and cloud resilience is seen as a challenge.

We include finance and banking as it is illustrative in both existing and evolving governance for resilience. Indeed, legislation in this established field – DORA – has been accepted as a *lex specialis* in the EU's horizontal cybersecurity legislation, given the existing extensive governance and rules for resilience in the finance/banking sector.

The DORA regulation refers to 'digital operational resilience' meaning "the ability of a financial entity to build, assure and review its operational integrity from a technological perspective by ensuring, either directly or indirectly, through the use of services of ICT third-party providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity makes use of, and which support the continued provision of financial services and their quality."

## 6.1 Description

Resilience is a topic of extremely high priority in the financial and banking sector. The financial crisis of 2008 and several banking crises have brought this home. Resilience threats can come from various sources. Best known are bad financial practices, insufficient guarantees, and risky investments. These also highlight systemic risks, which is cascading damaging effects. Internationally, practices have developed especially since 2008 and also in recent years to manage and contain such risks. Psychological effects can also play a role, for instance, they can trigger a bank run or a stock market crash.

Over recent years, *cyber*-risks have become ever more important. Banking and finance are the fourth most-hit target of cyber-criminals. Focusing, then, on ICT, this sector started to realise early on that they were ever more dependent on an ICT supply chain. An illustration of suppliers to financial institutions and banks and their position as suppliers to customers is in Figure 16.

## 6.2 Public Policies, Company Strategies

**Governmental policies:**

1. **EU**: DORA is a specific EU cybersecurity Regulation for financial and banking services. It is extensive on the relationship to the entities in the ICT supply chain that are so-called critical third-party service providers. It specifies audits, threat-led penetration testing, and oversight of the supply chain of critical financial institutions in the EU. It still needs to be clarified which

suppliers will be marked as 'critical' and substantial work is still ongoing to specify Regulatory Technical Standards (Ilias Chantzos, 2024).

Special to the finance/banking sector is that extensive governance for oversight, banking controls, and risk management already exist in the EU. Cybersecurity supply chain risk management gets 'hooked into' these existing mechanisms. This is different from NIS where new oversight had to be set up. However, and especially relevant from the perspective of ICT supply chain resilience, DORA introduces a Lead Overseer of critical third-party service providers, which can be any of the three European Supervisory Authorities in the sector.[32] As DORA states, the Lead Overseer should "fully grasp the magnitude of interdependences, discover specific instances where a high degree of concentration of critical ICT third-party service providers in the Union is likely to put a strain on the Union financial system's stability and integrity and maintain a dialogue with critical ICT third-party service providers where that specific risk is identified".

2. **USA**: the Treasury Department plays a central role in boosting cybersecurity in the sector. This includes coordinating with industry groups, conducting incident response exercises, sharing threat information, and developing risk assessment guidance. Treasury has, since 2023, maintained a Cloud Executive Steering Group, a public-private partnership dedicated to bolstering regulatory and private sector cooperation. This will document cloud third-party risk, outsourcing, and due diligence processes to increase transparency, develop best

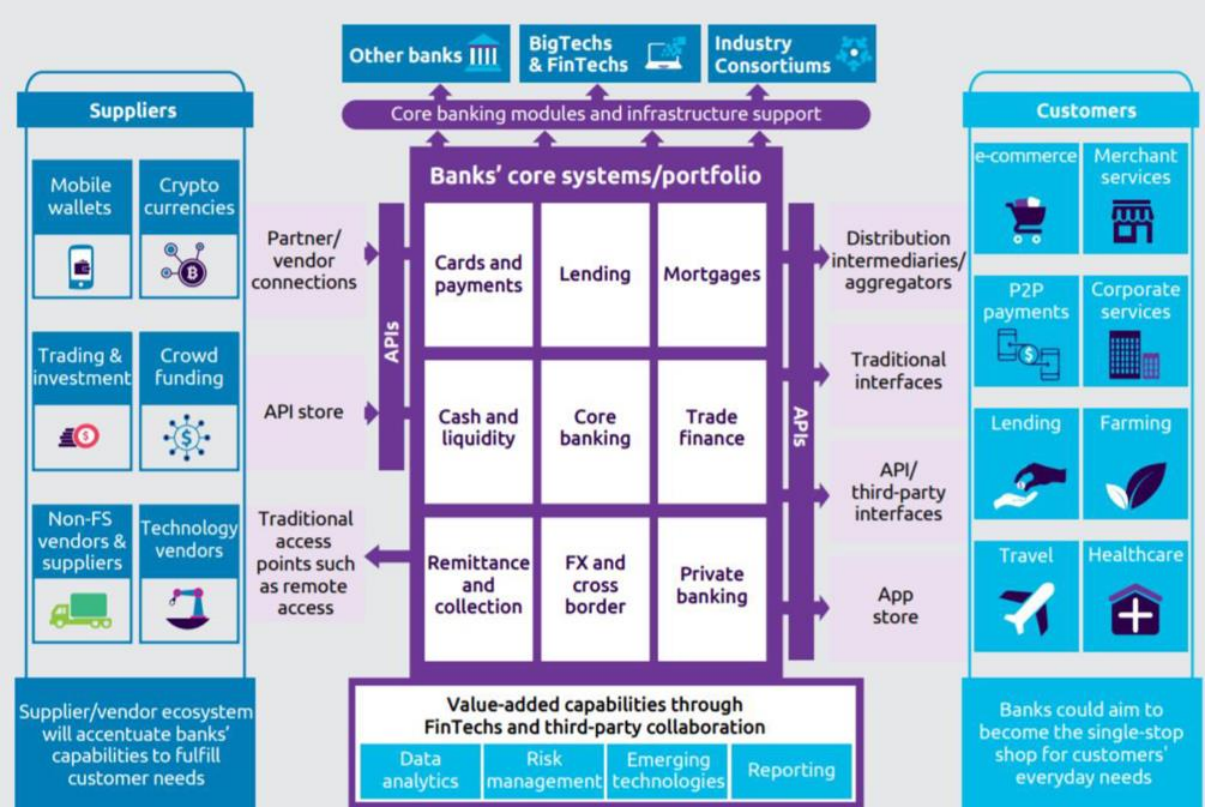



*Figure 16 Banks in open ecosystem context. Source: Capgemini, World Payments Report, 2019*

practices, and improve transparency and monitoring of cloud services for better Security by

[32] Namely, European Banking Authority, European Insurance and Occupational Pensions Authority, European Insurance and Occupational Pensions Authority.

Design, and, importantly, determine if existing authorities for cloud service provider oversight are sufficient and account for systemic risks. The Executive Order on supply chains resilience mentioned before is not specific about the financial sector.

3. **China**: public policy for resilience in finance and banking has, as in the US, been strongly influenced by the central bank, i.e. the People's Bank of China (PBC). The PBC has introduced technology risk management frameworks, next to demanding general cybersecurity and data security regulations. PBOC is also running a fintech development plan (2022-2025) that includes risk control through a common 'middle platform'.[33] Interestingly, the predecessor plan (2019-2021) put more emphasis on cybersecurity and systemic resilience.[34]

   Several characteristics of the Chinese system are special. Firstly, policy is always driven by the imperative to safeguard national security and sovereignty. This limits foreign involvement and makes it practically impossible to land into large dependencies on foreign cloud or fintech providers. Secondly, a number of digital platform companies such as Tencent and Alipay have become huge in payment services by leveraging on their e-commerce activities, next to digital insurers and financial conglomerates such as PingAn as well as digital banks and asset managers including WeBank. However, all of these have come under scrutiny by the state and the Communist Central Party (CCP) and been curtailed. Obviously, the same holds for the state-controlled enterprises that are the other big players in finance and banking. Thirdly, China is essentially a cashless economy, implying a ubiquitous dependency on digital resilience. Fourthly, China's financial institutions invest massively in technological innovation. They are also very much data-driven and data-intensive. Centrally there is a big push for the digital yuan as a central bank digital currency (CBDC), on which other countries and regions like the EU are still trailing behind. Finally, there is an attitude that disruption is opportunity to improve efficiency, drive innovation and build resilience (KPMG, 2023). Altogether then finance/banking is a largely self-sufficient system with strong government control across the whole supply chain and long-running extensive experience and a positive approach to digital resilience.

4. **International initiatives:** as far as resilience is concerned, the governance initiatives below are all about financial resilience (e.g., risky financial transactions such as loans, financial market fluctuations, banks financial buffers, debt defaulting, etc). The institutions listed below often have a long history. They have all added at a more recent time their insights on digital resilience such as cybersecurity and critical dependencies on IT providers. The initiatives are listed below from this perspective of financial resilience, briefly linking to their work on digital resilience, and notably to illustrate aspects of existing global/international governance in finance/banking. The fact that this sector has extensive cybersecurity regulations and governance has led the EU to declare these as adequate under a *lex specialis* clause in its Network and Information Security Directives.

   a. The Bank for International Settlements (BIS),[35] the oldest international financial institution, has as mission to "support central banks' pursuit of monetary and financial

[33] http://www.pbc.gov.cn/en/3688110/3688172/4437084/4441980/index.html.
[34] http://www.pbc.gov.cn/english/130721/3880801/index.html.
[35] https://www.bis.org/.

stability through international cooperation, and to act as a bank for central banks". Several BIS reports immediately linked to digital resilience have been referenced above.

b. The Basel Committee on Banking Supervision (BCBS)[36] is a forum for regular cooperation on banking supervisory matters. It has developed the Basel Accords, which are a set of international banking regulations. These regulations, including Basel III, set standards for capital adequacy, stress testing, and market liquidity risk, aiming to strengthen bank capital requirements and enhance the resilience of the international banking system. BCBS addresses digital resilience through guidelines for outsourcing of IT, IT governance and IT risk management, cybersecurity best practices, next to including disruptions related to digital systems in principles, regulation, and guidance for resilience in general. One of five pillars of the current BCBS work programme is digitalisation of finance.

c. The Financial Stability Board (FSB),[37] set up in response to the global financial crisis of 2007-2008, coordinates national financial authorities and international standard-setting bodies on regulatory, supervisory, and other financial sector policies to promote financial stability. This includes peer reviews across countries. Global Systemically Important Banks (G-SIBs) have been designated by FSB and BCBS. Their failure would have a significant impact on the global financial system and economy. They have higher capital buffer requirements for their resilience and to reduce the risk of financial instability. The FSB has cyber resilience as a key element of its work programme "to promote financial stability". It provides recommendations for greater convergence on cyber incident reporting and to handle cyber incidents.

d. The International Monetary Fund (IMF)[38] provides policy advice, financial assistance, and technical assistance to its member countries and offers recommendations to strengthen resilience. It includes cyber and digital resilience in its global and country financial stability assessments.

e. The G20 has been instrumental in coordinating international responses to financial crises and promoting financial stability measures, and addresses more generally, digital infrastructures as well as global supply chains. Its directives for finance/banking are taken up by, for instance, BIS, BCBS and FSB. The current G20's Digital Economy Working Group[39] does not, however, address digital resilience directly.

f. The G7 addresses supply chain security in general and notes specifically critical minerals, semiconductors, telecoms and batteries, recommending partnership approaches (G7, 2023). As regards digital resilience in finance/banking, the G7 has addressed cybersecurity for the financial sector since 2015. Most recently the G7 Cyber Expert Group[40] conducted a cross-border exercise on response to a widespread cyber incident affecting the financial system.

[36] https://www.bis.org/bcbs/about/overview.htm?m=77.
[37] https://www.fsb.org/.
[38] https://www.imf.org/en/Home.
[39] https://www.g20.org/en/tracks/sherpa-track/digital-economy.
[40] https://home.treasury.gov/policy-issues/international/g-7-and-g-20/g7-cyber-expert-group.

g. The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a global member-owned cooperative that provides secure financial messaging services since 1973 to over 11,000 financial institutions across more than 200 countries and territories. Its members include banks, financial institutions, and corporations involved in international trade. It provides for cybersecurity of its financial transactions network and systems.

**Company strategies**

This sector is so heavily regulated that corporate strategies are already strongly conditioned by or prescribed by public policy. Moreover, *business continuity management (BCM)* is a long-established practice, which can be comprehensive – addressing also the suppliers. In addition to or within business continuity planning, some examples of corporate strategies are:

1. *Cybersecurity*: foremost these companies and institutions have invested for many years in enhanced cybersecurity, making their operations, also at the interface with their suppliers, more robust. They can contractually extend this to their supply chain, and/or demand certification from their partners. ENISA provides several best practice guides for the financial sector.[41]

2. *Risk assessment*: regular audits, risk assessments, and contingency planning to mitigate the impact of supplier disruptions. HSBC has a supplier Code of Conduct that suppliers must comply with sufficient management systems and governance, as well as respond to information, compliance, and audit requests.[42]

3. *Scenario planning and stress testing*: scenario planning and stress testing help to evaluate the impact of supplier failures on operations, identify critical suppliers and develop strategies to mitigate the risks associated with supplier disruptions.

4. *Cooperation*: for instance, in Information Sharing and Analysis Centres (ISACs). An example is the US FS-ISAC, founded in 1999, that operates a real-time information-sharing network sharing intelligence, knowledge, and practices for the financial sector's collective security and defence. This also includes cyber-exercises. Similar in Europe is the FI-ISAC.[43]

5. *Transparency*: banks and other financial institutions are increasingly performing due diligence checks This is also an obligation under the Corporate Sustainability Reporting Directive (CSDR); relatedly they do supplier risk assessment on regulatory compliance (such as anti-money laundering), fraud risk (e.g., on shell companies), and reputational risk (such as for sanctions). Banks may be concerned about working with Chinese counterparts if these risk sanctions for financing war-related trade with Russia.

[41] https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/finance/?tab=publications.
[42] https://www.hsbc.com/-/files/hsbc/our-approach/risk-and-responsibility/pdfs/hsbc-suppliers-code-of-conduct-english.pdf?download=1.
[43] https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/finance/european-fi-isac-a-public-private-partnership.

6. *Insourcing*: banks invest in technical solutions such as AI for cyber-intelligence, backup, redundancy in connectivity. Instead of relying on third-party providers banks can also invest in own technological and service solutions. Generally, financial institutions are large investors in inhouse ICT.

7. *Diversification of suppliers*: reportedly it is ever more difficult for financial institutions to escape from lock-in with one large ICT service (cloud) provider. Nevertheless, they can make contracts for switching and backup with alternative providers.

## 6.3 Observations

**Structure and dynamics, policies and strategies**

The finance sector is particularly sensitive to systemic or cascading risks. These can be:

- Within the same organisation, e.g. from technical to psychological / customer interaction
- Between organisations, from one actor to others, e.g., from one back to others
- Hard to contain and requiring new expertise and skills for their handling.

Banking and finance are highly dependent on ICT providers. Notably, these are the ever more concentrated large cloud providers. Authorities are warning banks about this dependency. As the FT wrote "Regulators are getting nervous about the risks emanating from data storage and processing platforms dominated by a handful of big companies", see (Tett, 2023). This also raises concerns about market power (and is being investigated by competition authorities such as the UK's CMA). However, banks may no longer have a choice unless they either team up or self-provide alternatives or are forced by regulators to not put all their eggs in one basket, that is, to have alternative suppliers.

BIS states that dependencies on the ICT supply chain, especially on cloud providers, is a blind spot for banks and regulators Crisanto et al. (2022), and are a Single Point of Failure (SPOF). Banks would not have the expertise to handle these dependencies and potential (systemic) risks. Developments go – as much in ICT – very fast, at a speed that is hard to handle for the financial world. Path dependency plays a role as banking got confronted with resilience risks in 2008, when there was no crisis in other sectors, and acted correspondingly. BIS warned about SPOF risks (Koh & Prenio, 2023) and also analysed whether banks are using multiple Cloud Services Providers (CSPs) for resilience. The answer is that the trend is to use fewer CSPs rather than more. A worrying 50% of banks have, for their subscribed cloud service, no backup plan and even if they have it, it has often not been tested (Koh & Prenio, 2023). In a 2022 survey, Accenture reported that 63% of banks planned to move their mainframe workloads to public cloud environments, 31% to hybrid cloud and just 6% to use private cloud (Accenture, 2022).

Other sectors can learn much from the finance/banking's long experience with business continuity management, resilience, and cybersecurity. However, a downside of being a frontrunner can be that sector-specific approaches are devised where horizontal approaches could be equally valid. To some extent this can be said about DORA vs NIS2. Many requirements are comparable, yet there are two different laws. For third-party service providers such as cloud or identity/access management providers, who are subject to both, this can be a burden. Table 3 compares NIS2 and DORA.

