OECD

LAUNCH VERSION

New Approaches to Economic Challenges

Economic Security in a Changing World

New Approaches to Economic Challenges

Economic Security in a Changing World

Please cite this publication as:
OECD (2025), *Economic Security in a Changing World*, New Approaches to Economic Challenges, OECD Publishing, Paris, https://doi.org/10.1787/4eac89c7-en.

ISBN 978-92-64-87007-9 (print)
ISBN 978-92-64-62069-8 (PDF)
ISBN 978-92-64-98994-8 (HTML)

New Approaches to Economic Challenges
ISSN 2707-7926 (print)
ISSN 2707-7934 (online)

Photo credits: Cover © ImageFlow/Shutterstock.com.

Corrigenda to OECD publications may be found at: https://www.oecd.org/en/publications/support/corrigenda.html.

Preface

Economic security is key to the stability and prosperity of countries and societies. Throughout modern history, economies have sought to protect their critical supply chains and the basic needs of their populations from disruptions and external threats. Economic security continues to be a central objective in today's highly interconnected and complex global landscape.

As this report highlights, different aspects of economic security are closely intertwined, such as supply chain resilience, energy security and cybersecurity. For example, the security of supply chains, including for energy, is important for ensuring secure energy supply. Energy security in turn is key to cybersecurity, with blackouts being a threat to cybersecurity. Cybersecurity relies on the security of supply chains for specific critical inputs, such as advanced chips, and digital technologies.

This report is part of the OECD's New Approaches to Economic Challenges (NAEC) work programme. The NAEC initiative, established in 2012, follows an interdisciplinary approach to economic and policy analysis, drawing on new thinking from a range of disciplines and supporting the analytical work and policy advice that the OECD provides to its member and partner countries.

Insights in this report build on the expertise across the OECD Secretariat and the International Energy Agency. They highlight the importance of economic security in the context of high degrees of geopolitical uncertainty and global interconnectedness. The report contributes to facilitating informed policymaking and strategic responses to ensure economic stability and resilience in an ever-changing world.

Mathias Cormann

OECD Secretary General

Álvaro Santos Pereira

OECD Chief Economist

Acknowledgement

The report contains contributions from: Przemysław Kowalski and Andrea Andrenelli (Trade and Agriculture Directorate); Laurent Bernat, Lauren Crean, Antton Haramboure, Guy Lalanne, Lea Samek and Angela Attrey (Directorate for Science, Technology and Innovation); Keisuke Sadamori (International Energy Agency); and Benjamin Katz, Ana Novik, Joachim Pohl and Nicolás Rosselot (Directorate for Financial and Enterprise Affairs). It was co-ordinated and edited by Valentine Millot, Łukasz Rawdanowicz and Douglas Sutherland. The report benefited from useful comments by: Alain de Serres, Åsa Johansson and Alvaro Pereira (Economics Department); Marion Jansen and Julia Nielson (Trade and Agriculture Directorate); Julia Carro, Gallia Daor, Alice Holt, Guy Lalanne, Takako Kitahara, Jerry Sheehan, Filipe Silva and Jeremy West (Directorate for Science, Technology and Innovation); Oliver Denk (Office of the Secretary-General); and Miłosz Karpiński (International Energy Agency); as well as from delegates of the Economic Policy Committee, the Trade Committee, the Digital Policy Committee and its Working Party on Digital Security, the Committee on Industry, Innovation and Entrepreneurship, and the Investment Committee. Ane Kathrine Christensen provided statistical assistance. Presentations and discussions during the NAEC workshop on economic aspects of national security, held at the OECD on 9 February 2024, helped shape the report.

Table of contents

Tables

Figures

Boxes

Executive summary

Economic security refers to a nation's ability to protect and sustain its economic stability and growth by strengthening its resilience against external and internal threats. It is a loosely defined concept which overlaps with the broader concept of national security. Following a series of economic crises and geopolitical tensions in recent decades, the breadth of economic security risks targeted by policymakers has expanded. It encompasses the capacity to safeguard key economic assets, maintain critical infrastructure and ensure access to essential resources such as energy, food and technology. The main dimensions of economic security include the protection of strategic industries and supply chains and maintaining trade and investment flows. It also covers cybersecurity. In essence, economic security is integral to national security, as a strong and stable economy underpins a nation's overall ability to defend and advance its interests in a rapidly changing global environment.

Economic security risks have recently come to the fore in the public debate with the disruptions to supply chains during the COVID-19 pandemic and the volatility of energy and agricultural markets in the wake of Russia’s war of aggression against Ukraine. The resulting disruptions in the supply of critical raw materials (CRMs), energy, pharmaceuticals, semiconductors and other goods challenged the economic, health or military security of countries. The importance of many of these aspects has increased in the context of rising geopolitical tensions, the much-needed green transition to prevent dramatic consequences of climate change, and accelerating digitalisation of economies. Therefore, many governments are expanding and exploring policy instruments and policy actions to ensure economic and strategic security.

This report discusses these pressing issues, examining both longstanding and emerging challenges to economic security, along with potential policy responses. It highlights several aspects:

- Several economic security risks stem from concentrated production and trade of specific goods and technologies, including primary energy, semiconductors and CRMs. High concentration can be the outcome of increasing specialisation that helps to boost productivity and lower prices, including as a result of economies of scale in production. However, high concentration together with longer and more complex international supply chains may create potential for the propagation and amplification of micro-shocks and thereby raise geopolitical risks.
- Increased cross-border ownership of companies, including ones that operate critical infrastructure, has also raised concerns about investment security. In this context, many countries have established or updated investment review mechanisms.
- Risks to economic security tend to be interconnected. Disruptions in one area can have cascading effects on others. This stems from the complex interdependencies between different economic sectors and from the growing reliance on specialised intermediate inputs as well as connectivity services and infrastructure. Thus, efforts to enhance resilience in one area can indirectly contribute to resilience in another, highlighting the need for continued discussions and active collaboration across the various spheres of economic security.
- Policy responses aimed at minimising economic security risks are essential. However, there are legitimate concerns that poorly designed measures could unnecessarily undermine the benefits of market economies and international trade. Therefore, effective policy design and dialogue is crucial to balance economic security needs without eroding the advantages of open markets.

- While our knowledge about economic security risks in different domains is improving, there is still a need for more data and analysis. These are essential to formulating evidence-based policy recommendations.
- In this context, the OECD as well as the IEA have played an important role and will continue to do so. Our analysis of supply chain vulnerabilities (e.g. the OECD Supply Chains Resilience Review), restrictions on exports of CRMs (e.g. OECD Inventory of Export Restrictions on Industrial Raw Materials), energy security, policy frameworks and guidelines for foreign investment policies and digital security, and exchanges of expert groups (e.g. the Semiconductor Informal Exchange Network (SIEN), the Trade Chief Economists Network and the Medical supply Chains Network (MEDICON) initiative promoting resilience in medical supply chains) provide important contributions to debates and policy design about economic security.