*Table 3 NIS2 vs DORA*

| **NIS2** | **DORA** |
|---|---|
| Cybersecurity | Digital operational resilience |
| Horizontal, Directive | Vertical, Regulation |
| *Lex generalis* | *Lex specialis* |
| Focus on cyber in essential/important entities | Focus on systemic risks due to cyber |
| Digital infrastructure sector (cloud, eSign, …) | 'ICT Third Party Providers', notably cloud |
| Implicit on contract with third parties | Explicit on contract with ICT TPPs |
| Supply chain security requirements | Implicit in system risk assessment |
| Ex-ante and ex-post | Mostly ex-ante |
| Building up cybersecurity governance | Using legacy of financial sector governance |

**Global or International governance**

Digital supply chain resilience and related governance is only a part of the wider framing of resilience in the finance/banking sector. As shown, much international and even global inclusive governance is in place. Such governance is being extended to also handle the new digital risks. The advantage in doing so is that systemic risks that involve multiple parties in the sector can be addressed by existing governance, such as by joint monitoring and response and if needed, intervention by authorities. Such intervention can include halting transactions, providing temporary financial guarantees, and even nationalisation.

In this respect, this sector provides an interesting comparative case for global governance, and minimally provides important learning opportunities (Cowhey & Aronson, 2017). CERRE in its Global Governance for Digital Ecosystems (CERRE (Pascal Lamy, Bruno Liebhaberg et al), 2022) pointed to the Financial Stability Board (FSB) as a possible model for global digital governance.

However, generalised cross-sector action for resilience may be more difficult, for instance in a cyber incident where the financial sector is involved but also the cloud sector in general which then must act in compliance with both sectoral and horizontal cybersecurity regulation. Such fragmentation tends to be more costly as procedures and reporting lines are not one-to-one. If there is a systemic risk involving several sectors, response may suffer from lack of proper coordination.

Likewise, if more than one sector is involved, each may have its own international governance (if any at all), which poses the challenge of coordination in international governance.

# 7. Digital Supply Chains Resilience – Meso-Level

**Chapter Summary**

The comparison of the cases at the supply chain level (meso-level) shows that there is not a once-size-fits-all approach to global/international governance for digital supply chain resilience. Yet, a number of case findings can be generalised and, moreover, there are important lessons and practices to learn from and inform specific digital supply chains in terms of types of resilience actions, metrics (and the need to develop these), and trade-offs.

## 7.1 Semiconductors

Findings from the semiconductor supply chain (SC) resilience case include the following.

**Structure and dynamics, policies and strategies**

- A wide range of policy interventions and corporate strategies is being applied.
- These decrease average geo*graphical* distance but do not exclude remote SC partners.
- These keep equal or decrease geo*political* distance between SC partners.
- Buy-local policies are pursued by China and the USA but not by the EU.
- SCs are very complex with multiple two-way dependencies and specialisation.
- SCs are rather interconnected industrial ecosystems than linear chains.
- SCs for advanced semiconductors are reducing geopolitical distance, i.e. move from China.
- SCs for less-advanced semiconductors get more dependent on China though not exclusively.
- SC analysis is challenging due to complexity, metrics are little advanced.
- In semiconductors China is vulnerable and strong (counter-)action should be anticipated.
- Policies and strategies have short to mid-term timescales (2-7 years) but aim for the long-term.
- Anticipate that technological development, esp. quantum and AI, may radically impact the SC.

**Governance**

- SC governance reflects geopolitical closeness.
- SC governance is complex with company vs government and intergovernmental tensions.
- SC governance is commercially and politically sensitive, and time is needed to build trust.
- If the US pursues a self-sufficiency, this may be problematic for international cooperation.
- EU has strong cards but is realistic and knows it cannot go alone.

- EU struggles to compete internationally in investment funding (e.g., subsidy races, red tape).
- A loose geopolitical bloc is already forming of US-Japan-S. Korea-Taiwan and US-EU alliances.
- Some international industry alliances form to seek greater control on supply chain resilience.

In semiconductors, the overall emerging picture is of a liberal democracy West-led bloc which vigorously pursues increase of resilience and also seeks to constrain the rise of an authoritarian China-led bloc. This is a threatening situation for China and consequently retaliation should be expected and is already happening. This is either in the semiconductor sector itself, such as in less-advanced electronics and chips, and in related areas notably critical materials. Retaliation can also be in other sectors from automotive to food. A trade war could be triggered. Preparation for this may have to include stockpiling and semiconductor emergency production. The latter is foreseen in the EU Chips Act.

Policies and corporate strategies must cope with constraints and barriers in addressing resilience in supply chains. For one, collusion should be avoided, for instance, where downstream companies takeover upstream semiconductor companies. As supply chains are already rather dense this can lead to objections by competition authorities. An example is the failed takeover by NVIDIA of ARM in 2020.

A barrier to resilience in semiconductor supply chains for the EU is the financing challenge. Money matters: in the US, as of November 2023, private companies have announced more than $614 billion in planned investment in industries with a spike in investment across computer, electrical, and electronic industries. In September 2023, there was over $100 billion in investment for the construction of manufacturing facilities including plants for semiconductors and batteries. Some ways forward are to extend the policy toolbox by involving downstream user industries such as automotive, AI, & supercomputing, defence to reduce financial risks and unlock co-financing, and by mobilizing Cohesion Funding and public procurement (see also section **Error! Reference source not found.**).

Most public policies and corporate strategies aim at changing the structure and dynamics of the supply chain, such as to reduce chokepoints, increase supplier choice, etc. Public policies generally would shift a degree of control towards governments, which is being justified referring to the need to sustainably strengthen economic security and national security in the long run. In that respect, they seek to strengthen strategic autonomy at the expense of control by third countries or by companies.

In terms of governance, national or EU-level policies and industry strategies that include partnerships with likeminded or allies fit with the overall emerging picture of a liberal democracy-led geopolitical bloc or alliance. If this were to deepen based on sufficient trust, it would allow for specialisation and geographic distribution that is closer to the current global supply chains. Such an alliance would reduce the negative impact on efficiency from fragmentation and ongoing structural change towards reshoring and domestic capacity-building. However, the signs so far are not very encouraging for such deepening of cooperation, apart from reference by the US and the EU to trans-Atlantic cooperation on diversification ("To boost our economic security, we continue to cooperate through the TTC to diversify strategic supply chains, including […] semiconductors" (EU and US, 2024).

Regional or national semiconductor organisations such as the US Semiconductor Industry Association (SIA) seek to promote national interests. While they can provide very valuable information and

analysis, by the nature of their mission they are less suited to advance international governance in such an alliance of resilience in the semiconductor supply chains.

It can be an opportunity for EU policy makers to advance a wider semiconductor alliance of liberal democracy countries and move towards public - private governance on resilience in semiconductor supply chains.

International industry alliances could exert more influence on semiconductor supply chain resilience. While this is emerging in automotive (Catena-X was mentioned before), other sectors that report to have been impacted include electronics, digital in general, health, and renewables. Some of these have international platforms that can take up resilience of supply chains (semiconductor and others). For instance, the medical devices sector brings together many global or international companies at European level in MedTech Europe and at US level in AdvaMed, and moreover, works closely with governments internationally, in the WHO.

Some insights about the impact of the various semiconductor partnerships on resilience and economic performance start to appear. BCG (2024), comparing 2024 with 2021, concludes that the industry starts to improve resilience through geographic diversification and links this to the industrial policies esp. of the USA. Some 70 fabs are under construction in Arizona and Texas (McKinsey, 2024b). BCG has high expectations of the $500 million International Technology Security and Innovation (ITSI) Fund in the US Chips Act. This fund would support resilience in assembly, test, and packaging amongst others in Eastern Europe. As BCG (2024) states, “As we look to the future, it will be imperative for policy makers and industry participants to stay the course, building on recent positive momentum to increase resilience, without overcorrecting and putting at risk the more than $1 trillion of value created by the global nature of the semiconductor supply chain”. They also state “The United States and allied governments need to maintain open trade and cooperation by recognizing that extreme industrial policies, such as full country-level ‘self-sufficiency’ will undermine resilience, add cost, and stifle innovation.”

## 7.2 Critical Raw Materials

Findings from the critical raw materials supply chain (SC) resilience case include the following.

**Structure and dynamics, policies and strategies**

- A wide range of policy interventions and corporate strategies are being applied.
- These change the structure by decreasing geographical distance and supplier diversification.
- Shorter supply chains arise yet network density (concentration) also decreases.
- Alternative and advanced materials may both eliminate and create suppliers.
- More recycling increases the intensity of reverse buyer-supplier relationships (circularity).
- More efficiency reduces the intensity of supplier-buyer relationships.
- Most interventions and strategies have a long to very long timescale (10-15 years).
- SC analysis and metrics are well advanced.
- SC monitoring is feasible, even more so with AI and blockchain.

**Governance**

- SC governance can be relatively simple, thematically focused, but must be long-range.
- SC governance must be international from the EU perspective.
- SC governance is very geopolitical and cannot be limited to bipolarised governance.
- SC governance is geopolitically diverse.
- 'The West' is late to act, compared to China which will hamper international partnering.
- The colonial, imperialistic past of the West likely creates hostility to international cooperation.
- Critical Raw Materials Club is a win-win novel form of governance.

Investment funding is feasible but has not been explicitly earmarked although the EU legislation has defined the possibility to designate Strategic Projects and in a joint Board of Member States and Commission discuss their financing, in particular from the EU's Global Gateway Initiative.

Geo-strategically then, creating resilient CRM supply chains in collaboration with third countries requires developing closer relationships with them along several axes and perhaps even into exclusive partnerships. Indeed, EU and US policy in CRMs should reduce geopolitical distance though it may not decrease geographic distance. Likely, this cannot be done without negotiating about other matters such as economic development in general and/or military support, environmental sustainability, and human rights. Consequently, international governance in CRMs cannot be approached very narrowly in policy domain terms.

The inclusive, win-win, and multi-policy thinking appeared to be driving the EU's proposal for a Critical Minerals Club – and its linkage to the EU Global Gateway, with potential to evolve into a pluripolar global governance, that is, with several countries playing a very important role, depending on their natural resources, though with China and Russia not being member of the Club.

However, the CRM Club proposal has now been absorbed in the Minerals Security Partnership Forum, a joint initiative of the EU and US. This may be a pragmatic approach by the EU to accelerate international cooperation. However, it also raises the question whether EU is losing some control. Moreover, self-interest, national commercial interests and hard geopolitics will come into play, and it will be hard to address that in the MSP Forum.[44]

In principle, the driving force for this could be the EU together with the US, but it is not guaranteed that this will be the case, and it has not been endorsed at recent EU-US meetings. The EU and US do coordinate on shortages shocks. The TTC meeting of April 2024 mentioned collaboration on a joint early warning mechanism to identify and address potential supply chain disruptions, which is claimed to have been effective in the gallium and germanium markets (although it is not reported if and to what extent these restrictions have been countered)[45]; and more generally, to boost economic

[44] Recently, the US has been seeking to pre-empt the takeover of a Congolese mine by a Chinese military equipment manufacturer. (Dempsey & Wilson, 2024) report that the US both tried to prevent this sale and also get a US company interested in bidding.

[45] The reaction of markets appears to have been moot (FTI, 2023), though gallium prices have steadily risen since Sept '23. Germanium prices did not react at all at the time of the export controls (though there is a recent (June '24) price hike).

security, by cooperating to *diversify* strategic supply chains and reduce vulnerabilities, including those caused by other countries' non-market policies and practices.

The US invests much in domestic mining and processing capacity for its domestic supply. In parallel it seeks bilateral deals with third countries. The EU follows a similar approach but, with more limited domestic resources, it is even more dependent on third countries. In CRM policy then, the EU is better off acknowledging pluripolarity, that is, making deals that realistically recognise the power balance, seeking mutual added value of the EU as a mineral-consumer and of third countries as mineral-rich suppliers.

The EU CRM policy is criticised by Francesco Findeisen & Yann Wernert (2023) as failing to recognise the time scales (1—15 years) and costs involved to build up supply chains. The EU CRM policy does indeed not come with a budget envelope, though it may well be possible to mobilise private and other investment. Another criticism is that it does not anticipate geopolitically motivated export restrictions i.e. that dependencies get weaponised – which is already happening, viz. the restrictions on exports from China of germanium and gallium. Finally, many states controlling CRMs have painful memories of colonial times, and several have non-democratic regimes. They are not waiting to be lectured about human rights and labour conditions by the EU or the US.

## 7.3 Software Supply Chains

Findings from the software supply chain (SC) resilience case include the following.

**Structure and dynamics, policies and strategies**

- Proprietary software originates from across the world, notably from EU, USA and regional allies, India, as well as in embedded form (as in mobile phones, machinery) from S. Korea, Taiwan, and Japan.
- An important part of the supply chain comes from open-source developers and open-source intermediaries (collaboration and distribution platforms).
- Therefore, distinct from other supply chains, open-source software, and even some proprietary software, includes a community effort to find and repair vulnerabilities.
- On top of existing quality control mechanisms, more recently ICT security certification is imposed by law, notably by the EU Cyber Resilience Act and US Executive Order.
- A supply chain digital infrastructure will thereby take shape, centred on Software Bills of Materials (SBOM), certificates, and possibly blockchain-secured software distribution.

**Governance**

- Bilateral, EU-US, governance is developing on ICT security certification and Software Bill of Materials efforts. This has potential to get internationalised in terms of standards and mutually recognised inspection and certification authorities, though this is not likely to become global, given national security concerns in several countries.
- Open-source security governmental initiatives are so far initiatives confined to the USA and to a limited extent the EU (in the CRA). They lend themselves for a global approach, notably since there is support (in the US) of software foundations and open software standards

collaborations, such as IETF, Open Software Foundation, and Apache. Open-source security and resilience can be supported by global standards that in turn may be applied for proprietary software as well. Law such as the EU Cybersecurity Act and Cybersecurity (which may show a 'Brussels effect' (Bradford, 2020)) and international cooperation with likeminded countries such as in the OECD Global Forum for Technology can give momentum to such global governance.

Software supply chain resilience will become ever more important with the growing reliance on ICT in most other supply chains and, indeed, in most economic activities. The open-source way of managing software innovation and quality is a unique social-economic phenomenon with huge value. It is, however, at risk of under-resourcing and by weaponisation (i.e., manipulation for geopolitical purposes, as illustrated by the SolarWinds and xz cyber-incidents mentioned above). Global governance to maintain and reinforce open-source development and quality management in as any areas as possible would contribute to building a global common good as a win-win for all actors involved.

## 7.4 Finance/Banking

Findings from the finance/banking supply chain (SC) resilience case include the following.

**Structure and dynamics, policies and strategies**

- Digital supply chain resilience is embedded in and an extension of a long history of engagement with financial resilience.
- Despite its maturity, supply chains and related governance are challenged by 1) the increasing dependency on a small number of very large cloud and platform providers who come with their own approach to resilience especially as regards cybersecurity and 2) the geopoliticisation of the existing governance and systems (or weaponisation), of which sanctions and transactions surveillance is an example.

**Governance**

- Global governance is well-developed and illustrative as a model for other sectors. This also holds for governance of shared technical infrastructure, i.c., SWIFT. The sector shows how across the sector and internationally technology, norms, rules, and supervision can be combined.
- Yet, even fairly recently following the 2008 financial crisis, governance has been significantly enhanced (e.g., globally with the FSB, regionally with several European financial supervisory authorities).
- In the finance/banking sector China still has significant dependencies in particular on the USA currency, banking and securities systems. Attempts to set up alternative global governance or bifurcate the global financial transaction system have had limited success so far, although China and Russia will not cease to decouple or derisk in international finance.

Attempts by China and Russia to set up an alternative global finance system may lead to future bifurcation. Cybersecurity resilience increasingly relies on powerful cloud providers. These have on the one hand their own, proprietary resilience and emergency mechanisms. On the other hand, they

also must comply with strong legislation. Complicating matters, the applicable rules are both sector-specific ones and horizontal ones (e.g., in the EU resp. DORA and NIS2).

These two changes, geopoliticisation and digital dominance, may put global governance in the sector under stress. Experts also warn that systemic risks increase due to these structural changes (Crisanto et al., 2022). Nevertheless, in terms of capability and capacity to handle resilience this sector remains one of the most experienced and advanced in dealing with supply chain shocks and systemic effects.

The sector has several strong international governance assets. SWIFT is both the global backbone and a global governance for communications and processing of international financial transactions. The SWIFT cooperative society is an established and tightly coupled entity in global financial supply chains. It operates resilience emergency mechanisms next to regular operations. Another asset is the Bank of International Settlements which, as the oldest global bank, has credibility in establishing joint understanding and norms. There is a high awareness of interdependencies in the supply chain and possible systemic effects. Such governance assets and global technological infrastructures are a model, at least to learn from, for global governance of supply chains in other sectors, the essence being to establish global governance that reinforces supply chains to deliver resilience and efficiency as global common goods.

## 7.5 Generalising

Here we seek to draw some general observations on resilience of digital supply chains, based on the cases, still within a meso-level analysis which focuses on a supply chain as a structure of entities and relationships. An upfront disclaimer is that our meso-analysis toolbox is still limited today, and many questions remain for further investigation.

### *7.5.1 Types of Resilience Actions*

Generalising, the actions to improve resilience in supply chains are then either about 1) hardening the existing supply chain, 2) structural reinforcement of the supply chains, or 3) structural change of the supply chain. Hardening means that entities themselves (suppliers, buyers) strengthen their internal resilience and enhance resilience in their existing relations but there are no new entities or relations between the entities in the supply chain. This cannot be defensive only, but must also be pro-active, combining business continuity management with 'resilience engineering'.[46] Structural reinforcement means that new structures are superimposed on the existing supply chain such as an infrastructure for monitoring supply chain performance. Such superstructures[47] can also include new supply chain governance. These, in turn, may get internationalised and are then of interest for this study. Structural change means that new entities and relations are added to the supply chain. This is illustrated for each of the cases in Table 4.

As regards the second type, structural reinforcement of the supply chain, an example would be a supply chain data infrastructure that enables the provision of information about suppliers and buyers and 'measures' the state of the supply chain.

[46] Aiming at managing the adaptive capacity of the company and its supply chain partners in an uncertain and dynamic world, see for instance, (Steen et al., 2024).

[47] These map onto entities and relationships of the supply chain (by a functor in category theory language).

As regards the third type in the table, resilience may be improved by changing the supply chain structure, for instance adding new suppliers or supply chain intermediaries, marketplaces, or platforms. Examples of business models of such intermediaries to run have been developed in sectors such as logistics. Examples of using AI to for supplier diversification are starting to come from other areas of business.[48]

*Table 4 Three types of supply chain resilience action with examples*

| | Semiconductors | Critical Raw Materials | Software Supply Chains | Finance and Banking |
|---|---|---|---|---|
| **(1) Hardening the existing supply chain** | Stocks<br>Expand domestic manufacturing | Stocks | Cybersecurity<br>Certification | Data backups |
| **(2) Structural supply chain reinforcement** | Emergency allocation of manufacturing | Monitoring across supply chain | Vulnerability sharing | Systemic risk audits |
| **(3) Structural supply chain change** | Diversification of supply<br>Marketplaces | Diversification of suppliers | Transforming proprietary to open-source | Diversification of suppliers |

The various types of resilience actions, where governments can act, can be combined into a comprehensive public policy package. Where it is applicable that for an individual company to act, they can be combined into a comprehensive corporate strategy package.[49] Throughout this study we showed that this may well be needed. An example of an impressively comprehensive approach is given by the White House report of November 2023 for the case of semiconductors. Listing policy actions and indicating the type of resilience actions they relate to with number as in the table above, it includes: a data-gathering and analysis structure and monitoring (2); communication across the supply chain (2); incentives and investment for reshoring (1), domestic capacity (3), diversified supply and redundancy (3); cooperation with international allies (2), and systematic review of supply chain issues, with supporting governmental structures such as Department of Homeland Security's Supply Chain Resiliency Centre (2), which amongst others should "help secure the semiconductor supply chain, strengthen resilience, and further the implementation of the CHIPS Act." (The White House, 2023).

[48] Hoek & Lacity, (2023) in "How Global Companies Use AI to Prevent Supply Chain Disruptions" refer to chemicals, food, retail and logistics.

[49] McKinsey (2024a) advises companies to develop 'insurance' action such as holding strategic inventories or having contracts for backup supply, i.e. type (1) action, developing real alternatives through technology (type (1) or (3)), new partnerships and diversification of suppliers (type (3), or shifting supply chains or production locations (type (3) or (1), and end markets (type (3)).

The EU's economic security package is comparably comprehensive but is still being filled up with proposals for concrete interventions and with the actual implementation.

China's approach has a much longer history, and its effectiveness has already been shown in terms of fostering dependencies of other economies on China and creating independence at home.

### *7.5.2 Supply Chain Metrics*

Much work has been done to map dependencies in selected supply chains. For the EU, see for instance such mapping for critical raw materials (JRC, 2023a) and for semiconductors (European Commission, 2022a). Yet, mapping is not completely and is also continuing to change.

Assuming we know the supply chains, that is the entities and relationships or dependencies, we can try to measure some overall their characteristics. Some such supply chain metrics are given by McKinsey (2024a). They include network density or concentration, geographic distance, and geopolitical distance (see also footnote 56). Others are providing a supply chain stress indexes such as the Global Supply Chain Pressure Index of the Federal Reserve Bank of New York (Federal Reserve Bank of New York, 2024) which integrates transportation cost data and manufacturing indicators. This index is, however, only applicable where digital supply chains either directly, or via input supply chains, relate to physical products (in our cases resp. semiconductors and critical raw materials). It is not applicable to purely digital situations such as software supply chains or mixed situations such as in finance/banking (the latter case is illustrated in Figure 16).

Habibi et al. (2023) provide an overview of some 20 academic references, which show a great variety of resilience metrics. They then propose six metrics that address resilience in terms of performance and time (duration) of the regular state of a supply chain, the disruptive stage, and the recovery stage. This can readily be mapped onto the widely referenced NIST approach to cybersecurity resilience (NIST, 2024). Resilience may also be translated into system impact cost and recovery effort cost (Aguila & ElMaraghy, 2019). However, such metric work has not yet been extensively validated, let alone standardised.

Having several metrics may be useful for developing strategies and actions to counter supply chain disruption, and even – with underlying graph theory and simulation – to separate the risks of idiosyncratic shocks from systemic (cascading) risks. A single metric for supply chain resilience may be useful for policy goal setting. Habibi et al. (2023) warn, however, that current examples of a single index are oversimplifying and risk yielding biased results.

Over and again, the cases illustrate that a single policy perspective cannot address resilience. Several policies need to be joined up, from trade, to industrial, to foreign policy. The larger policy perspective in the EU is strategic autonomy for which resilience is a *conditio sine qua none*, but not sufficient. The larger perspective in the US is geopolitical and geoeconomic competition. As formulated by the US Trade Representative Katherine Tai, "Industrial policy is now part and parcel of trade policy. This is absolutely necessary if we are going to win the economic competition of the 21st century" (USTR, 2023b).

Several studies point to the growing overlaps of cybersecurity risk management and supply chain risk management due to ever-deeper digitisation of supply chains (IBM & Microsoft, 2024). Others are

pointing to the need for intersectoral risk management such as between energy and digital communications (VDE, 2024). From the cases we also saw that critical raw materials and the semiconductor supply chains are closely related. Addressing related risk and risk perspectives is complicated. For instance, it raises the assessment of geopolitical risks to the intersectoral dimension,[50] and also requires combining physical security risks and cyber risks. It requires bridging risk management, security, and business continuity cultures.

Risks in logistics and finance can affect the resilience of many supply chains. For instance, ports across the world widely use the Chinese logistics platform LOGINK. It is free of charge and subsidised by the Chinese government. As reported by Foroohar (2024), the 2022 US-China Economic and Security Review Commission report states that the platform allows Beijing access to "sensitive data, including commercial transport of US military cargo, insight into supply chain vulnerabilities, and critical market information." China would then have a panopticon monitoring capability that could be weaponised. This is – whether theoretical or not – a resilience concern. Not dissimilar, financial and software supply chains underpin almost any other supply chain. Reasoning along the lines of Farrell & Newman (2019), they can enable panopticon control (if there is a central point) or chokepoint control (if there is a unique supplier).

### *7.5.3 Some Trade-offs*

The dire situation in supply chain resilience has roots in lack of awareness or understanding over the past 20-30 years of the erosion of resilience and more generally, of strategic autonomy, by neoliberalism and globalisation. For the business world, the watershed moment of resilience vs efficiency probably was COVID-19. This triggered the debate on Just-In-Time versus Just-In-Case.[51] For policy makers, COVID-19 added to the already growing geopolitical and geoeconomic concerns strategic autonomy. No wonder that we see the rise of post-neoliberalism, accompanied by resilience, economic security, and strategic autonomy policies. The current debate is about how to best combine and weigh these policies and characterised by terms such as decoupling or derisking, small yard-high fence, dual circulation, and 'economic nationalism done the right way'[52] (Rodrik, 2023) These all reflect a trade-off between local and global interests.

It would wrong to frame the current debate, post-neoliberalism included, as an 'end of globalisation' debate. Firstly, the facts do not support this (some more detail is given below). Secondly, new forms of globalisation develop that enable greater resilience, such as wider supplier choice, supply chain information globalisation, win-win value building in supplier-buyer relationships, and international standards for resilience as we have seen in finance/banking and software supply chains. How these developments affect efficiency and the global level playing field remains to be seen.

[50] E.g., recently between the EU and China, raising e-vehicle tariffs leading to retaliation through wine and pork import restrictions.
[51] See earlier references to Jiang et al. (2021) and Masters & Edgecliffe-Johnson (2021).
[52] This argues that public policy intervention such as R&D support combined with import controls, buy-local, and other relatively protectionist actions ('economic nationalism') can only lead to a sustainable industry if it is accompanied with opening at the appropriate time and manner to global market competition.

Building greater control, domestic capacity, and home-grown capabilities in digital supply chains often means investing in basic technologies and complex industrial ecosystems. This takes a lot of time. This shows a trade-off between short-term and long-term.

Where supply chain resilience requires large sums of (public) money, this appears to go at the expense of the economic efficiency of open global markets with specialisation, and the rapid innovation of competition without barriers. This is a trade-off between efficiency and sovereign control. However, is the assumption correct that 'always bigger' is better? Firstly, what is the definition of 'better' – or to put it in starker wording: 'are cheaper products better than sovereignty?' or 'what is the price of autonomy?', or does 'the trilemma hold that hyper-globalisation, democracy, and sovereignty cannot all be realised at the same time' (Rodrik, 2007; Stein, 2016). Here the question translates into: what is the marginal cost of supply chain resilience and is that cost politically acceptable? Secondly, there is some counter-evidence, which suggests that from a business performance perspective, a degree of regionalisation may be better, as argued by JPMorgan's economists (Wise & Loeys, 2023). The question then becomes, when and how is building supply chain resilience an attractive business proposition?

Reinforcing supply chain resilience, for instance by diversifying suppliers can also run into concerns about human rights in non-democratic countries or about environmental protection. Guardrails in this respect should be provided in the EU, for instance by the Corporate Sustainability Due Diligence (CSDD) Directive (European Commission, 2024f) and the EU's economic security risk assessments, and in the US by the Entity List.[53]

Do regimes in likeminded countries differ in compliance with human rights or environmental standards in international supply chains to the extent that they lead to disadvantages in global competition? The answer is not (yet) available. We observe that companies are rather complaining about red tape and uncertainty associated with these policies. Moreover, some would argue that there is a Brussels or Washington effect of such regimes, i.e., companies would rather comply with the stricter regime provided that there is a big market behind this. In international supply chain governance comparability and compatibility of human rights and environmental standards is often included, at least in political wording. Hard mutual control mechanisms are rare, if existing at all (the Montreal Protocol on protection of the ozone layer is a positive and global example). A more sobering observation is that, in practice, companies and countries continue making, as awful as it is, trade-offs between human rights and economic or political interests.

Several of the trade-offs above are illustrated in speeches by US Treasury Secretary Jellen and USTR Katherine Tai (USTR, 2023b, 2023c), the small-yard big-fence speeches of US National Security Advisor Jack Sullivan (Jake Sullivan, 2022, 2023), and the de-risking speech of EC President Ursula van der Leyen (Ursula von der Leyen, 2023).

[53] The Entity List contain names of 'certain foreign persons – including businesses, research institutions, government and private organizations, individuals, and other types of legal persons – that are subject to specific license requirements for the export, reexport and/or transfer (in-country) of specified items', see (Bureau of Industry and Security, US Dept of Commerce, 2024).

## 7.5.4 Governmental Influence and Involvement

When we relate supply chain structure and dynamics to the structure and dynamics of international governance, we may wonder, how does this relationship come about and continue to evolve under influence of the actors? That is, what is the influence of government on the formation and running of such governance? Conversely, what is the influence of companies? Importantly, does this differ between governments, in particular, EU, US, and China?

Let's summarise our specific cases: China can exert a large amount of control on the international involvement of its companies but whether this results effectively in a large control over international governance varies between sectors, from high in critical raw materials supply chains to low in software supply chains. Next is the US in terms of government control in creating and running international governance of supply chains, be it – based on anecdotal evidence – this varies from highly effective in finance/banking, to effective in semiconductors and software, to only somewhat effective in critical minerals. The EU, also limited by its mandate, is least effective in state-centric international governance overall, with its strongest area being finance/banking, followed by a weak control on semiconductors and software, and little control in critical raw materials.

This analysis can of course be contested and needs detailing to explain the simple marking in Table 5.

*Table 5: Influence of the state on international governance*

| | Semicon Formation | Semicon Operations | CRM Formation | CRM Operations | Software Formation | Software Operations | Finance Formation | Finance Operations |
|---|---|---|---|---|---|---|---|---|
| EU | + | 0 | + | + | + | - | + | 0 |
| US | + | + | + | + | + | + | + | + |
| CN | 0 | 0 | + | + | + | + | - | - |

## 7.5.5 Setting Priorities

There are very many supply chains that may be of concern. The EU economic security strategy lists 10 key technology areas that each have a number of sub-areas. Even within the digital domain, this concerns any of the key technologies (semiconductors, telecommunications, IoT, AI, high-performance computing, cybersecurity, etc.) and supply chains to support key infrastructures that have massively become digitally dependent (energy, transport & logistics, health & pharmaceuticals, agriculture and food, etc.). Not all can be a priority at the same time and choices will have to be made. Are semiconductors more important than AI? Are medicines more important than safe ports?

In usual risk assessment approach two dimensions for setting priorities would be considered: 1) cost of lack of resilience (economic importance) and 2) likelihood of a resilience break (supply risk). Prioritisation for action would then be in first instance on these digital supply chains where the product of these two is the highest. The EU Critical Raw Materials Act contains a methodology for

calculation of economic importance and supply risk[54]. The EC's Joint Research Centre has provided an assessment of open strategic autonomy in industrial ecosystems and strategic technologies of which the economic dimension is close to this prioritisation (Kroll, 2024). However, the feasibility to act must also be taken into account. The JRC assessment looks at this from an innovation perspective but other criteria also need to be taken into account such as capacity, capability, and control in political decision-making, institutional policy-making, and international governance/diplomacy (see for the general perspective section **Error! Reference source not found.**).

[54] See Annex II, section 2 of (Regulation (EU) 2024/1252 of the European Parliament and of the Council of 11 April 2024 Establishing a Framework for Ensuring a Secure and Sustainable Supply of Critical Raw Materials and Amending Regulations (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1724 and (EU) 2019/1020Text with EEA Relevance., 2024).

# 8. Digital Supply Chains Resilience – Macro-Level

**Chapter Summary**

At macro-level, the drive for resilience of supply chains shows up in structural changes to global trade, economic impact, and other indicators of geopolitics/geoeconomics[55] and evolving global/international governance.

Academic theory that causally links a supply chain meso-economic perspective to global governance is still limited. However, when discussing the cases we argued some plausible linkages. In particular, public policies for global/international governance explain how supply chains entities should behave. They prescribe a path for supply chain entities to link to global or international governance.

However, when companies or sector organisations are initiators of changes for resilience in their supply chain, the path towards global governance is less obvious. Some established global governance of industry itself may even risk to get paralyzed or fragmented due to increasing geopoliticisation. Examples of this are the SEMI semiconductors industry collaboration and the geopoliticisation of standardisation in the ITU on the future of the internet ('New IP').

## 8.1 Structural Changes in Global Trade

A recent study on the geometry of global trade by McKinsey (2024a), finds that China, Germany, the UK, and the US have reduced the geopolitical distance of their trade by 4-10% since 2017. McKinsey uses as a proxy for geopolitical distance the UN General Assembly voting records showing – admittedly as an imperfect approximation – geopolitical alignment on global issues.[56] In addition, the US has reduced both the geographic distance to suppliers and diversified its suppliers. Investment in China for upstream production has significantly reduced but has jumped up in Africa and India compared to pre-pandemic averages, suggesting further supply side shifts to come. McKinsey adds that for concentrated products, that is, where there are only a few suppliers, geopolitical distance is larger than for non-concentrated products. This implies a double risk for resilience, namely supplier concentration and geopolitical stress.