The report consists of four chapters. Each chapter addresses distinct yet interconnected risks facing contemporary economies and outlines a range of policy approaches to mitigate them.

The first chapter focuses on risks stemming from vulnerabilities in international supply chains. The emergence of global value chains (GVCs), supported by falling communication and data transfer costs and reduction of barriers to foreign investment and trade since the 1990s, has transformed the global economy. This has brought many benefits in terms of higher productivity, lower prices and a greater variety of goods, and has accelerated income convergence of many emerging market economies. At the same time, dependence on exports and imports has increased globally, including for energy and products essential for the digital and green transitions, but to a varying degree across countries and sectors. The production of some products has become highly concentrated in specialised firms and countries. GVCs have become longer and more complex. These features ensure efficiency gains and facilitate diversification of supply and demand. However, they may create potential for choke points and for propagation and amplification of micro-shocks. They may also raise geopolitical risks, including economic coercion. OECD research finds that, while the majority of global exports and imports remain well diversified, sectors such as commodities and agriculture show higher levels of concentration, increasing exposure to potential disruptions.

In the face of these risks, there are growing calls for policies to reduce dependence on specific countries, enhance security and improve the resilience of supply chains. Diversifying, bringing production home or to nearby locations (the so-called re-shoring and near-shoring), and optimising stockpiling are the three most frequently discussed strategies. However, some of such policies may undermine the benefits of international trade. As discussed in this first chapter, empirical research, including OECD studies, shows that shocks transmitted through GVCs on average tend to have small impacts on other sectors, although there are exceptions. Well diversified GVC linkages also offer options to source from alternative sources or to sell to alternative destinations when shocks occur. As policymakers consider strategic shifts in response to supply chain vulnerabilities, maintaining open markets and managing trade interdependencies will be key to balance economic security with continued growth.

The first chapter ends with a special focus on two specific supply chains which are crucial in today's economy: semiconductors (Special Focus 1) and CRMs (Special Focus 2). Semiconductors are vital for economic growth and security. They are essential for various electronic devices, including vehicles and appliances and they play a crucial role in leading-edge technological development, such as artificial intelligence. However, the semiconductor value chain is highly concentrated, with few economies able to contribute significantly to every stage of production for all semiconductor types. For instance, more than 90% of leading-edge logic chips are produced by a single company, TSMC, in Chinese Taipei, and just three companies control nearly 80% of the market for the software required to design chips. Shortages in semiconductor supply have led to significant supply chain disruptions, particularly during the COVID-19 pandemic. Governments are responding to these challenges by seeking to build domestic semiconductor ecosystems and to reduce dependency on foreign suppliers as well as to diversify sources or critical inputs.

To enhance the resilience of semiconductor GVCs, international collaboration, information sharing and best practices are essential. The OECD convenes the SIEN to promote policy dialogue and transparency and to develop early warning mechanisms for value chain disruptions. Several OECD countries have implemented policies, including subsidies to investment, to develop local semiconductor ecosystems. However, establishing new manufacturing facilities requires more than financial support to companies – it also depends on a skilled workforce and critical infrastructure. Addressing the global shortage of semiconductor talent requires renewed efforts to improve science, technology, engineering and mathematics education and to foster stronger industry-academia partnerships.

CRMs, explored in the second Special Focus of the first chapter, are set to play an increasingly vital role for energy generation and economic security, as they are key components of green energy and digital technologies. Demand for CRMs has grown robustly and is set to increase further. These raw materials such as lithium, cobalt, nickel, gallium, titanium or tungsten are used for a broad range of goods, including batteries and semiconductors. The demand for such minerals has increased significantly in the recent years, driven by the demand for electric vehicles, solar panels and other clean technology applications. As nations strive to shift away from fossil fuels and accelerate decarbonisation, the demand for critical minerals necessary for green technologies is poised to skyrocket. The production of CRMs is concentrated in a few geographic regions. This creates supply chain risks and incites major producers to impose export restrictions to support domestic downstream industries. Such restrictions have risen significantly in the past 15 years.

Case studies show that while export restrictions can sometimes foster domestic industries, they do so at the expense of trading partners and may lead to increased foreign dominance. The high volatility in prices of CRMs, which can be further exacerbated by export restrictions, hampers investment decisions in the whole supply chain. International co-operation is therefore necessary to diversify CRM sources and secure stable supplies, while also promoting economic development in resource-rich countries. Balancing responsible sourcing with supply security requires careful management to avoid disruptions. Effective due diligence in supply chains is crucial for identifying and mitigating risks, especially in conflict-affected regions. Although initiatives to enhance traceability and transparency are in place, challenges persist due to unreliable data and ongoing geopolitical tensions.

The second chapter focuses on energy security, a longstanding concern but with new challenges. Energy security is part of the broader concept of national security and involves technical, economic and political aspects. It frequently deals with short-term risks (for example exposures to potential disruptions of energy systems) and resilience (for example the ability to withstand disruptions) for energy supply, transformation, distribution and end-use energy services for main energy sources. It also relates to the affordability of energy.

Energy security has been increasingly debated in the context of the green transition, highlighting the imperative of ensuring stable and sustainable energy supplies in a rapidly evolving environmental landscape. Renewable energy sources offer opportunities to reduce dependency on fossil fuels. However, they also introduce new challenges, such as the dependence on critical materials mentioned above and on technological innovations to ensure stable energy supply.

To guarantee energy security during the transition, when both clean energy and fossil fuels will be needed, countries will have to boost investments in low-carbon energy while phasing out fossil fuels. Energy efficiency measures will be essential to avoid mismatches between supply and demand. Policies to encourage retrofitting of buildings will be especially crucial to reduce energy consumption. Maintaining and reusing some critical fossil fuel infrastructure will also be necessary to avoid disruptions, for example using gas-fired power plants to meet peak electricity demand, as well as strengthening electricity systems with grid flexibility solutions such as battery storage and demand response. Reducing the very high capital costs in emerging market and developing economies will be essential to lowering the costs of the transition. At the same time, addressing the specific risks faced by fossil fuel-exporting economies requires promoting

diversification and investment in renewables, hydrogen and carbon capture. Finally, addressing market distortions (in particular fossil fuel subsidies) and correcting market failures will be key to leveraging private investment for an efficient green transition.