IMD's Richard Baldwin observes that industrial supply chains are changing indeed, but that localisation, regionalisation and globalisation are all happening (Richard Baldwin, 2024). Research by BIS finds that "Global value chains (GVCs) are in the midst of a far-reaching realignment." (Qiu et al., 2023)

[55] Geoeconomics is taken here in the sense of the intersection of economics, politics and geography, focusing on where economic factors are used for geopolitical goals. In a wider view geoeconomics addresses next to political also geographic and temporal factors in relation to economics.

[56] Summarizing McKinsey geopolitical distance measurement: this is the distance on a one-dimensional scale of 1 to 10 of voting in the UN General Assembly on global issues, which included over 200 relevant votes between 2005 and 2022.

IMF records increasing geoeconomic fragmentation since the war against Ukraine started (IMF, 2024), see Figure 18. Setser (2024), however, argues that deglobalisation is not happening to the extent believed and it would be dangerous to build resilience policy on this belief. China's manufacturing surplus is still rising rather than declining. It reflects China's capabilities and capacities to produce at extremely competitive prices, Figure 17.

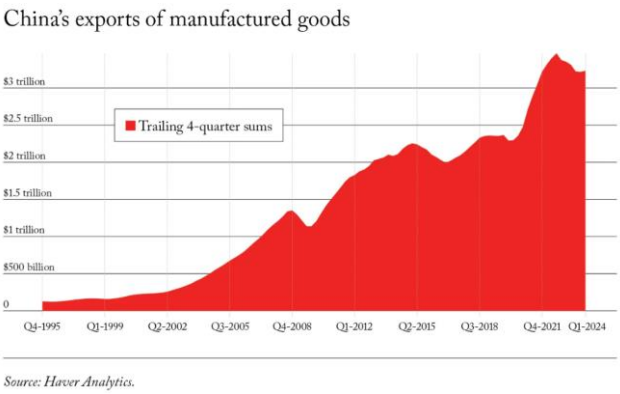
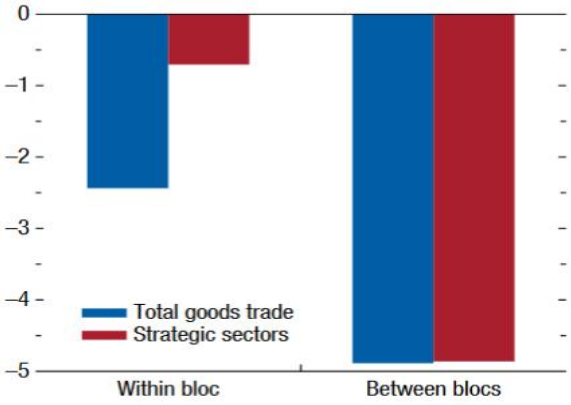



*Figure 18 China's exports of manufactured goods, source: Haver Analytics*




Sources: Trade Data Monitor; and IMF staff calculations. Note: Bilateral quarterly growth rates are computed as the difference in log bilateral trade averaged using weights equal to the bilateral nominal trade. Strategic sectors include the following Harmonized System two-digit chapters: 28, 29, 30, 38, 84, 85, 87, 88, 90, and 93. Before the war is between 2017:Q1 and 2021:Q4. The bloc definition is based on a hypothetical bloc comprising Australia, Canada, Europe, New Zealand, and the US and a hypothetical bloc including China, Russia, and countries siding with Russia during the March 2, 2022, UN General Assembly vote on the war in Ukraine. Other countries are considered nonaligned.

*Figure 17 Fragmentation affecting trade (difference in trade growth before and after the war against Ukraine, in %), source IMF*

Yet, there is a considerable shift, markedly so since December 2021, towards 'China +1', that is, maintaining sourcing from China but diversifying to have suppliers from other economies. Notably, next to Mexico, a number of Asian countries benefit from 'China +1', such as India, Bangladesh, Thailand, Malaysia, Vietnam, Indonesia, and Taiwan. BIS studies also show that Asian suppliers are interposing themselves in existing supply chains. Likely behind these other suppliers there are again suppliers from China (Qiu et al., 2023). The Economist states that this rather constitutes a rerouting from China, with limited added value – no more than packaging – in these other countries (The Economist, 2023a). The ongoing reconfiguration may therefore not be a full remedy against China-related geopolitical risks to resilience. The Chinese government may still be able to control the Chinese companies that are the source as these flows. European manufacturers and producers, especially in non-food, are reportedly rushing towards diversification, ahead of possible EU sanctions and tariffs against China, in which the EU hasn't yet been acting as fast and forcefully as the US (Langley & Ho-him, 2024).

Altogether, a differentiated, nuanced picture emerges: the US has advanced more than the EU in reshoring and is firmly on a path in certain sectors such as semiconductors to more domestic production. EU companies are also starting to diversify suppliers at least as much as the US, with possibly less reshoring, yet with domestic production on the increase in certain sectors such as automotive and less advanced semiconductors. However, even domestic production may not

eliminate geopolitical risks. For instance, in automotive this includes that Chinese companies set up production in the EU (BYD in Hungary, Geely/Volvo in Belgium).

Generally, both the US and the EU are far behind China in building domestic supply even if certain sectors China (still) has a high dependency on the US and EU.

Definite economy-wide conclusions are hard to draw but in individual sectors the pattern is clear that supply chains are getting more geopolitically concentrated or contracted. Yet at the same time and even in those sectors not all critical dependencies get eliminated.

# 8.2 Economic Impact

## *8.2.1 Resilience*

We can be short about resilience at macro-level. Firstly, there is no global indicator for supply chains resilience (let alone for *digital* supply chains resilience). Resilience may be measured for a specific supply chain, and even this is not happening yet.[57] A composite, global, indicator is not available.

Nevertheless, politically it may be important to have a global indicator on digital supply chain resilience as it may help to agree on common political directions, for instance at UN level. To develop this, inspiration can come from the Resilient Planet initiative of UNDRR (UN Disaster and Risk Reduction), the Insurance Development Fund and the University of Oxford as well as from sectoral analyses such as the IMF's Global Financial Stability Report and the EC/JRC Resilience Dashboards.

## *8.2.2 Investment and Business Opportunities*

As noted before, investment in upstream production in China has significantly reduced but has jumped up in Africa and India compared with pre-pandemic averages. The trend towards more national/regional industrial policy of the US and the EU, where this comes with large public investments other incentives, increases the investment attractiveness of the US and EU according to Wise & Loeys (2023).

Supply chain transparency – in any sector – is a precondition for increasing resilience. ICT should come to the rescue here. This creates business opportunities in smart supply chain management by digitizing supply chain information. Deloitte (2024) gives the example of the construction industry: "Implementing digital supply chain technologies can allow construction companies to connect with suppliers in real time and can provide greater visibility and control over the supply chain by streamlining internal processes and improving overall efficiency. These proactive approaches can potentially address downtime during disruptions and manage lead time, finances, and customer confidence."

Digital supply chain resilience has become a big business opportunity for consultants, data/AI analysts, and investment advisors. Cybersecurity in supply chains gets boosted by legislation such as the EU's

[57] JRC has developed a synthetic 'digital resilience' indicator which combines information on the state of digital for the personal space, industry, and public space as well as cybersecurity per EU country, but this indicator is not split up by supply chain.

Cyber Resilience Act and US Presidential Executive Orders.

Economic security does not come for free even if there may be a payback in the longer term. Already today budgets put up global competitors to build a domestic ecosystem in semiconductors or green economy run into hundreds of billions. In addition, there are the investments needed to collaborate with third countries such as on critical raw materials. The EU will be challenged to increase the budget for economic security even if digital supply chains may not be the most expensive. Several opportunities exist though. Global Gateway was already mentioned in this report. Another opportunity to explore is Cohesion Funding, as argued by Luc Soete (2024), and Rainer Kattel & Luc Soete (forthcoming).

Finally, and as mentioned repeatedly in this report, public procurement in the EU has only partially been unlocked. It presents an opportunity in several ways: 1) public procurement can prioritise buying European technologies and solutions where these flow from EU-supported innovation and where there is an important public interest, in this case resilience, and there is no breach of WTO rules; this is a Europe-First approach not dissimilar from what the US and China pursue and can facilitated by an update of the EU Procurement Directive,[58] as announced in the Political Guidelines of the European Commission 2024-2029 by EC President Ursula von der Leyen (Ursula von der Leyen, 2024b)[59]; 2) public procurement can be executed jointly at EU level as has been done for COVID-19 vaccines and is proposed for certain critical raw materials, obviously learning from past experience and; 3) public procurement is a natural road into synergies between the civil and military sector who often have a comparable interest in resilience (see e.g., CCDCOE (2022). It will also be important to gain more insight into the impact and possibly trade-distortive effects of public procurement of the US and China.[60]

### *8.2.3 Negative Effects*

#### Costs

Simon J. Evenett & Nicolai Ruge (2024) analyse 16 studies on the costs of increased fragmentation, reshoring, protectionism, decoupling, and derisking. Such economic studies do not result in unanimous views, but generally they conclude that losses for China are larger than for the US and possibly the EU, whereas neutral countries gain most by filling gaps. As an example, the IMF (2023) estimates global GDP losses of up to 2% for moderate fragmentation within which the US suffers a 0.5% GDP loss, the EU and China some 2%. Carlos Góes & Eddy Bekkers (2022) find for a moderate scenario that the US and the EU lose 2% and 2.5% respectively, while China and Russia lose 3.5% and 7% respectively. For more severe fragmentation, the Economist estimates that global losses can be up to 4%, with losses for the US of 1.2% and China of 16.5%. McKinsey (2024a) estimates that economic growth suffers in a strong fragmentation scenario by 6% for China, while the Western group (US, EU, Japan, South Korea), representing 60% of global GDP, will suffer less. Yet, according to another study, a hard decoupling from China would reduce German GDP by 4-5% (Paris Report 2, 2024).

[58] (Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on Public Procurement and Repealing Directive 2004/18/EC Text with EEA Relevance, 2014).

[60] For China see the important inventory of possibly trade-distortive measures, (European Commission, 2024h)

These studies do not, however, factor in all the commercial workarounds to geopolitics, or how 'globalisation evolves in response to geopolitics rather than retrenches'(Simon J. Evenett & Nicolai Ruge, 2024). For instance, if companies see the risk of reduced business in a country due to policy intervention, they often find new markets or deepen existing markets. Australia is a case in point having been able to compensate for import restrictions by China.[61]

While transitioning to a situation of increased resilience, costs may, paradoxically, also be severe disruption in case of retaliation. Furthermore, though evidence is scarce, potentially there may be reduced innovation from increasing resilience. Finally, there may be democratic backlash against large resilience subsidies that go to industry rather than to social causes.

## Inflation

Jiang et al. (2021) argue that heuristic behaviour notably based on probability matching (such as spot-purchasing) and survival seeking behaviour are necessary for a supply chain to be robust against systemic shocks. Tactical behaviour can, however, lead to suboptimal outcomes such as price gouging which can drive up inflation. Giovanni et al. (2022), Tett (2024), and Rubbo (2024) argue that investment in resilience can have an inflationary effect and can wrongfoot government policy based on inflation forecasts that do not take (the lack of) supply chain resilience into account. For instance, studying the effect of the COVID-19 supply chain shock on inflation, Giovanni et al. (2022) show that foreign shocks and global supply chain bottlenecks significantly explain Euro-zone inflation over 2020–2021. Understandably, bottlenecks that manifest themselves during a crisis and then create a supply shocks reduce the effectiveness of stimulating demand by government. As The White House, Council of Economic Advisers (2023) writes "[the] collision of pandemic-induced supply shocks and strong demand for goods generated inflationary pressure across the global economy".

## Excessive Investment and Subsidy Races

As described in section **Error! Reference source not found.**, in the semiconductor sector many countries are mobilising large financial support, with the risk that this leads to subsidy races. The US and EU have agreed in the TTC to at least inform each other of investment support. Nevertheless, one may wonder if the co-existence of EU, US, Chinese, and Indian individual efforts to enhance resilience of their respective digital supply chains can result in anything but subsidy races, investment in inefficient firms, and over-production. A PIIE study warns about this for semiconductors (Chorzempa, 2024). There are reports that much semiconductor investment since 2015 in China has been wasted. Of e-vehicles and other areas it has been said that the world cannot absorb China's surplus production (Ursula von der Leyen, 2024a).

## Too Important to Fail and Freeriding

There is some concern about signalling that governments will step in to maintain resilience (too big to fail, taking advantage of industrial policies) and therefore resilience efforts by companies shift back to

[61] See for instance, Clyde Russell (2023), going as far as stating that "One of the main tools of statecraft in recent years has been trade sanctions or tariffs, but with China taking another step to normalising its trade relationship with Australia, the main lesson is these actions seldom work. In fact, they are more likely to backfire on the nation imposing the trade action, especially if it is unilateral and not supported by significant players in the rest of the international community."

performance (i.e. efficiency) rather than resilience (Deloitte, 2024). At the launch of the US Chips Act, US Secretary of Commerce Raimondo warned industry that the public investments would come with strings attached about delivery (and national security).

## Too Small to Succeed

Paradoxically, investment may also be too small to achieve the policy goals. The US and EU have similar goals in terms of their future market share of advanced semiconductors (20% of the global market by 2030) but investment in the US is three times larger. There is no way that euros deliver three times the bang for the buck.

## Trade Wars, Subsidy Races

As suggested several times before, increasing resilience by trade interventions may well trigger retaliation which can escalate into a trade war. So far, however, this has not happened. Perhaps mutual interdependencies are still too strong?

Subsidy races are a fact, where companies are signalling both that they consider the size of subsidies of competing nations, as well as the ease and speed of getting support. The EU should learn in this respect from the EU Chips Act which was out of the blocks before the US Chips & Science Act, but where the US appeared to be more attractive in putting up larger subsidies, offering easier instruments such as tax incentives and faster in execution. In other areas where there is a limited number of alternative suppliers such as in critical raw materials or a limited capacity to make deals such as for compliance in security specifications, geopolitical races are likewise unfolding. As regards rules and specifications, the EU may have an edge as a first comer in proposing these, assuming that there is a Brussels effect. The EC does actively engage in promoting the Cyber Resilience Act, for instance. Whether on balance this matches the efforts of the USA or China should be very critically assessed, notably as both have an easier ride than the EU in making a richer offering, combining technical specifications with easier market access, a large size of the market, and investment.

## Risk of Failure

A valid question is whether attempts to increase resilience actually work. For instance The Economist (2023b) argues that efforts to curtail Huawei – which were initially motivated by removing risky dependency on Huawei's telecoms equipment – have failed and have triggered domestic substitution, that is, have ultimately lead to a rebound effect. Some interesting scenarios are provided by the IMF (2024): in one scenario in which countries must choose between the US or China – using geopolitical distance as the decision criterion – GDP would drop by about 5% in the worst case, especially in South-East Asia. The IMF assesses that the net effect of reconfiguration of global supply chains may be both loss of efficiency and loss of resilience and anticipates that "geoeconomic fragmentation could intensify, with higher barriers to the flow of goods, capital, and people implying a supply-side slowdown" as well as slowing the pace of innovation. Yet, the IMF also estimates that diversification can reduce GDP losses from large shocks by more than half for the West (IMF, 2022). Baldwin et al. (2023) argue that at the macro level for the US, exposure remains relatively modest, given that over 80% of US industrial inputs are sourced domestically.

The IMF argues that "multilateral cooperation is needed to limit the costs and risks of geoeconomic fragmentation and climate change, speed the transition to green energy, and facilitate debt restructuring." (IMF, 2024)

### Leadership

As a response to potential negative effects, BCG (2024) has a statement that can be generalised beyond chips supply chain: "In a world that is becoming as heavily reliant on chips as on energy, the impact of a potential "black swan" event—such as another global pandemic— would be considerably worse than the near-term externalities of "excess." Confident leadership and communication, by both companies and governments, will be critical." Yet, another manifestation of political leadership is to convince stakeholders that the bigger and long-term picture is more important than short-term financial returns associated with an individual supply chain. For instance, in the EU 'juste retour' is sought regularly in negotiations between Member States, that is, all countries get equally compensated. Of course, that fails for an individual supply chain as these are generally concentrated in a few countries . It can be countered by arguing that there are benefits for all by taking an aggregate view across several supply chains and across several policy areas (industrial, cohesion, etc),resulting in long-term returns in GDP and jobs rather than a one-off boost of capital and jobs. Even if not exclusively, it is certainly a responsibility of the European Commission, the European Parliament, and the President of the European Council to show such leadership. Such leadership should also show capability with respect to the challenges of speed of political decision-making and policy implementation. As argued before, speed matters much when supply sources are scarce and when geopolitical rivals move forward and technology advances very fast. We mentioned the EU starting to fall behind in semiconductor investment, competing for access to mines, and lagging in AI. There is no benchmark for such speed yet but having one may help to step up the urgency for EU international engagement in resilience of digital supply chains.