The third chapter sheds light on recent developments in the management of international investment security. Geopolitical risks and concerns about the security of supply of critical goods and services are prompting heightened attention to foreign investments in critical sectors. In this context, many countries have established or updated investment review mechanisms, have broadened their scope of application to include emerging technologies and sensitive information. Investment security was an early, arguably pioneering, aspect of governments' broader efforts to enhance their economic security and aligns closely with more recent efforts to address other dimensions of risks. Investment-related tools may inspire and inform economic security initiatives in other areas.

The fourth and final chapter focuses on the role of cybersecurity in advancing economic and social prosperity. The accelerating digitalisation of economies has led to a growing reliance on connectivity services and infrastructure, coupled with increasing vulnerability to cyber threats and cybercrime.

Cybersecurity is crucial for protecting critical activities and information, including energy, financial systems, intellectual property and sensitive data. A breach in digital security, particularly in the case of ransomware, can have severe economic repercussions, leading to financial losses and the disruption of services, including those provided by public institutions. It can also tarnish stakeholders' reputation. This could have profound implications for trust in public governance, financial and healthcare systems, and democratic processes at large. As economies become more interconnected and reliant on digital technologies and their underlying infrastructure, investing in and implementing robust digital security measures is essential to safeguarding economic stability, promoting innovation, and fostering trust among businesses and individuals.

The OECD Policy Framework on Digital Security, further detailed in the final chapter, outlines key strategies for addressing the economic and social dimensions of cybersecurity, including high-level principles as well as more detailed policy and technical recommendations. This includes establishing a culture of digital security to address some of the associated risks of digital transformation while reaping security benefits. The framework encourages national strategies that involve all stakeholders (governments, firms and individuals) to raise awareness of cyber threats, build incident response capacity, and promote risk management standards, workforce development and international co-operation.

Governments can foster an enabling environment for the adoption of digital security best practices among all stakeholders. This includes promoting a co-ordinated and holistic approach to digital security (i.e. across the entire lifecycle of products and services), incentivising network operators to adopt comprehensive risk management frameworks and encouraging suppliers to improve supply chain transparency (e.g. through enhanced traceability of components and digital security certification) and to diversify supply chains.

1. Economic security and vulnerabilities in international supply chains

Przemysław Kowalski and Andrea Andrenelli[1]

Introduction

Economic efficiency gains associated with international supply chains continue to be widely acknowledged. Yet there is also debate about whether the greater fragmentation of production in supply chains contributed to the spread and amplification of recent negative economic shocks (such as the COVID-19 pandemic or Russia's invasion of Ukraine) or whether it was an attenuating factor in reducing the impact of those shocks. Against this background, growing geopolitical tensions, expanded intervention by governments in the economy, and intensifying international competition for natural resources, have all led to a greater focus by the public and policymakers on the potentially negative implications of trade interdependencies.

The perceived likelihood of politicisation or weaponisation of trade interdependencies is triggering interest in identifying areas of vulnerability. These potential "trade dependencies" can be broadly defined as commercial links that could cause high economic or societal damage in case of unexpected disruptions, and that could be used as a tool of coercion, compromising national security and disrupting strategic activities.

Following a discussion of how supply chain interdependence has influenced the efficiency of production, and the transmission and management of shocks in the global economy, the remainder of this chapter discusses trade and supply-chain specific economic security risks. It then discuses key challenges of measuring trade dependencies more broadly and presents selected results of recent OECD analysis attempting to quantify elements of the historical evolution and economic significance of trade dependencies using different data and empirical methodologies.

Efficiency and interdependency of international supply chains

The emergence of international supply chains has been transformative. The falling costs of long-distance communication and data transfer, which accelerated in the early 1990s, created new business opportunities and boosted productivity through finer specialisation at the task or specialised input level (Baldwin, 2011[1]). Supply chains have also created new opportunities for less developed countries to grow and create jobs by participating in trade and production of advanced products by providing specialised inputs. Organising production in supply chains also made different production locations and national economies more interdependent. It is now common for the different stages of a production process of a good or service (e.g. design, production, marketing, manufacturing, assembly and distribution) to be carried out in parallel or sequentially in several geographical locations. Profit-seeking multinational enterprises are the key actors managing these activities and they make strategic decisions about locations of different specialised activities and their co-ordination. The interdependency which underlies these

activities is therefore an integral feature of international supply chains and one of the main sources of their economic efficiency.

However, supply chain interdependencies can also have important – although not always straightforward – implications for how national economies can be affected by – and how they can respond to – unexpected external shocks or events and how they may be affected by the policies of other countries.

- On the one hand, well diversified supply chain activities can support resilience to both domestic and external shocks by drawing on more varied sets of commercial partners and markets and thereby creating a wider range of options to assist in coping and recovery from disruptions. For example, in the face of some disruptions, it may be easier to change a supplier, or reconfigure or relocate just a segment of a supply chain rather than overhaul a whole industry. In this sense, global value chains (GVCs) have also opened new possibilities for diversification and improved resilience (e.g. Lafrogne-Joussier (2021[2]), Arriola et al. (2020[3])).
- On the other hand, by depending more on foreign inputs and foreign demand, national economies linked through international supply chains may be more exposed to external shocks. Sometimes this exposure may be difficult to assess in advance as intricate cross-border movements of physical and intangible inputs in supply chains can create complex links between different stages of production. These multifaceted and multitiered links can nevertheless be sensitive to even small changes in regulation and trade, transport and communication costs, while not being always fully transparent or straightforward to track for lead firms. To the extent they involve trade in specialised differentiated inputs, they may also be associated with significant lock-in effects for buyers and sellers and thus may constrain the possibility to switch to an alternative party (Antras and Staiger, 2012[4]). They also often span across countries characterised by different levels of development, institutions, and political systems, which may make the containment of shocks and co-ordination of responses more difficult.

The emergence of international supply chains has also changed the nature of trade and trade-related policy making. Relative to the pre-supply chain era, trade policies have been focused less on negotiating access to foreign markets for final products (lowering of barriers to accessing foreign markets) and more on having access to competitive high-quality inputs and on lowering various types of trade costs to ensure a smooth multidirectional exchange of intermediate products and services (lowering of own and foreign trade costs) (Baldwin, 2011[1]). Decisions about a geographical location of specific supply chain segments are highly sensitive not only to international trade costs but also to various domestic costs which are influenced by regulation (e.g. permits), business environment (e.g. taxation) and quality of infrastructure (e.g. energy availability and costs, ports, roads and connectivity). In this sense, the fragmentation of supply chains has expanded the range of what are, in principle, domestic policy interventions, but which nevertheless have significant international spillover effects (see also Staiger (2022[5])).