## 8.3 Global and International Governance

### General

The cases illustrate that the shape of global/international governance for resilience of supply chains is different for each. How this may look in the future in these cases is illustrated in Figure 19. The art of international governance in policymaking and international diplomacy will be to manage a set of such configurations, and potential spill-over of conflicts from one to the other.

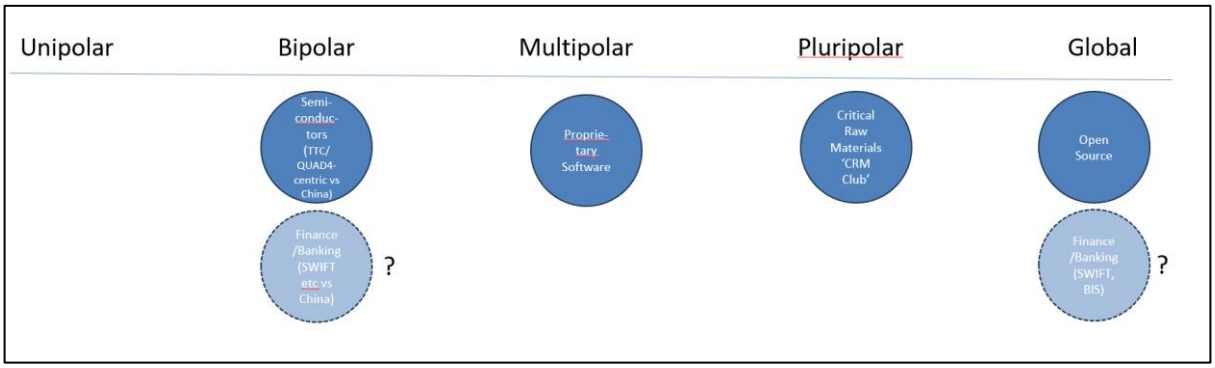



*Figure 19 Possible future global governance*

To illustrate such spillovers: when trade measures are taken, retaliation can happen in a completely different sector, or, in a related sector as long as there is a one-sided dependency. Chinese investment in mining in third countries which ignores respect for human rights, or the environment can trigger sanctions by the West against Chinese banks in the international financial system. This in turn could trigger a cyber-response. Conversely, EU tariffs on Chinese e-vehicles, may trigger Chinese tariffs on EU foodstuff. One of the elements of the art of international governance will be to use the threat of sanctions or retaliation to keep countries moderate in their actions and where possible to continue international dialogue on supply chain resilience.

Mathieu Duchâtel (2024) argues that the issue of extraterritorial reach is not currently covered by an economic security approach, that is, extraterritorial intervention affecting EU companies. An instance of this is the lack of access of inspectors which is relevant for CRA cybersecurity certification. The reverse may also hold, viz. concerns of non-EU semiconductor companies about reporting in case of a crisis on their production to the European Commission as they are required to do by EU Chips Act.

Effective governance must be 'geopolitically aware', meaning that even if there is international collaboration, the realist view on international relations is that self-interest and national security will prevail and is better taken as the starting point.[62] This also holds when seeking collaboration with 'likeminded' countries. As observed by Jacob Mardell (2024) in the context of green policy: "Transatlantic [Critical Materials] policy contains a true contradiction between value creation in partner countries and the goal of onshoring [green] value chains. Despite a rhetorical emphasis on mutually beneficial partnerships, the US and EU's own economic interests are prioritised. This is unsurprising, but in the context of strategic rivalry with China, the EU and US should concentrate on providing a genuinely competitive offer to partner countries." The EU Chips Act can be criticised as not having been well-prepared for geoeconomic response, i.e., a subsidy race with the USA (Timmers, 2022a).

Coming back to the future shape of governance in Figure 19, geopolitical bipolarisation of supply chains may become acceptable for future concentrated products in which the West (US, EU, Japan, South Korea, Taiwan) envisions to have significant control, such as the downstream products in the advanced semiconductors supply chains (e.g., AI-chips based datacentres). It may be less acceptable where there will, likely also in the future, be a great dependency on authoritarian regimes and where these can readily turn to competing buyers, as is the case for CRMs. This also implies that resilience policy must be placed in a wider contact of international economic relations. For instance, Alessia Amighini (2022) observes a lack of linkage between economic security and the EU's Indo-Pacific approach.

Resilience of digital supply chains is an additional topic in the crowded field of global/international governance. On the one hand this can be helpful as there are forums to build upon, whether in trade, security, interoperability, or digital standards, e.g., WTO, UN, ITU, and ISO. On the other hand, none of these has a focused activity on resilience of digital supply chains and it will take time and effort to enhance their agenda, even if they have activities on digital matters that can be closely related (e.g.,

[62] As renowned international relations scholar Joseph Nye recently expressed it: "start as a realist and aspire something better".

WTO/Information Technology Agreement ITA, UN Disarmament/UNODA, ITU/ ITU-Telecommunications, ISO/IEC JTC 1).

Of particular interest could be to link resilience of supply chains to the development of the Global Digital Compact (GDC) by the UN. The GDC is, broadly speaking, about inclusive and sustainable digital cooperation. On the topic of resilience, the GDC seeks commitment to "Invest in and deploy resilient and trustworthy digital infrastructure that provides network coverage to all areas" by 2030 and recognises "that digital public goods, which include open-source software, platforms, data, AI models, standards and content that can be freely used and adapted, empower societies and individuals to direct digital technologies to their development needs. These goods support the development of digital public infrastructure that can deliver services at scale and increase social and economic opportunities for all." GDC commits by 2030 to "Promote the adoption of open standards and interoperability to facilitate the use of digital public goods across different platforms and systems". Clearly, the GDC is strongly linked to the Sustainable Development Goals (SDGs) and promotes the concept of digital public goods, linking it to trust, interoperability, and open standards. All of this may be helpful for to promote global governance of resilience of digital supply chains.

Of course, one can argue that the UN is rather ineffective as it has no enforcement mechanisms in the field of digital supply chains. While true and indeed a frustration in digital diplomacy, the UN can exert some influence. Examples are 1) agenda-setting in international standardisation such as in the ITU; 2) exercising digital supply chain resilience in subfield such as global health, through WTO; 3) developing common norms that underpin cyber-/digital capacity building in development cooperation through UNDP; 4) monitoring as mandated by the UN General Assembly– generally, of course, international law would be a stronger instrument and tends to develop on the basis of practice of behaviour of states (customary international law), even if also then it is not exceptional that international law gets flouted by the 'great powers' –; and 5) UN cooperation in this field can bring leverage in other fields of international relations and vice-versa. Earlier, in this respect, we referred to the art of international governance - or perhaps better, the art of diplomacy.

Supply chains are generally very complex. This makes achieving resilience a daunting venture. Can defensive resilience policy address such a challenge at all? We can learn from cybersecurity. Here the defender is always the underdog, as they must fortify and defend all the attack surface, whereas the attacker only needs to find and exploit one vulnerability. Increasingly then pro-active cyber-defence is exercised. An example is the take-down by the FBI of Volt Typhoon, a massive, long-lasting, and extremely worrying Chinese cyber-infiltration in critical digital infrastructures.

This suggests that in complement to defensive resilience there should be pro-active resilience policy which eliminates dependencies and at the same time reinforces own strengths with a view to creating supply chain dependencies for non-likeminded countries. Certainly, there are differences with cybersecurity. For one, in the world of offensive cyber, the mantra is to keep vulnerabilities of the adversary secret. Using them may be a one-off opportunity, as, once exposed, the adversary would quickly patch that weak spot. However, in supply chains dependencies of the other party would rather be advertised as a deterrent.

In other words, in economic systems such as supply chains and more generally, in trading relationships, one approach could be to ensure that there are mutual interdependencies and with this, economic specialisation that creates efficiencies. This, so international relations theory says, would

allow a balance such that neither party will be inclined to weaponise the dependency as it both risks retaliation and foregoes greater benefits. This would then create the kind of 'properly understood' stability that is desirable for international commerce and trade and conducive to building global governance as a common interest (see also below). This is a more liberalist view on international relations which contrasts with a realist hard-power view. In this thinking it makes sense to develop global norms for (digital) supply chain resilience, cf. Paris Call (2021b) and Paris Call (2021a).

Mutual interdependency theory or complex interdependency theory, advanced by thinkers such as Robert Keohane and Joseph Nye was developed at a time of rising global trade, dismantling of the Soviet Union, and where China was still a small power, and technology less of a geopolitical factor.[63] Recently, however, Joseph Nye, recognizing that geopolitical polarisation and adversity appears to be winning the day, recommended to "start as a realist and aspire something better".

Finally, words matter. The shift in terminology from decoupling as previously often used by the US to derisking as introduced by the EC President (Ursula von der Leyen, 2023) suggests a less confrontational attitude.[64] Likewise, mutual interdependence is less confrontational. This may help reducing supply chain resilience stress.

## International Governance for Supply Chain Resilience

The OECD recommendations on international governance for resilient supply chains (OECD, 2024), argues that international governance is necessary as having "common approaches between governments is paramount in times of crisis when rapid action is essential, as it allows to save time by recognising the conformity assessment carried out by other countries. International regulatory co-operation is important to help harmonise approaches to avoid unnecessary frictions and negative cross-border effects when developing emergency measures. It is also fundamental to increase predictability, foster consistency of policy approaches, and mitigate unnecessary impacts on trade." The OECD recommends four types of international cooperation:

- Co-ordinated efforts among governments, firms, and international organisations to develop common approaches, such as agreements on simplified procedures or adoption of international standards to facilitate the flow of essential goods.
- Recognising conformity assessment procedures – such as testing conducted by partner economies – to facilitate regulatory delivery by expediting administrative procedures.
- Communication and information-sharing to assist sectors in adjusting to changing requirements.
- Promoting the inclusion of chapters on international regulatory cooperation in trade and investment agreements and the conclusion of Mutual Recognition Agreements (MRAs).

[63] The first edition of their influential book Power and Independence was published in 1977. The most recent, fourth edition, in 2011.
[64] Although some Chinese experts recommend China to exploit perceived differences between the EU and US (Geddes, 2023).

International collaboration of states is characterised by realism, strategic ambiguity,[65] loose strategic-tactical linkages, and technocratic continuity conditioned by political volatility. International relations science is rich in theories or perspectives to describe these characteristics (see **Error! Reference source not found.**). These characteristics pose risks for the effectiveness of international collaboration. Often then international collaboration stays light-weight. We have seen an example in the exchange of information on subsidies in semiconductors with the hope to avoid subsidy races. Parties then also likely engage in hedging such as complementing multilateral collaboration with bilateral deals. We have seen an example in supply chains of raw materials. More profound international collaboration is certainly not impossible but in general this must be underpinned by formal agreements. We have seen a supply chain example in the formalised international governance of finance/banking, and in principle (but less in practice) the WTO is such a mechanism too. Though rare, such mechanisms can be truly global too.

The above assumes that international cooperation is state-centric and that there is a large control of the state on companies. From the previous chapter, there is some variation in that respect between

[65] For instance, national security interests will be overriding and fundamentally cannot be the same between countries ('my country first'). This is not spelled out in such agreements but does play out at the implementation level. For examples in tech alliances see (Timmers, 2022b).

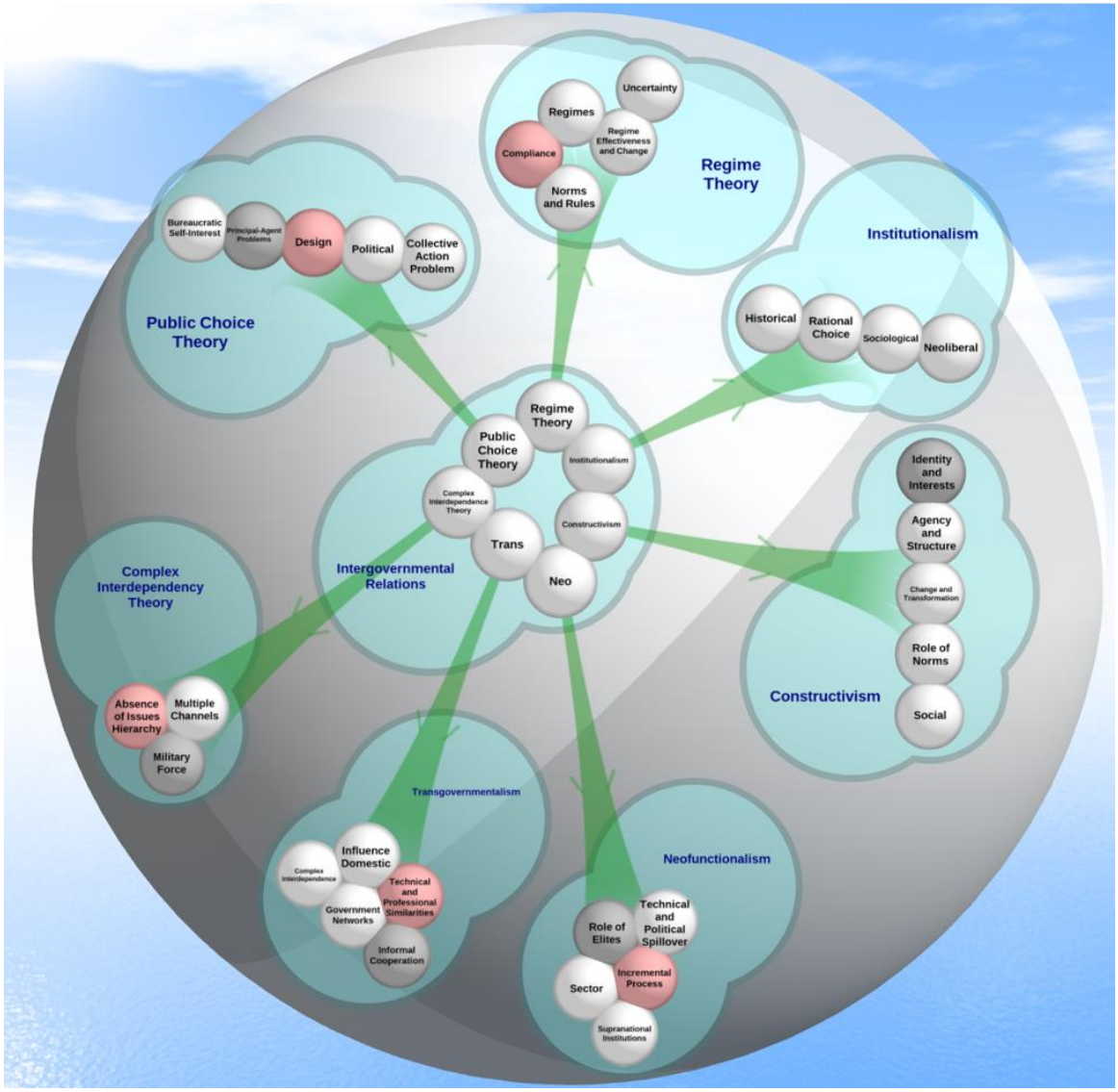



*Figure 20 Theories of intergovernmental relations*

supply chains and between countries. If we can generalise from these cases, we would say that China overall has largest control, followed by the US, and then the EU.

However, we have also seen an alternative, namely, company-centric international cooperation, that is, where supply chain resilience is addressed within an industry or amongst a few dominant companies. In digital supply chains we do not see this happening, not even by 'big tech', due to geopolitical tensions. However, scholars argue that big tech can effectively capture government agendas, also in international cooperation ('governmentalism' as described by Cohen (2019)).

Yet another alternative is (tech) community-centric international cooperation as we see it in software supply chains. Open-source software quality control for resilience does function in practice and is to some extent even truly global.

### Trade Governance

International governance can take many shapes, from broad forums to bilateral agreements. As regards the latter, a particularly important one is free trade. BCG (2024) Illustrates this for semiconductors: “Mainland China is working to ensure its domestic companies have ready access to foreign markets to sell their semiconductor products. Mainland China has bilateral investment agreements with over 100 countries, including many across Europe and Asia. […] The US government has been less active in furthering its trade agenda. It has no active Free Trade Agreement (FTA) negotiations. […] The EU has an active trade policy agenda, with 47 active preferential agreements with 79 trading partners. It also has nine agreements either under negotiation or in the process of being ratified, including with India, South Korea, Indonesia, and Mexico.”