Supply chain linkages are rarely characterised by perfect competition. The differences in market and bargaining powers of different supply chain actors and the often-unequal distribution of gains from supply chain participation across the different supply chain segments, have also prompted policymakers to try to improve the position of national firms and to create conditions to attract the most lucrative supply chain segments to their countries, in particular through industrial policy. For example, governments have tried to lower the costs of upstream inputs and to boost profitability of domestic firms via other forms of government support. These measures have aimed at attracting domestic and foreign investment in preferred downstream activities, as well as enlarging influence in specific upstream and downstream segments of supply chains to gain access to superior capital and technology or to gain a strategic or economically preferred supply chain position. Even if not always well defined,[2] moving up or upgrading of the value chain position has been a frequently declared policy objective in the 2010s, particularly in developing and emerging economies. Then, the policy debate focused on how to best maximise the benefits from supply chain participation.

Supply chains and economic security

One of the factors that has contributed to a greater focus on possible negative aspects of interconnectedness and propagation of shocks in international supply chains is a perceived increase in geopolitical, policy and economic uncertainty. While measurement of these phenomena is complex, and results are not always straightforward to interpret, a few recent studies and measurement initiatives have gathered evidence for increased uncertainty. The methodology developed initially by Baker, Bloom and Davis (2016[6]) showed that global economic policy uncertainty increased markedly in the aftermath of the 9/11 terrorist attacks in 2001, during and in the aftermath of the 2008-09 global financial crisis (GFC), during the COVID-19 pandemic, and after Russia's large-scale invasion of Ukraine in 2022. According to this index, in the last four years, policy uncertainty was on average significantly higher than in any previous period since the end of 1990s. Caldara and Iacoviello (2022[7]) measured the perception of risk related to wars, terrorism and tensions among states and political actors, and similarly showed an increase in geopolitical risk following the 9/11 terrorist attacks in 2001 and another significant increase in the aftermath of large-scale Russia's invasion of Ukraine in February 2022.[3]

This new environment is forcing a reassessment of economic policy assumptions and consideration of new trade-offs. Policymakers are confronted by a landscape characterised by rising geopolitical tensions; heightened national security concerns, notably in relation to digital technologies; strategic competition and the quest for leadership on new technologies, notably for the green and digital transitions; reassessment of the role of global supply chains in ensuring access to essential goods and services, including for those same transitions; and the weaponisation of trade interdependencies in instances of economic coercion. These forces come at a juncture where both the GFC and the COVID-19 pandemic had already seen governments playing a greater role in the economy in several countries, and where there is a growing discussion of how the "rules of the road" (including WTO rules) for an integrated global economy can most effectively function across countries with very different economic systems.

Against this background, the concept of "economic security" has been gaining prominence among policymakers. While economic security entails a range of issues that go beyond the trade and investment policy community, it is a concept that deeply engages the trade policy community, as international economic linkages are both an enabler of economic security (for example, in enabling diversification of supply and demand) and a source of risks to that security.

A key issue in discussions on economic security is security of supply of critical goods and services. This is part of a wider agenda of ensuring the resilience of global supply chains, which requires an understanding of the nature and extent of vulnerabilities (notably in relation to concentration). Vulnerabilities can be used by third parties to interrupt the supply of critical goods and services and can also be used to coerce vulnerable parties into policy changes.[4] Beyond critical goods and services, certain dependencies upon certain countries can become vulnerabilities under geopolitical tensions, or where countries or regions are at a risk of conflict.

This changing landscape has triggered reflections on possible policy responses to economic security concerns. While the debate on the best policy responses continues, diversification of supply appears to be seen as one of the most effective policies to reduce risks arising from the geopolitical environment. Co-operation between trusted partners is important and can help reduce risks. This can be seen both as a means for trade to provide mutual benefit to trusted partners, as well as to reduce the risk of supply disruption from partners perceived as less reliable. In a wider debate on ensuring resilience, a range of other approaches has been put forward, from greater transparency on supply chains to assisting with risk identification and management, including through public-private dialogue; through to efforts to diversify supply across companies and countries; to the creation of domestic production capacity.

Certain technologies or products are also seen as being strategically important representing an additional argument for co-operation among trusted partners to ensure resilient production and trade of these

sensitive products. This can involve ensuring the supply of critical inputs, such as critical raw materials, by tackling export restrictions or reaching supply deals with trusted partners (see Special Focus 2). In other cases, it may mean paying additional attention to the sources and range of suppliers for products not seen as sensitive themselves, but which may be essential inputs into critical infrastructure.

There is also the debate over whether some goods and services are so important or sensitive strategically, technologically or because they may have military applications, that countries want to ensure supply through domestic production. While this is not realistically an option for all or even many countries depending on the good or service concerned, where this is possible it can raise issues for integrated global markets. For example, building domestic production capacity (notably where it represents a decision that companies would not have taken on their own commercially) can involve government support, raising issues related to the impact on other countries (including in terms of attracting investment that might have otherwise gone elsewhere) and on competition in global markets.

In this wider landscape, policymakers are dealing with difficult decisions, which require new data and analysis (such as on trade dependencies and vulnerabilities). With an increasing number of these decisions to be made, evidence-based policymaking remains important.

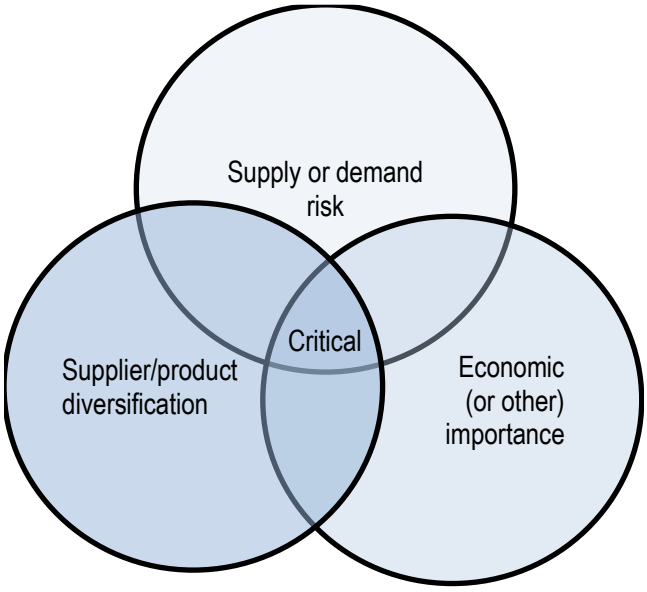
The challenges of measuring trade dependency

Notwithstanding the increased interest in identifying trade vulnerabilities, it is difficult to identify objective analytical criteria that would enable a clear separation of those trade links that may be sources of concern from those that are advantageous. This is in part related to the fact that the concerns that lie behind the debate on trade dependencies are often non-economic and that what is considered to be of concern from the point of view of, for example, protection of the environment, social sustainability or national security, can be country specific. Thus, it is not immediately obvious what role economic analysis could play in addressing such concerns.

From an economic point of view, however, there are concerns that policy responses which are aimed at minimising trade-related risks may unnecessarily undermine the economic benefits of international trade or have unwanted or unintended economic and non-economic effects. Economic analysis can thus be used to help draw a comprehensive picture of the economic characteristics of trade linkages which could be viewed as trade dependencies. It could also help assess the economic costs and benefits associated with different policy options for addressing trade dependency.

The emerging economic literature suggests that trade dependencies can be usefully defined as trade flows combining three characteristics: high risk of disruption, high economic (or other) importance, and constrained possibility of diversification or substitution (Figure 1.1). In a recent analysis aiming to shed empirical light on the question of trade dependency, the OECD has investigated different sources of data and key modelling frameworks to identify trade flows appearing to meet these criteria and to examine their characteristics and evolution (Arriola et al., 2024[8]).

Figure 1.1. Criteria for identifying critical trade dependency



Source: Arriola et al. (2024[8]), "Towards demystifying trade dependencies: At what point do trade linkages become a concern?", *OECD Trade Policy Papers*, No. 280, OECD Publishing, Paris.

What do product-level trade data tell us about trade dependencies?

Several measures of trade dependency build on the concept of trade concentration; that is, reliance on only a few suppliers for imports or only a few markets for exports of specific products. If a country's imports or exports of a product are accounted for by only a few partners (are highly concentrated), the country may struggle to find alternatives in the face of disruptions in foreign supply or demand.[5] The evolution of global trade data at a detailed product level in the period 1997-2021 has been studied through the lens of trade shares and trade concentrations.[6] Trade concentration matters for economic security as shown econometrically, for example, in the context of the COVID-19 pandemic foreign supply disruptions by Schwellnus et al. (2023[9]), who found that foreign supply disruptions have larger adverse effects in sectors where industry and geographic suppliers are highly concentrated. While the measures – or combinations of measures - as well as the specific quantitative thresholds used to delineate normal and concerning degrees of trade concentration often differ from one study to another, the trade concentration approach has been used frequently to quantify trade dependency or vulnerability in the recent literature (Bonneau and Nakaa, 2020[10]; European Commission, 2022[11]; Vicard and Wibaux, 2023[12]; Berthou, Haramboure and Samek, 2024[13]).

Imports of specific products have become on average more concentrated across trading partners between 2008-10, i.e. at the time of the global financial crisis, and 2014-16, i.e. during the period before the first US-China trade tensions episode (Figure 1.2). In part, this likely reflects finer levels of specialisation in international supply chains which proliferated during this period. The trend is also consistent with the perception of an increase in vulnerabilities to unexpected shocks transmitted through international trade and supply chains. In addition, global exports of products are on average more concentrated than global imports, while national imports of products are more concentrated than national exports, which might explain the focus in public debate on supply or import dependencies.

However, the data also show that the current levels of trade concentration of global exports and imports are, overall, not alarming and that large, if not dominant, portions of trade are relatively well diversified. For

example, for global exports of products, which are on average more concentrated across exporting countries than global imports are across importing countries, only about 30% of products record relatively high levels of concentration, while exports of the remaining products are relatively well diversified. This suggests that large portions of international markets are characterised by a reasonable degree of competition, and that specific exporters and importers have limited control over total supply or price formation.

This is not to say that the levels of concentration seen for some products in some countries are not of concern, but rather that, for many products, international markets in fact offer good options for diversification. Products with some of the highest levels *of global export concentration* include, for example, a range of industrial raw materials (e.g. tin, lead, copper and wood, see also the Special Focus on critical raw materials) and a range of products of light manufacturing (e.g. textiles and footwear or headgear) and products of the agri-food industries (e.g. fibres, coffee, tea and fishery products). Products with some of the highest levels of *global export diversification* include several advanced manufacturing industries (e.g. aluminium, iron and steel, base metals and machinery manufacturing) notwithstanding the perception that they are vulnerable.

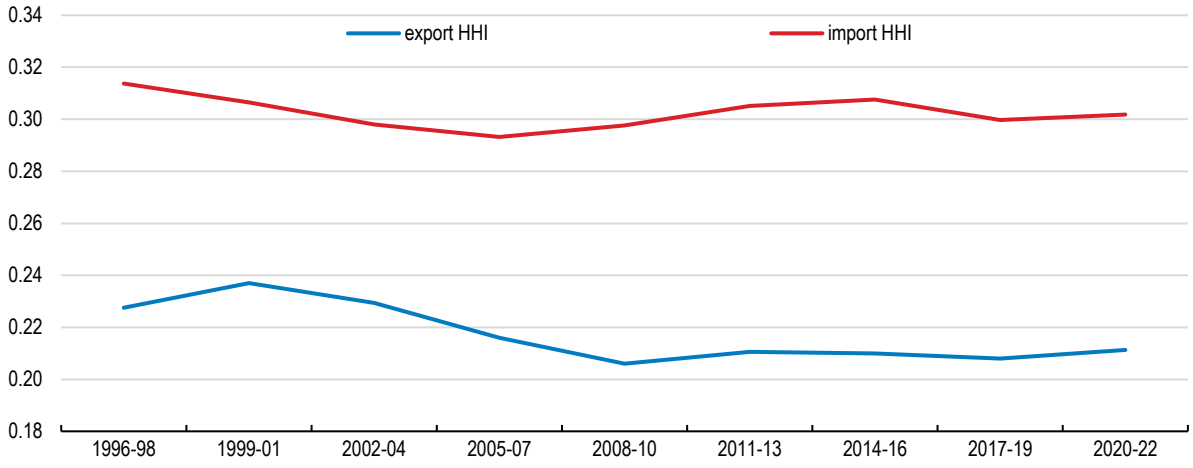
Overall, the uneven – and sometimes counterintuitive – patterns of global export concentration across products highlight the multiple factors which drive concentration of trade in international supply chains. These include availability of natural endowments, patterns of comparative advantage, and economies of scale, but also trade and industrial policies which influence relative costs of production in different locations.

Interestingly, *concentrations of national trade* tend to be higher than *concentrations of global trade* which means that countries typically source their imports from – and ship their exports to – fewer partners than is in principle globally possible. This likely reflects a combination of natural factors, such as the role of geography and trade costs, particularly in the context of international supply chains which tend to be concentrated regionally, as well as countries' preferences and policies. The latter have been revealed for example in the expansion of regional and preferential trade agreements which by design tend to lower trade costs and give other advantages to selected trade partners, contributing thereby to trade concentration. Strategic economic policies of importers and exporters could also have played a role.