### Information Governance

Critical to supply chain resilience management is proper and shared information on what is the state of the supply chain. On 25 April 2024 the EU adopted the single market emergency instrument (SMEI), to have greater transparency and coordination when a critical situation emerges. This should a.o., maximise the availability of products needed in the crisis response (European Commission, 2022b). Likewise, in the trans-Atlantic setting the EU and US are working towards enhanced information sharing. We have also seen the far-reaching information sharing on vulnerabilities in software supply chains. All these examples require more or less sophisticated forms of information governance. Plenty of cases like these provide important examples, in some cases standards, and in any event lessons to learn for stepping up global information governance. One lesson is that creating a shared information or data infrastructure, brings along its own governance. Such ‘operational’ or ‘technical’ governance can provide a stable basis to develop further common governance for norms and other forms of supply chain coordination, possibly even for crisis coordination (cf., SWIFT). The White House, Council of Economic Advisers (2023) recommends working on improved data availability and data flows within supply chains.

## 8.4 Resilience and Strategic Autonomy

When resilience of supply chains is addressed within the broader context of strategic autonomy, this will also affect the handling of global or international governance. There are 3 + 1 ways to develop strategic autonomy (Timmers, 2022a), namely through:

1. Risk management, based on best-effort according to state-of-the art.
2. Strategic partnerships with likeminded parties.
3. Global cooperation in the common interest.

Autarky or self-sufficiency is the fourth approach. This is pursued by China for the supply chains of a large range of critical technologies, but it is neither possible for all supply chains nor for less powerful countries or regions – such as the EU.

Option 2 can be complemented by strategic and mutual interdependencies with not-likeminded countries. The two-way interdependency, so the theory says, should help to create stability. The likelihood of option 2 is obviously increased by actively seeking cooperation with potentially

likeminded countries. Telling in this respect is, as USTR Katherine Tai remarked, that the EU and US have been settling trade conflicts "so that we can focus on our shared goals and priorities" – read, China relations (USTR, 2023b). In the same spirit free trade agreements can be helpful.

Options 2, 3 and 4 correspond to what Emily Benson (2023) lists in a contribution to the Italian G7 Presidency in 2024, as 'moderate cooperation', 'institutionalized rules via international institutions', and 'each party for itself'. She points out that strategic partnerships or moderate cooperation may run into 'my country first' thinking and therefore likely has its limits to develop into strong global governance.

Based on the geometry of global trade analysis of McKinsey (2024a) two possible scenarios then are:

1. 1) Fragmentation geometry: economies shift their trade to more geopolitically aligned partners, that is, geopolitical distance reduces. This results in larger trade concentration (i.e. trade with fewer countries) but reduces economic growth and increases prices. The McKinsey report argues that trade concentration for the Eastern group (those aligned with China) increases by 70% and economic growth suffers for instance for China by 6%, while the Western group (US, EU, Japan, South Korea), representing 60% of global GDP, will suffer less. For the US and the EU, the report concludes that resilience will increase, probably more in the US than in the EU and with less drag on growth in the US than in the EU.

2. 2) Diversification geometry: diversification of trade relationships so that no economy is highly dependent on another. In this scenario, geopolitical distance increases by 3%, i.e., geopolitical risks increase. In particular, for China, import concentration would rise (e.g., closer ties to Russia). Overall resilience decreases.

Mapping these two scenarios on the governance options above: fragmentation economy corresponds to option 2, whereas diversification economy corresponds to option 1, or in some cases to option 3.

The implication for global governance is to seek alignment between business strategies and government policies: the choice of scenarios or approaches is determined by governmental policies. It would be inconsistent if governments drive for strategic partnerships and business diversifies suppliers at their will. Conversely, business can argue that stockpiling is necessitated by geopolitical or other international developments (such as climate change) and that therefore stockpiling is a public common interest, requiring government support – in the first case under option 2, i.e. with support from likeminded countries and in the second case under option 3, i.e. with global support.

As will be clear from earlier analysis, China has systematically over decades pursued an autarkic strategic autonomy approach in many areas, setting clear priorities, systematically combining internal and external policies. Examples of internal policies are the support of domestic companies and state-owned enterprises, import substitution, public procurement, domestic supply prescription to manufacturers, massive education and skills programs, digitisation of finance and supply chains, promotion of military-civil linkages, etc. Examples of external policies are foreign investment under the Belt and Road initiative, shareholding and acquisition of mining operations in Congo and Latin-America and of critical technology companies in Europe, engagement in international standardisation, or intellectual property theft. China's economic approach has been framed by President Xi Jinping as

'dual circulation', consisting of a domestic and an international cycle, with primacy for the domestic market.

China has been consistent in pursuing control. This now pays off with a strong hold on many supply chains. Moreover, tensions over political differences between the liberal democracies and authoritarian China continue to rise. There seems to be little room – geoeconomically and geopolitically – for the EU to cooperate with China on resilience of digital supply chains. Nevertheless, some China experts argue that the EU has certain strengths to arrange for mutual interdependency or at least a high cost for China to retaliate (Tim Rühlig, 2024). EU strengths are in research and innovation, regulation, technologies such as wireless connectivity, semiconductor lithography, space exploration, genomic data, and quantum sensing.

For about a decade, the US government has started to engage increasingly in economic security and strategic autonomy. With its massive resources and extensive control of key digital technologies, the financial system, military-civil linkages, and large domestic market, the USA is in a strong position to go for autarky in many supply chains, but still needs partners internationally, both political allies and other third countries.

It is not clear where the US will be moving in the future, but shared across the political spectrum is instrumentalist thinking about international governance, as a means to an end, namely, America's economic and national security. This does not exclude EU-US cooperation in international governance for resilience of digital supply chains, but it is nevertheless important to understand the difference in mindset with the EU. For the EU institutions, multilateralism is fundamental; it is in the EU's DNA and the basis of the EU Treaties. The EU cannot 'just' move over to instrumentalism as that would risk putting in question the very international cooperation of Member States that the EU is based on. Yet, the EU must have an answer to instrumentalism, a challenge that will become even more pressing when isolationists win the day as an outcome of US elections.

Next to the questions about the EU's capabilities and capacities, this is another instance that illustrates that international governance of resilience of digital supply chains raises fundamental questions about the EU's institutional and foundational legitimacy. It touches the heart of EU sovereignty.

# 9. Conclusions and Policy Recommendations

**Chapter Summary**

EU institutions, EU Member States, and EU industry can play a major role in promoting global/international governance in digital supply chain resilience.

This chapter provides a set principles for policy and strategy in the EU for global/international governance for resilience in digital supply chains, followed by recommendations. Each recommendation is intended for specific parties and illustrated with actions without seeking to be exhaustive. Most recommendations hold for any digital supply chains, with case-specific detail added.

## 9.1 Conclusions

With a systematic approach to analysing digital supply chain resilience and related governance and learning lessons from major cases it is possible to propose concrete ways forward to advance resilience through global/international governance. There is no one-size-fits-all. Any approach to governance for resilience must be anchored in the broader policy settings for economic security and strategic autonomy. The EU institutions, EU Member States, and EU industry have strong assets to bring to the international table. Yet, clear vision, the art of diplomacy, and a strong dose of realism will be needed for the EU to manage the challenging geopolitics and geoeconomics of the different types of global/international governance for digital supply chain resilience.

## 9.2 Principles

EU involvement in global/international governance for digital supply chain resilience should be based on the following principles:

- ***Decisiveness and leadership*** answering the need for speed. Global rivals move fast. With a limited number of suppliers, first-comers win. At EU level there must be political leadership which includes leading in timely decision-making and responsible risk taking.
- ***Comprehensive and consistent*** mobilisation of all policy instruments, in a holistic way, from internal market access regulation to investment, employment policy to trade agreement, back-to-back civil – defence innovation and procurement, and internal to external (foreign) policies.
- ***Win-win and mutual interdependency*** with suppliers, co-developers, customers from across the world. This should aim to enable value creation for all from economic specialisation and to deter from the weaponisation of supply chains.
- ***Realism and flexibility***, where the EU cannot, should not, and does not need to claim leadership in all technologies and supply chains, it should rather be selective, nurturing like-mindedness and interdependency in the long run while accepting that today there are trade-offs for EU resilience such as on labour and environmental conditions in third countries.

- ***Anticipation, pro-activeness, and deepening***: policy must be able to respond and anticipate, to be geopolitically aware, technology-aware, and society-aware.

## 9.3 Recommendations

The recommendations below are accompanied by concrete action. These are not intended to be exhaustive. Rather they should inspire policy makers and strategists in EU institutions, Member States, and industry to act.

1. Consistently advance and focus on **integrated policy for digital supply chains resilience**:

    a. EC/EEAS to put forward a realistic strategy in the form of a joint Communication for digital supply chains resilience, joining up digital, green, industrial (R&D, skills, investment, EU-internal supplier industries-user industries partnering e.g., in automotive, energy, medical devices, defence and space), market access, corporate due diligence, trade and foreign policies. This should be based on lessons from the integrated policy approach of US and China in semiconductors and CRMs and from the EU in CRMs. This Communication should provide the policy embedding of resilience and economic security within open strategic autonomy.

    b. EC to provide a list of digital supply chains, prioritised on criticality and feasibility to act. This should use the EC (JRC) open strategic autonomy assessment (Kroll, 2024) (see also (Tim Ruehlig et al, 2023)) and list of key technologies in the EU economic security policy. For technologies, the consideration should be to focus more on emerging technology areas rather than catching up.

2. Promote **win-win global/international cooperation for digital supply chains resilience**:

    a. EC/EEAS to rapidly move forward with realistic win-win projects that fully mobilise the Global Gateway in the EU-US led Minerals Security Partnership (MSP) Forum of resource-rich and consuming countries for secure and sustainable supply of critical raw materials. Generally, lessons should be learned from EU economic security policy in critical minerals as the most developed case of a comprehensive and internationally oriented policy, which moreover is likely to be extended by the new European Commission.[66]

    b. EC/EEAS to propose a similar approach in digital supply chains, both technological (AI, software, semiconductors, IoT, 5G/6G, etc.) and sectoral (logistics, manufacturing, health, etc.) to coordinate on supply shortages, enable specialisation, and pre-empt trade and subsidy wars and weaponisation of digital supply chains.

3. **Mobilise public procurement**:

[66] The Political Guidelines for the new Commission announce Clean Trade and Investment Partnerships and a Circular Economy Act, (Ursula von der Leyen, 2024b).

a. EC to update the Public Procurement Directive[67] to enable Europe-First and EU joint procurement for digital supply chains resilience where this promotes resilience and strategic autonomy (quantum, AI and cybersecurity, advanced semiconductors, drones, and 6G) and issue a related Recommendation to unlock Cohesion Funds for economic security.[68]

b. Member States to include digital supply chains resilience in their public procurement and promote this by combining civil and military public procurement.

4. **Lead in a global community approach to digital supply chains resilience**:

   a. EC/EEAS to take the lead in cooperation for software supply chain resilience, leveraging cyber-cooperation of Member States and European open-source communities and associations; and with US and OECD promote standards for open-source security certification and more generally standards for digital supply chains resilience.

   b. EC and industry to set up an 'International Reserve' of experts on digital supply chains resilience to assist individual companies in their digital supply chains resilience.[69]

   c. EEAS and EU Member States to promote norms and confidence-building measures for resilience of digital supply chains in the UN Global Digital Compact.

5. **Advance monitoring of international governance in digital supply chains resilience**:

   a. EC, EU Member States and industry to form a resilience monitoring group to critically assess international governance of digital supply chains resilience on the basis of indicators and qualitative criteria such as policy synergies, best practice learning in global governance.

   b. EC to set up a Digital Supply Chains Resilience Lab for public-private-civil society partnerships among allies, fostering innovation and shared supply chain data infrastructures.

   c. EEAS/EC to develop governance strategies for digital supply chain resilience and benchmark policymaking speed relative to the US, China, India and others, supporting EU engagement in international governance and diplomacy.

6. **Advance understanding and long-term strategic thinking**:

[67] Dating from 2014: (Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on Public Procurement and Repealing Directive 2004/18/EC Text with EEA Relevance, 2014). The Political Guidelines, see footnote above, announce an update.
[68] Further detail on the promising role of Cohesion Funds is expected to be published shortly.
[69] This Reserve can learn from the Cybersecurity Reserve as being established following the adoption of the Cyber Solidarity Act.

a. EC (JRC) with OECD and industry to develop supply chain resilience metrics and supply chain modelling and where appropriate propose these for international standardisation.

b. EC (JRC)/EEAS to set up a Digital Supply Chains Resilience Expertise Centre; exercise scenarios that consider both the cost of a break in resilience and the likelihood or risk of a break of resilience including geopolitical risks.

c. Industry and academia to simulate the interplay of international governance and supply chain structure and dynamics in order to understand the limits of mutual interdependence such as in semiconductors, incentives for resilience in open-source communities, and systemic or cascading resilience risks in coupled supply chains such as energy and telecoms.

# References

Accenture. (2022, April 28). *Accenture Research Finds Four in Five Banks Planning to or Already Migrating Mainframes to the Cloud Are Doing So Quickly*. https://newsroom.accenture.com/news/2022/accenture-research-finds-four-in-five-banks-planning-to-or-already-migrating-mainframes-to-the-cloud-are-doing-so-quickly

Acemoglu, D., & Tahbaz-Salehi, A. (2024). The Macroeconomics of Supply Chain Disruptions. *Review of Economic Studies*, rdae038. https://doi.org/10.1093/restud/rdae038

Aguila, J. O., & ElMaraghy, W. (2019). Supply chain resilience and structure: An evaluation framework. *Procedia Manufacturing*, *28*, 43–50. https://doi.org/10.1016/j.promfg.2018.12.008

Antonia Hmaidi. (2024, March 4). *China's long-term struggle to become integral in semiconductor supply chains | Merics*. https://merics.org/en/comment/chinas-long-term-struggle-become-integral-semiconductor-supply-chains

Baldwin, R., Freeman, R., & Theodorakopoulos, A. (2023). *Hidden Exposure: Measuring US Supply Chain Reliance* (Working Paper 31820). National Bureau of Economic Research. https://doi.org/10.3386/w31820

BCG. (2024, May 7). *Emerging Resilience in the Semiconductor Supply Chain*. BCG Global. https://www.bcg.com/publications/2024/emerging-resilience-in-semiconductor-supply-chain

Bellamy, M. A., & Basole, R. C. (2013). Network analysis of supply chain systems: A systematic review and future research. *Systems Engineering*, *16*(2), 235–249. https://doi.org/10.1002/sys.21238

Bert Hubert. (2023, December 30). *EU CRA: What does it mean for open source?* Bert Hubert's Writings. https://berthub.eu/articles/posts/eu-cra-what-does-it-mean-for-open-source/

Boston Consulting Group & Semiconductor Industry Association. (2021). *Strengthening the Global Semiconductor Supply Chain in an Uncertain Era | BCG*. https://www.bcg.com/publications/2021/strengthening-the-global-semiconductor-supply-chain

Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*.

Bureau of Industry and Security, US Dept of Commerce. (2024). *Entity List*. https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list

Carlos Góes & Eddy Bekkers. (2022). *The Impact of Geopolitical Conflicts on Trade, Growth, and Innovation* (WTO Working Papers) [WTO Working Papers]. https://doi.org/10.30875/25189808-2022-9

Carrara, S., Bobba, S., Blagoeva, D., Alves, D. P., Cavalli, A., Georgitzikis, K., Grohol, M., Itul, A., Kuzov, T., Latunussa, C., Lyons, L., Malano, G., Maury, T., Prior, A. A., Somers, J., Telsnig, T., Veeh, C., Wittmer, D., Black, C., … Christou, M. (2023). *Supply chain analysis and material demand forecast in strategic technologies and sectors in the EU – A foresight study*. https://doi.org/10.2760/386650

CCDCOE. (2022). *Military Movement Risks From 5G Networks*. https://ccdcoe.org/library/publications/research-report-military-movement-risks-from-5g-networks/

Center for Strategic and International Studies (CSIS). (2024). *Investing in Leading-Edge Technology: An Update on CHIPS Act Implementation"*.