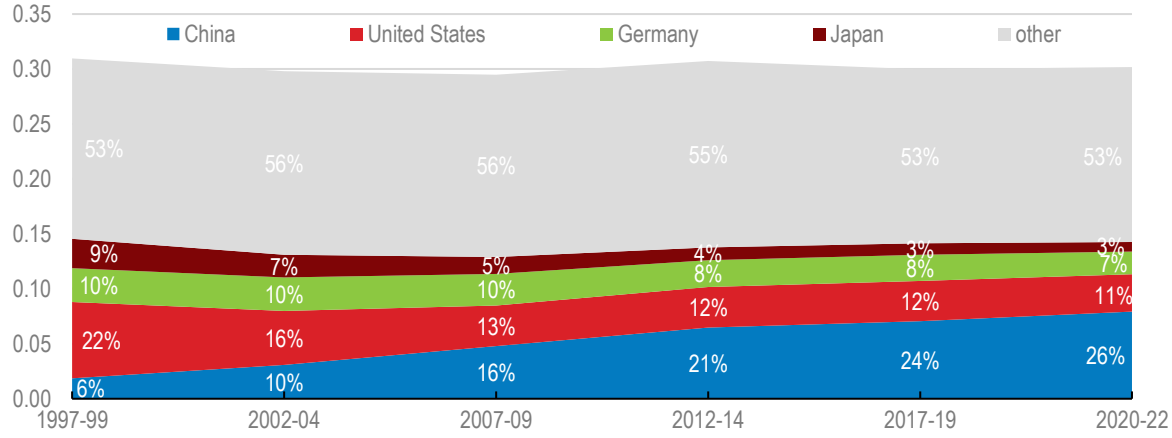
On the export side, the overall rise in national import concentrations of other nations has coincided with raising shares of China as a source of imports (Figure 1.2, Panel B).

Figure 1.2. Country-level concentrations of exports and imports of merchandise products

A. Average country-level concentration of exports and imports across all HS6 products



B. Contributions of China and other countries to the average country-level import concentration



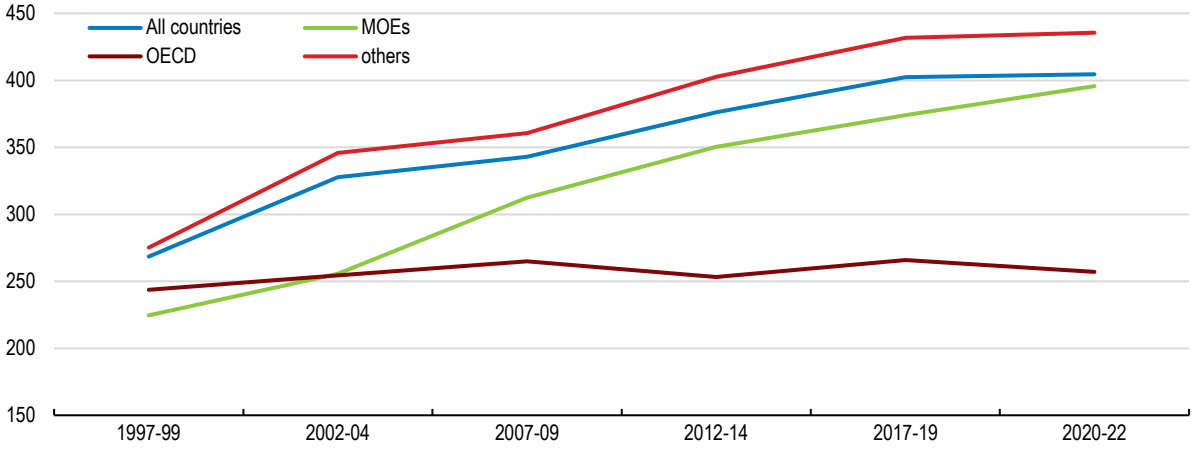
Note: In Panel A, the average country-level concentration of imports and exports is obtained by calculating, first, for each HS6 product and, for exports (imports), each exporting (importing) country an index of concentration (HHI) across all importers (exporters) from (to) that country, and second by calculating a weighted average across all relevant product lists, with weights equal to the value of exports (imports) in that product across all partners. '1996-98', '2002-04', etc., denote the averages for the three-year periods 1996, 1997 and 1999; 2002, 2003 and 2004; and so on. Panel B shows the decomposition by selected exporters of the above values of the HHI index for imports of all products. For more information on methodology see Arriola et al. (2024[8]).

Source: OECD calculations using the BACI data.

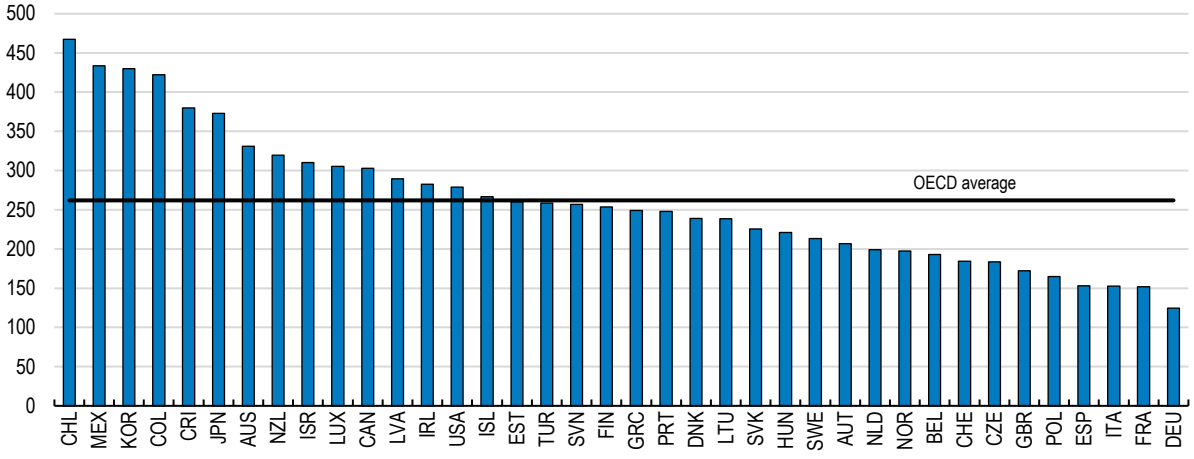
Defining the extent to which countries rely on significantly fewer suppliers (national import concentration) than is offered by the global economy (global export concentration) as *significant import concentration* reveals that the overall incidence of such significant concentration of national imports has been on the rise in the investigated period. This has been mainly accounted for by non-OECD economies as significant import concentration has not changed much on average for OECD countries (Figure 1.3, Panel A). This suggests that to some extent firms and consumers in OECD countries have been able to take advantage of diversification possibilities offered by international markets to diversify and reduce dependency.