CERRE (Pascal Lamy, Bruno Liebhaberg et al). (2022). *Global Governance for the Digital Ecosystems | CERRE*. CERRE. https://cerre.eu/publications/global-governance-for-the-digital-ecosystems/

Chorzempa, M. (2024, June 10). *The US and Korean CHIPS Acts are spurring investment but at a high cost | PIIE*. https://www.piie.com/blogs/realtime-economics/2024/us-and-korean-chips-acts-are-spurring-investment-high-cost

Chu, A. (2024, February 13). Chinese-backed solar factory stirs suspicions in rural Ohio. *Financial Times*. https://www.ft.com/content/38e29526-d4ef-4ab8-92c0-6eb2e3aba157

CISA. (2024, February 7). *CISA and Partners Release Advisory on PRC-sponsored Volt Typhoon Activity and Supplemental Living Off the Land Guidance | CISA*. https://www.cisa.gov/news-events/alerts/2024/02/07/cisa-and-partners-release-advisory-prc-sponsored-volt-typhoon-activity-and-supplemental-living-land

Claburn, T. (2024, April 1). *Malicious xz backdoor reveals fragility of open source*. https://www.theregister.com/2024/04/01/xz_backdoor_open_source/

Clyde Russell. (2023, August 7). *Live and don't learn. The lesson of China's failed Australia trade bans | Reuters*. https://www.reuters.com/markets/commodities/live-dont-learn-lesson-chinas-failed-australia-trade-bans-russell-2023-08-07/

Cohen, J. E. (2019). *Between truth and power: The legal constructions of informational capitalism*.

Cornish, C., & Wiggins, K. (2024, February 9). Abu Dhabi AI group G42 sells its China stakes to appease US. *Financial Times*. https://www.ft.com/content/82473ec4-fa7a-43f2-897c-ceb9b10ffd7a

Council of the European Union. (2022, October 17). *The Council agrees to strengthen the security of ICT supply chains*. https://www.consilium.europa.eu/en/press/press-releases/2022/10/17/the-council-agrees-to-strengthen-the-security-of-ict-supply-chains/

Council of the European Union. (2024, March 18). *Critical raw materials act*. Consilium. https://www.consilium.europa.eu/en/press/press-releases/2024/03/18/strategic-autonomy-council-gives-its-final-approval-on-the-critical-raw-materials-act/

Cowhey, P. F., & Aronson, J. D. (2017). *Digital DNA: Disruption and the Challenges for Global Governance*. Oxford University Press.

Crisanto, J. C., Ehrentraud, J., Fabian, M., & Monteil, A. (2022). *Big tech interdependencies – a key policy blind spot*. https://www.bis.org/fsi/publ/insights44.htm

Davies, C. (2024, June 9). The graphite fight: US tariffs trigger race to build non-Chinese supply chain | Financial Times. *Financial Times*. https://www.ft.com/content/9117e5e6-baf9-4bdf-8080-9aa019ef1bfc

De Filippi, P., & Wright, A. (2020). Primavera De Filippi and Aaron Wright, Blockchain and the Law: The Rule of Code, Cambridge, Mass: Harvard University Press, 2018, 312 pp, hb £28.95. *The Modern Law Review*, *83*(1), 233–236. https://doi.org/10.1111/1468-2230.12459

Deloitte. (2024, May 23). *Restructuring the supply base: Prioritizing a resilient, yet efficient supply chain*. Deloitte Insights. https://www2.deloitte.com/us/en/insights/industry/manufacturing/global-supply-chain-resilience-amid-disruptions.html

Dempsey, H., & Wilson, T. (2024, July 5). US intervened in Congo mine sale to Chinese arms group. *Financial Times*. https://www.ft.com/content/4c5faaa4-d041-4f58-b9ef-ca84f074009d

Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on Public Procurement and Repealing Directive 2004/18/EC Text with EEA Relevance, CONSIL, EP, 094 OJ L (2014). http://data.europa.eu/eli/dir/2014/24/oj/eng

Elder, B. (2024, February 5). 'Sell Nvidia'. *Financial Times*. https://www.ft.com/content/e1beb7a5-6c91-4d7f-bc90-79689774881d

Emily Benson. (2023, December 21). Broken Value Chains. *ISPI*. https://www.ispionline.it/en/publication/broken-value-chains-158071

ESIA & SIA. (2022). *ESIA / SIA Joint Position on "Guiding Principles for EU-U.S. Semiconductor Standardisation Cooperation*. https://www.eusemiconductors.eu/sites/default/files/uploads/20220509_GuidingPrinciplesforUS-EUSemiStandardisationCooperation.pdf

EU and US. (2024, April 5). *U.S-EU Joint Statement of the Trade and Technology Council*. The White House. https://www.whitehouse.gov/briefing-room/statements-releases/2024/04/05/u-s-eu-joint-statement-of-the-trade-and-technology-council-3/

EU and USA. (2023, April 28). *Declaration for the Future of the Internet* [Text]. European Commission - European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2695

European Commission. (2022a). *European Chips Act: Staff Working document | Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/library/european-chips-act-staff-working-document

European Commission. (2022b, September 19). *Single market emergency instrument—European Commission*. https://single-market-economy.ec.europa.eu/single-market/single-market-emergency-instrument_en

European Commission. (2023a). *A secure and sustainable supply of critical raw materials in support of the twin transition*. https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52023DC0165

European Commission. (2023b). *Commission Recommendation (EU) 2023/2113 of 3 October 2023 on critical technology areas for the EU's economic security for further risk assessment with Member States*. http://data.europa.eu/eli/reco/2023/2113/oj/eng

European Commission. (2023c, March 16). *Study on the Critical Raw Materials for the EU 2023—Final Report—European Commission*. https://single-market-economy.ec.europa.eu/publications/study-critical-raw-materials-eu-2023-final-report_en

European Commission. (2023d, June 20). *An EU approach to enhance economic security* [Text]. European Commission - European Commission. https://ec.europa.eu/commission/presscorner/detail/en/IP_23_3358

European Commission. (2024a, January 24). *WHITE PAPER on Outbound Investments, COM/2024/24 final* [Website]. Publications Office of the EU; Publications Office of the European Union. https://op.europa.eu/en/publication-detail/-/publication/061d9f0d-bb7b-11ee-b164-01aa75ed71a1/language-en

European Commission. (2024b, January 26). *New tools to reinforce the EU's economic security—European Commission*. https://commission.europa.eu/news/new-tools-reinforce-eus-economic-security-2024-01-24_en

European Commission. (2024c, February 2). *Commission publishes its Annual Union Work Programme on European Standardisation for 2024—European Commission*. https://single-market-economy.ec.europa.eu/news/commission-publishes-its-annual-union-work-programme-european-standardisation-2024-2024-02-02_en

European Commission. (2024d, February 14). *The 2024 Annual Single Market and Competitiveness Report—European Commission*. https://single-market-economy.ec.europa.eu/publications/2024-annual-single-market-and-competitiveness-report_en

European Commission. (2024e, February 27). *Advanced Materials for Industrial Leadership—European Commission*. https://research-and-innovation.ec.europa.eu/research-area/industrial-research-and-innovation/key-enabling-technologies/chemicals-and-advanced-materials/advanced-materials-industrial-leadership_en

European Commission. (2024f, April). *Corporate sustainability due diligence—European Commission*. https://commission.europa.eu/business-economy-euro/doing-business-eu/corporate-sustainability-due-diligence_en

European Commission. (2024g, April 3). *Commission opens two in-depth investigations under the Foreign Subsidies Regulation in the solar photovoltaic sector | Public Buyers Community*. https://public-buyers-community.ec.europa.eu/news/commission-opens-two-depth-investigations-under-foreign-subsidies-regulation-solar

European Commission. (2024h, April 10). *Commission updates report on state-induced distortions in China's economy—European Commission*. https://policy.trade.ec.europa.eu/news/commission-updates-report-state-induced-distortions-chinas-economy-2024-04-10_en

European Commission & U.S. National Security Agency. (2024, January 31). *EU-US Joint Statement on CyberSafe Products Action Plan*. https://digital-strategy.ec.europa.eu/en/library/eu-us-joint-statement-cybersafe-products-action-plan

Executive Office of the President. (2021, May 17). *Improving the Nation's Cybersecurity*. Federal Register. https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

Farrell, H., & Newman, A. (2023a). *Underground Empire: How America Weaponized the World Economy*. Henry Holt and Co.

Farrell, H., & Newman, A. (2023b, October 19). The New Economic Security State. *Foreign Affairs*, *102*(6). https://www.foreignaffairs.com/united-states/economic-security-state-farrell-newman

Farrell, H., & Newman, A. L. (2019). Weaponized Interdependence: How Global Economic Networks Shape State Coercion. *International Security*, *44*(1), 42–79. https://doi.org/10.1162/isec_a_00351

FCC. (2023, September). *FCC Proposes Cybersecurity Labeling Program for Smart Devices | Federal Communications Commission*. https://www.fcc.gov/consumer-governmental-affairs/fcc-proposes-cybersecurity-labeling-program-smart-devices

Federal Reserve Bank of New York. (2024). *Global Supply Chain Pressure Index*. https://www.newyorkfed.org/research/policy/gscpi#/interactive

Flaningam, E. (2023, May 27). *An Overview of the Semiconductor Industry*. https://www.generativevalue.com/p/an-overview-of-the-semiconductor?utm_medium=reader2

Foroohar, R. (2023, March 13). The rare earths race entails difficult choices | Financial Times. *Financial Times*. https://www.ft.com/content/94802287-2b26-47cf-a94f-cc542fca0a01

Foroohar, R. (2024, February 25). The global trade system is in desperate need of an overhaul. *Financial Times*. https://www.ft.com/content/416671be-4d0d-4a43-8119-b3638589c6b9

Francesco Findeisen & Yann Wernert. (2023). *Meeting the costs of resilience: The EU's Critical Raw Materials Strategy must go the extra kilometer | Hertie School Jacques Delors Centre*. https://www.delorscentre.eu/en/publications/eu-critical-raw-materials

FTI. (2023, December 23). *Chinas Export Controls on Critical Minerals | FTI*. https://www.fticonsulting.com/insights/articles/chinas-export-controls-critical-minerals-gallium-germanium-graphite

G7. (2023, May). *G7 Leaders Statement on Economic Resilience and Economic Security*. https://www.consilium.europa.eu/media/64501/g7-statement-on-economic-resilience-and-economic-security.pdf

G7. (2024, March 14). *G7-Industry-Tech-and-Digital-Ministerial-Declaration*. https://www.g7italy.it/wp-content/uploads/G7-Industry-Tech-and-Digital-Ministerial-Declaration-Annexes-1.pdf

G7 Italia. (2024, June 15). *Documents | G7 Italia*. G7 Italia 2024. https://www.g7italy.it/en/documents

Geddes, T. des G. (2023, July 11). *De-Risking as Viewed from China*. https://www.sinification.com/p/de-risking-as-viewed-from-china

Giovanni, J. di, Kalemli-Özcan, Ş., Silva, A., & Yildirim, M. A. (2022). *Global Supply Chain Pressures, International Trade, and Inflation* (1024; Federal Reserve Bank of New York Staff Reports). https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr1024.pdf?sc_lang=en

GMF. (2024, June 7). *The GMF Tech Semiconductor Investment Tracker | German Marshall Fund of the United States*. https://www.gmfus.org/gmf-tech-semiconductor-investment-tracker

Habibi, F., Chakrabortty, R. K., & Abbasi, A. (2023). Evaluating supply chain network resilience considering disruption propagation. *Computers & Industrial Engineering*, *183*, 109531. https://doi.org/10.1016/j.cie.2023.109531

Hancock, A., & Wilson, T. (2024, May 21). Mining industry sceptical of EU joint purchasing plan for critical minerals. *Financial Times*. https://www.ft.com/content/26f25251-0d6b-4a0a-a7b5-2d515242b0f3

Hijink, M. (2023). *Focus: De wereld van ASML - De wereld van ASML - Marc Hijink*. https://www.uitgeverijbalans.nl/boeken/focus-de-wereld-van-asml/

Hmaidi, A. (2023). *"Here to stay" – Chinese state-affiliated hacking for strategic goals | Merics*. MERICS. https://merics.org/en/report/here-stay-chinese-state-affiliated-hacking-strategic-goals

Hoek, R. V., & Lacity, M. (2023, November 21). How Global Companies Use AI to Prevent Supply Chain Disruptions. *Harvard Business Review*. https://hbr.org/2023/11/how-global-companies-use-ai-to-prevent-supply-chain-disruptions

IBM & Microsoft. (2024). *All supply chains are digital*.

IEA. (2023). *Recommendations for the G7 – The State of Clean Technology Manufacturing – Analysis*. IEA. https://www.iea.org/reports/the-state-of-clean-technology-manufacturing/recommendations-for-the-g7

IEEE Spectrum. (2024, July 2). *EV Motors Without Rare Earth Permanent Magnets—IEEE Spectrum*. https://spectrum.ieee.org/ev-motor

Igan, D., Rungcharoenkitkul, P., & Takahashi, K. (2022). *Global supply chain disruptions: Evolution, impact, outlook*. https://www.bis.org/publ/bisbull61.htm

Ilias Chantzos. (2024, May 29). *DORA vs. GDPR. Part I: Loose ends and four pillars*. https://www.broadcom.com/blog/dora-vs-gdpr-part-i-loose-ends-and-four-pillars

IMF. (2022, April). *World Economic Outlook, April 2022: War Sets Back The Global Recovery*. IMF. https://www.imf.org/en/Publications/WEO/Issues/2022/04/19/world-economic-outlook-april-2022

IMF. (2023, April). *World Economic Outlook, April 2023: A Rocky Recovery*. IMF. https://www.imf.org/en/Publications/WEO/Issues/2023/04/11/world-economic-outlook-april-2023

IMF. (2024, April). *World Economic Outlook, April 2024: Steady but Slow: Resilience amid Divergence*. IMF. https://www.imf.org/en/Publications/WEO/Issues/2024/04/16/world-economic-outlook-april-2024

International Energy Agency. (2022, July). *Solar PV Global Supply Chains – Analysis*. IEA. https://www.iea.org/reports/solar-pv-global-supply-chains

ISPI. (2024a). The World in 2024: The Great Fragmentation. *ISPI*. https://www.ispionline.it/en/the-world-in-2024-the-great-fragmentation

ISPI. (2024b, May 27). Logistics in Transition. Exploring Geopolitical, Economic, and Technological Trends. *ISPI*. https://www.ispionline.it/en/publication/logistics-in-transition-exploring-geopolitical-economic-and-technological-trends-174643

ITIF. (2021, February 24). *ITIF Welcomes Executive Order Reviewing Critical Supply Chains | ITIF*. https://itif.org/publications/2021/02/24/itif-welcomes-executive-order-reviewing-critical-supply-chains/

Jacob Mardell. (2024). *Transatlantic Strategy on Critical Raw Materials | Heinrich Böll Stiftung | Washington, DC Office—USA, Canada, Global Dialogue*. https://us.boell.org/en/2024/03/06/transatlantic-strategy-critical-raw-materials

Jake Sullivan. (2022, October 13). *Remarks by National Security Advisor Jake Sullivan on the Biden-Harris Administration's National Security Strategy*. The White House. https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/10/13/remarks-by-national-security-advisor-jake-sullivan-on-the-biden-harris-administrations-national-security-strategy/

Jake Sullivan. (2023, April 27). *The Biden administration's international economic agenda: A conversation with National Security Advisor Jake Sullivan | Brookings*. Brookings. https://www.brookings.edu/events/the-biden-administrations-international-economic-agenda-a-conversation-with-national-security-advisor-jake-sullivan/

Janeway, W. H. (2024, May 17). *The Rise of Mesoeconomics | by William H. Janeway*. Project Syndicate. https://www.project-syndicate.org/onpoint/mesoeconomics-study-of-networks-supply-chains-key-to-successful-industrial-policies-by-william-h-janeway-2024-05

Jean Pisani-Ferry, Beatrice Weder di Mauro, & Jeromin Zettelmeyer (Eds.). (2024). *Paris report 2: Europe's economic security*. https://www.bruegel.org/external-publication/paris-report-2-europes-economic-security

Jiang, B., Rigobon, D. E., & Rigobon, R. (2021). *From Just in Time, to Just in Case, to Just in Worst-Case: Simple models of a Global Supply Chain under Uncertain Aggregate Shocks.* (Working Paper 29345). National Bureau of Economic Research. https://doi.org/10.3386/w29345

John Seaman, Florian Vidal and Raphaël Danino-Perraud. (2024). Critical Raw Materials: What Chinese Dependencies, what European Strengths? In Tim Ruhlig (Ed.), *Making Europe's Digital Technological Strengths Indispensable To China*.