Figure 1.3. Average incidence of significant import concentration by country grouping

A. Average number of imported HS6 products with significant import concentration per country



B. Number of imported HS6 products with significant import concentration (average for 2017-19 and 2020-22)



Note: Significant import concentration is defined in cases of bilateral import links at the product level where the value of country-level HHI for imports is more than double the value of the corresponding HHI for global exports. To further constrain the spectrum of cases of significant concentration, an additional minimum cut-off value of HHI calculated for global product-level exports was set at 0.2. This means that only products with a global exports HHI of at least 0.2 and products with country-level imports HHI of at least 0.4 were considered. The country group "others" comprises all non-OECD, non-MOE countries for which data are available in the BACI database. This focus is purely analytical and is without prejudice to the relationships between the OECD or any of its members and any of the individual countries of the major other economies (MOE) grouping. The MOE grouping includes Brazil, China, India, Indonesia, Russia and South Africa. For more information on methodology see Arriola et al. (2024[8]).

Source: OECD calculations using BACI data.

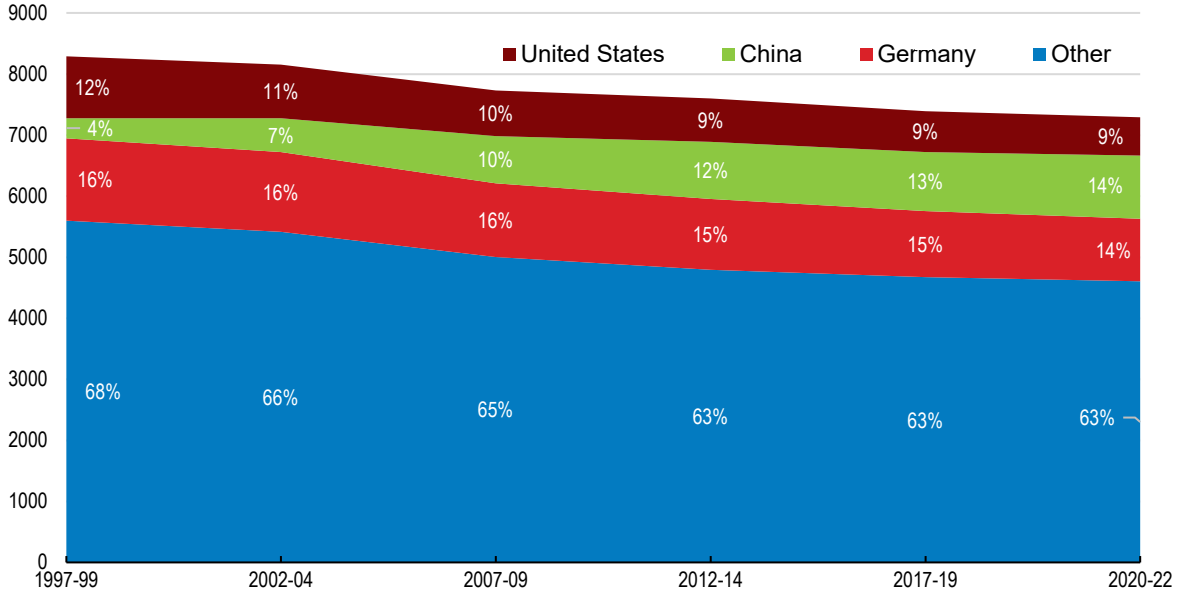
However, the differences in the levels of such significant import concentration also suggest that, even amongst OECD countries, there is untapped potential to diversify further (Figure 1.3, Panel B). For example, in the OECD countries which recorded the highest scores for significant import concentration such as Chile, Mexico and Korea, these scores are more than three times higher than in the countries with the lowest scores (Germany, France and Italy).

Which trading partners are the main counterparts in the highly concentrated trade linkages matters as geographic, economic and geopolitical risks vary across countries. Dependency on China has increased significantly across all OECD countries and regions since the late 1990s and China is now the single most important counterpart in trade dependencies of the OECD as a whole and of several OECD countries individually (Figure 1.4). Thus, there is interest in a better understanding of the reasons for the emergence of China as a source of dependencies. In particular, the contributions of natural and policy-related factors, including policies which may have involved market distortions or targeted non-economic objectives, need to be better understood.

At the same time, trade dependencies of OECD economies on China also need to be put in the context of China's dependencies on OECD economies. The OECD as a group – and several OECD countries on their own – are a much more important counterparts in dependencies of China. Moreover, China's sectoral dependencies involving OECD countries include several industries in which several OECD countries also depend on China, underscoring the mutual character of some trade interdependencies (Figure 1.5).

Figure 1.4. Evolution of OECD countries' import dependencies, by major exporting country

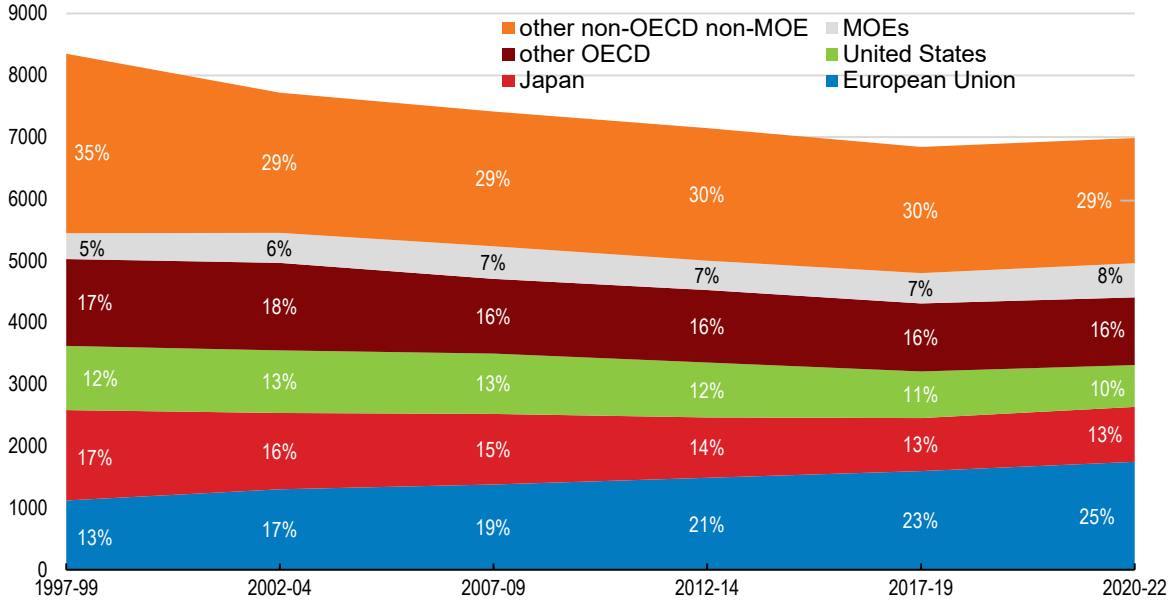
Average per country number of bilateral import dependencies on the United States, China, Germany and other countries (shares in labels)



Note: Other – all the other OECD and non-OECD countries covered in the BACI database. For more information on methodology see Arriola et al. (2024[8]).
Source: OECD calculations using the BACI data.