JRC. (2023a, March 16). *Solutions for a resilient EU raw materials supply chain*. https://joint-research-centre.ec.europa.eu/jrc-news/solutions-resilient-eu-raw-materials-supply-chain-2023-03-16_en

JRC. (2023b, July 6). *2023 Strategic Foresight Report—European Commission*. https://commission.europa.eu/strategy-and-policy/strategic-planning/strategic-foresight/2023-strategic-foresight-report_en

Kaur, D. (2023, February 28). *Chip 4 Alliance: Senior officials finally meet to discuss semiconductor supply chain*. Tech Wire Asia. https://techwireasia.com/02/2023/chip-4-alliance-the-first-meeting-of-senior-officials-finally-transpired/

Koh, T. Y., & Prenio, J. (2023). *Managing cloud risk – some considerations for the oversight of critical cloud service providers in the financial sector*. https://www.bis.org/fsi/publ/insights53.htm

KPMG. (2023, February 16). *Unpicking China's Financial Services resilience—KPMG Global*. KPMG. https://kpmg.com/xx/en/home/insights/2021/03/unpicking-chinas-financial-services-resilience.html

Kroll, H. (2024, January 4). *Assessing Open Strategic Autonomy | JRC*. JRC Publications Repository. https://doi.org/10.2760/767279

Langley, W., & Ho-him, C. (2024, June 9). European companies step up efforts to decouple from China | Financial Times. *Financial Times*. https://www.ft.com/content/fb448978-e4ff-4f3e-b650-13fda73f58a9

Le Grand, J. (2003). *Motivation, Agency, and Public Policy: Of Knights and Knaves, Pawns and Queens*. Oxford University Press. https://doi.org/10.1093/0199266999.001.0001

Li, L., Tabeta, S., & Ting-Fang, C. (2024, May 22). China asks carmakers to use up to 25% local chips by 2025 | Financial Times. *Financial Times*. https://www.ft.com/content/98a50ed8-1265-4f31-986f-6c874bc815f0

Maillart, T., Zhao, M., Grossklags, J., & Chuang, J. (2017). Given enough eyeballs, all bugs are shallow? Revisiting Eric Raymond with bug bounty programs. *Journal of Cybersecurity*, *3*(2), 81–90. https://doi.org/10.1093/cybsec/tyx008

Martins, L. (2023, December 6). Best practice alignment for supply chain security across standards and regulatory frameworks | Tech Accord. *Cybersecurity Tech Accord*. https://cybertechaccord.org/best-practice-alignment-for-supply-chain-security-across-standards-and-regulatory-frameworks/

Masters, B., & Edgecliffe-Johnson, A. (2021, December 20). Supply chains: Companies shift from 'just in time' to 'just in case' | Financial Times. *Financial Times*. https://www.ft.com/content/8a7cdc0d-99aa-4ef6-ba9a-fd1a1180dc82

Mat Honan & James O'Donnell. (2024, April 1). *How ASML took over the chipmaking chessboard – MIT Technology Review*. https://www.technologyreview.com/2024/04/01/1090393/how-asml-took-over-the-chipmaking-chessboard/

Mathieu Duchâtel. (2024, April). *Demystifying Economic Security: A Framework for the EU*. Institut Montaigne. https://www.institutmontaigne.org/en/publications/demystifying-economic-security-framework-eu

McKinsey. (2024a). *Geopolitics and the geometry of global trade | McKinsey*. https://www.mckinsey.com/mgi/our-research/geopolitics-and-the-geometry-of-global-trade

McKinsey. (2024b, May). *The CHIPS and Science Act: What is it and what is in it? | McKinsey*. https://www.mckinsey.com/industries/public-sector/our-insights/the-chips-and-science-act-heres-whats-in-it

MERICS. (2021, May 19). *China bets on open-source technologies to boost domestic innovation | Merics*. https://merics.org/en/report/china-bets-open-source-technologies-boost-domestic-innovation

Michael E. Porter. (1990). *The Competitive Advantage of Nations*. https://hbr.org/1990/03/the-competitive-advantage-of-nations

Miller, C. (2022). *Chip War*. Scribner. https://www.christophermiller.net/semiconductors-1

Mui, C. (2024, February 5). *Washington shores up friends in the global chip war*. POLITICO. https://www.politico.com/newsletters/digital-future-daily/2024/02/05/washington-shores-up-friends-in-the-global-chip-war-00139698

Murphy, B. (2022, May). Chokepoints—China's Self-Identified Strategic Technology Import Dependencies. *Center for Security and Emerging Technology*. https://cset.georgetown.edu/publication/chokepoints/

Naughton, B. (2021). *The rise of China's industrial policy 1978 to 2020*.

News, B. (2019, May 17). *Huawei Built At Least a Three-Month Stockpile Ahead of Trump Ban—BNN Bloomberg*. BNN. https://www.bnnbloomberg.ca/huawei-built-at-least-a-three-month-stockpile-ahead-of-trump-ban-1.1260495

NIST. (2022, April 27). *Software Security in Supply Chains, Guidance* [Text]. NIST. https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains

NIST. (2024). NIST Releases Version 2.0 of Landmark Cybersecurity Framework. *NIST*. https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework

Northvolt. (2023, May 17). *Breaking a dependency*. https://northvolt.com/articles/breaking-a-dependency/

OECD. (2024). *Resilient Supply Chains—The OECD's 4 keys to #resilient supply chains present analysis and evidence in response to unprecedented disruptions to international trade, in pursuit of #sustainable and #inclusive recovery.* https://www.oecd.org/trade/resilient-supply-chains/

Paris Call. (2021a). *Paris Call for Trust and Security in Cyberspace—Advancing international norms*. https://pariscall.international/assets/files/WG4-Final-Report-101121.pdf

Paris Call. (2021b). *Paris-Call-Working-Group6-Report-Securing ICT Supply Chain.pdf*. https://pariscall.international/assets/files/2021-11-12-Paris-Call-Working-Group6-Report-SecuringICTSupplyChain.pdf

People's Republic of China. (2017). *PRC National Intelligence Law (as amended in 2018)*. https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/

Platform Africa. (2023, November 8). Global Gateway: EU signs strategic partnerships on critical raw materials value chains with DRC and Zambia and advances cooperation with US and other key partners to develop the 'Lobito Corridor'. *Platform Africa*. https://platformafrica.com/2023/11/08/global-gateway-eu-signs-strategic-partnerships-on-critical-raw-materials-value-chains-with-drc-and-zambia-and-advances-cooperation-with-us-and-other-key-partners-to-develop-the-lobito-corrid/

Ponomarov, S. Y., & Holcomb, M. C. (2009). Understanding the concept of supply chain resilience. *The International Journal of Logistics Management*, *20*(1), 124–143. https://doi.org/10.1108/09574090910954873

Qiu, H., Shin, H. S., & Zhang, L. S. Y. (2023). *Mapping the realignment of global value chains | BIS*. https://www.bis.org/publ/bisbull78.htm

Regulation (EU) 2024/1252 of the European Parliament and of the Council of 11 April 2024 Establishing a Framework for Ensuring a Secure and Sustainable Supply of Critical Raw Materials and Amending Regulations (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1724 and (EU) 2019/1020Text with EEA Relevance. (2024). http://data.europa.eu/eli/reg/2024/1252/oj/eng

Richard Baldwin. (2024, February 3). Are Industrial supply chains localising, regionalising, or globalising? *Factful Friday*. https://www.linkedin.com/pulse/q-industrial-supply-chains-localising-regionalising-yes-baldwin-tg15e/?trackingId=Rp18xNvjSiOLKCWAdtD8rg%3D%3D

Rodrik, D. (2007, June 27). The inescapable trilemma of the world economy. *Dani Rodrik's Weblog*. https://rodrik.typepad.com/dani_rodriks_weblog/2007/06/the-inescapable.html

Rodrik, D. (2023, November 7). *Doing Economic Nationalism the Right Way | by Dani Rodrik*. Project Syndicate. https://www.project-syndicate.org/commentary/east-asian-model-vindicates-economic-nationalism-by-dani-rodrik-2023-11

Rubbo, E. (2024). *What Drives Inflation? Lessons from Disaggregated Price Data* (Working Paper 32194). National Bureau of Economic Research. https://doi.org/10.3386/w32194

Setser, B. (2024, June 4). The Dangerous Myth of Deglobalization. *Foreign Affairs*. https://www.foreignaffairs.com/china/globalization-dangerous-myth-economy-brad-setser?utm_medium=newsletters&utm_source=fatoday&utm_campaign=The%20Dangerous%20Myth%20of%20Deglobalization&utm_content=20240604&utm_term=FA%20Today%20-%20112017

Shunsuke Tabeta. (2024, June 29). *China says rare earths belong to state in new regulation*. Nikkei Asia. https://asia.nikkei.com/Business/Markets/Commodities/China-says-rare-earths-belong-to-state-in-new-regulation

Simon J. Evenett & Nicolai Ruge. (2024). *The Costs Of Geopolitical Rivalry For Business—Ten Lessons For Better Policy Design*. World Economic Forum. https://www3.weforum.org/docs/WEF_Geopolitical_Rivalry_and_Business_2024.pdf

Smith, N. (2024, June 11). *Three holes in the U.S.' economic strategy against China*. https://substack.com/home/post/p-145431823

Steen, R., Haug, O. J., & Patriarca, R. (2024). Business continuity and resilience management: A conceptual framework. *Journal of Contingencies and Crisis Management*, *32*(1), e12501. https://doi.org/10.1111/1468-5973.12501

Stein, A. A. (2016). The great trilemma: Are globalization, democracy, and sovereignty compatible? *International Theory*, *8*(2), 297–340. https://doi.org/10.1017/S1752971916000063

Tabeta, S., & Ting-Fang, C. (2024, May 28). Chinese chipmakers push to limit foreign suppliers | Financial Times. *Financial Times*. https://www.ft.com/content/d9044108-891a-4463-b8a2-88435cbf1565

Tett, G. (2023, June 15). A new threat to financial stability lurks in the cloud. *Financial Times*. https://www.ft.com/content/0a20fe94-c128-4aad-a8a0-a0cb828c88f6

Tett, G. (2024, May 23). Forget macro and micro, it's mesoeconomics that matters. *Financial Times*. https://www.ft.com/content/79cf81af-5073-4c73-938b-93e8ac08c74d

The Economist. (2023a, August 3). How America is failing to break up with China. *The Economist*. https://www.economist.com/finance-and-economics/2023/08/08/how-america-is-failing-to-break-up-with-china

The Economist. (2023b, October 2). Attempts to make supply chains "resilient" are likely to fail. *The Economist*. https://www.economist.com/special-report/2023/10/02/attempts-to-make-supply-chains-resilient-are-likely-to-fail

The Economist. (2024a, June 6). Should the world fear China's chipmaking binge? *The Economist*. https://www.economist.com/business/2024/06/06/should-the-world-fear-chinas-chipmaking-binge

The Economist. (2024b, June 13). America's assassination attempt on Huawei is backfiring. *The Economist*. https://www.economist.com/briefing/2024/06/13/americas-assassination-attempt-on-huawei-is-backfiring

The White House. (2023, November). *Biden-Harris Administration Announces Supply Chain Resilience Center to Protect U.S. Supply Chain from Evolving Threats | Homeland Security*. https://www.dhs.gov/news/2023/11/27/biden-harris-administration-announces-supply-chain-resilience-center-protect-us

The White House, Council of Economic Advisers. (2023, November 30). *Issue Brief: Supply Chain Resilience*. The White House. https://www.whitehouse.gov/cea/written-materials/2023/11/30/issue-brief-supply-chain-resilience/

Thieu Vaessen. (2024, February 5). *Zorgverzekeraar VGZ eist duidelijkheid over herkomst medicijnen | FD*. FD.nl. https://fd.nl/bedrijfsleven/1505288/zorgverzekeraar-vgz-eist-duidelijkheid-over-herkomst-medicijnen

Tim Ruehlig et al. (2023). *Digital Power China report: Europe's strategic technology autonomy from China – assessing foundational and emerging technologies.* https://timruhlig.eu/p/strategic-autonomy-report

Tim Rühlig. (2024). *Reverse Dependency: Making -Europe's -Digital -Technological Strengths -Indispensable to -China | DGAP*. https://dgap.org/en/research/publications/reverse-dependency-making-europes-digital-technological-strengths

Timmers, P. (2022a). *Digital Industrial Policy for Europe | CERRE report*. CERRE. https://cerre.eu/publications/digital-industrial-policy-for-europe/

Timmers, P. (2022b). Strategic Autonomy Tech Alliances. *FEPS Strategic Autonomy Series*. https://www.feps-europe.eu/attachments/publications/220331%20final_strategic%20autonomy%20tech%20alliances-3a.pdf

Triolo, P. (2024). *China's Semiconductor Industry Advances despite U.S. Export Controls*. https://www.csis.org/analysis/chinas-semiconductor-industry-advances-despite-us-export-controls

UN. (2024). *Global Digital Compact | Office of the Secretary-General's Envoy on Technology*. https://www.un.org/techenvoy/global-digital-compact

Ursula von der Leyen. (2023, March 30). *Speech by the President on EU-China relations* [Text]. European Commission - European Commission. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_23_2063

Ursula von der Leyen. (2024a, May 6). *Press statement by President von der Leyen following the trilateral meeting with French President Macron and President of the People's Republic of China Xi Jinping*. https://ec.europa.eu/commission/presscorner/api/files/document/print/en/statement_24_2464/STATEMENT_24_2464_EN.pdf

Ursula von der Leyen. (2024b, July 18). *Political Guidelines 2024-2029—European Commission*. https://commission.europa.eu/about-european-commission/political-guidelines-2024-2029_en

US Senate Committee on Finance. (2024, May 20). *Automakers Shipped Cars and Parts Made by Chinese Company Banned for Forced Labor to the United States; Car Companies Are Failing to Police Their Supply Chains For Chinese Components Made with Forced Labor, Finance Committee Majority Staff Investigation Finds | The United States Senate Committee on Finance*. https://www.finance.senate.gov/chairmans-news/automakers-shipped-cars-and-parts-made-by-chinese-company-banned-for-forced-labor-to-the-united-states-car-companies-are-failing-to-police-their-supply-chains-for-chinese-components-made-with-forced-labor-finance-committee-majority-staff-investigation-finds

USTR. (2023a, March 28). *United States and Japan Sign Critical Minerals Agreement*. United States Trade Representative. https://ustr.gov/about-us/policy-offices/press-office/press-releases/2023/march/united-states-and-japan-sign-critical-minerals-agreement

USTR. (2023b, April). *Remarks by Ambassador Katherine Tai at American University Washington College of Law*. United States Trade Representative. https://ustr.gov/about-us/policy-offices/press-office/speeches-and-remarks/2023/april/remarks-ambassador-katherine-tai-american-university-washington-college-law

USTR. (2023c, September). *Remarks by Ambassador Katherine Tai on the World Trade Organization and the Multilateral Trading System*. United States Trade Representative. https://ustr.gov/about-us/policy-offices/press-office/speeches-and-remarks/2023/september/remarks-ambassador-katherine-tai-world-trade-organization-and-multilateral-trading-system

VDE. (2024, February 5). *Mehr Resilienz für die Strom- und Kommunikationsnetze in Deutschland*. https://www.vde.com/resiliente-strom-kom-netze

Wise, A., & Loeys, J. (2023). *Industrial policy, deglobalization and strategic asset allocation | J.P.Morgan* (Global Long-Term Strategy). https://d1e00ek4ebabms.cloudfront.net/production/uploaded-files/JPM_The_Long_term_Strate_2023-01-27_4318021-91952e6d-55c7-4f46-97ad-3cbc444609c7.pdf

World Bank. (2024, April 16). *Trade Watch (First Quarter 2024)* [Text/HTML]. World Bank. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099921104162412037/IDU1522a8b3911f8f142031aac6119a32986ed97

Wu, S., & Wu, S. (2022, September 30). Taiwan says U.S.-led 'Chip 4' group discussed supply chain resilience. *Reuters*. https://www.reuters.com/technology/taiwan-says-us-led-chip-4-group-discussed-supply-chain-resilience-2022-09-30/

Zeyi Yang. (2022, May 30). *How censoring China's open-source coders might backfire | MIT Technology Review*. MIT Technology Review. https://www.technologyreview.com/2022/05/30/1052879/censoring-china-open-source-backfire/

cerre Centre on Regulation in Europe

Avenue Louise 475 (box 10)
1050 Brussels, Belgium
+32 2 230 83 60
info@cerre.eu
www.cerre.eu

Centre on Regulation in Europe (CERRE)
CERRE Think Tank