Figure 1.5. Evolution of China's import dependencies, by major exporting country or region

Average per country number of bilateral import dependencies of China on the United States, Germany, Japan, other OECD, MOEs and other countries (shares in labels)



Note: *Other OECD* are all the OECD countries except the United States, Japan and OECD countries that are EU members. The major other economies (MOE) grouping includes Brazil, China, India, Indonesia, Russia and South Africa. For more information on methodology see Arriola et al. (2024[8]).
Source: OECD calculations using the BACI data.

Anticipating the effects of shocks transmitted through international supply chains

While product-level analysis can provide valuable insights into trade dependency, exposure of national economies to potential shocks depends on the nature of their specialisation and integration into international supply chains. These characteristics go beyond trade concentrations and bilateral trade shares. The OECD global trade model METRO can be used to unpack some of the broad relationships with a view to informing government and business efforts to enhance resilience to shocks (Arriola et al., 2020[3]).[7] While the modelling relied on several assumptions which necessitate a careful approach to policy implications, a few broad findings and policy consequences can be identified.

Production disruptions in most segments of the global economy cause relatively small output responses elsewhere. This suggests that the current structure of domestic and international linkages and economic adjustment mechanisms tend to dampen the impacts of shocks rather than amplify them. That said, there are also some large outliers indicating that shocks in some segments of the global economy may have more consequential effects.

The impacts of shocks occurring in other domestic sectors tend to be larger than impacts of shocks occurring in foreign sectors. This is because in most sectors the reliance on foreign inputs and foreign markets for final products is still smaller than reliance on domestic inputs and product and factor markets. In addition, international markets offer broader adjustment and diversification options than domestic markets. Therefore, production disruptions originating in foreign vertically-linked sectors – the kind of shocks that are at the centre of the debate on propagation of shocks in international supply chains (GVC shocks hereafter in this section) – do not appear to be the main source of disruptions. While disruptions in

upstream sectors in the value chain can constrain access to intermediate inputs, and output declines downstream can lower demand for inputs, most impacts are two orders of magnitude smaller than the original shocks. The dispersion of impacts is also smaller than for domestic shocks. Again, this reflects the current levels of diversification and greater possibilities for adjustment in GVCs.

A wide variety of domestic and international economic adjustment mechanisms may be at play. Price signals leading to substitution towards other suppliers or other market outlets, and responses of labour and capital markets play an important role in shaping responses to shocks. They should therefore be part of assessments of resilience to shocks and trade dependency.

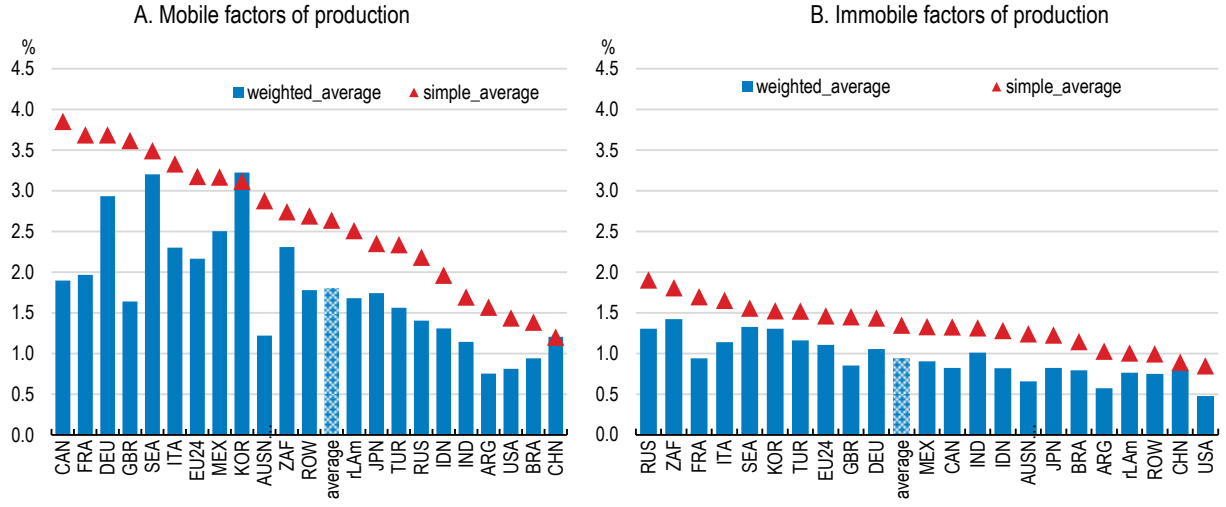
The degree of factor market adjustment can affect the transmission of shocks. Impacts of shocks across national economies tend to be smaller when factors of production cannot move across sectors (short term) than when they can move freely (medium to long term). This underscores that short-lived disruptions may matter less than disruptions which last longer and allow more time for factor markets to react and pass on the impacts to other sectors. It also suggests that policies protecting employment or restricting capital movements may play an attenuating role in the face of temporary shocks.[8]

While most of the impacts of GVC shocks are much smaller than the initial shocks, in a small portion of cases the opposite is true, with responses being more than three times larger. In addition, a cumulation of multiple adverse shocks (as was for instance the case during the COVID-19 pandemic) can have more significant implications.

Statistics summarising responses to such highly adverse constellations of shocks suggest that some sectors and countries may be more exposed than others. Economies with strong vertical links to major foreign economies tend to be more exposed to GVC shocks, with Canada, France, Germany and the United Kingdom leading the rankings, and the United States, Brazil and China being relatively less exposed due to their greater reliance on domestic product and factor markets in most sectors. Russia and South Africa move to the top of the ranking of the most exposed countries under the assumption of immobile factors. This is because the sectors in which they tend to specialise, such as petroleum and coal, mining and chemicals, are more exposed to external shocks and have more difficulty adjusting when labour and capital cannot migrate to other sectors (Figure 1.6).

Figure 1.6. Maximum exposure to GVC shocks across countries

A maximum per cent combined impact of all possible 1%-shocks



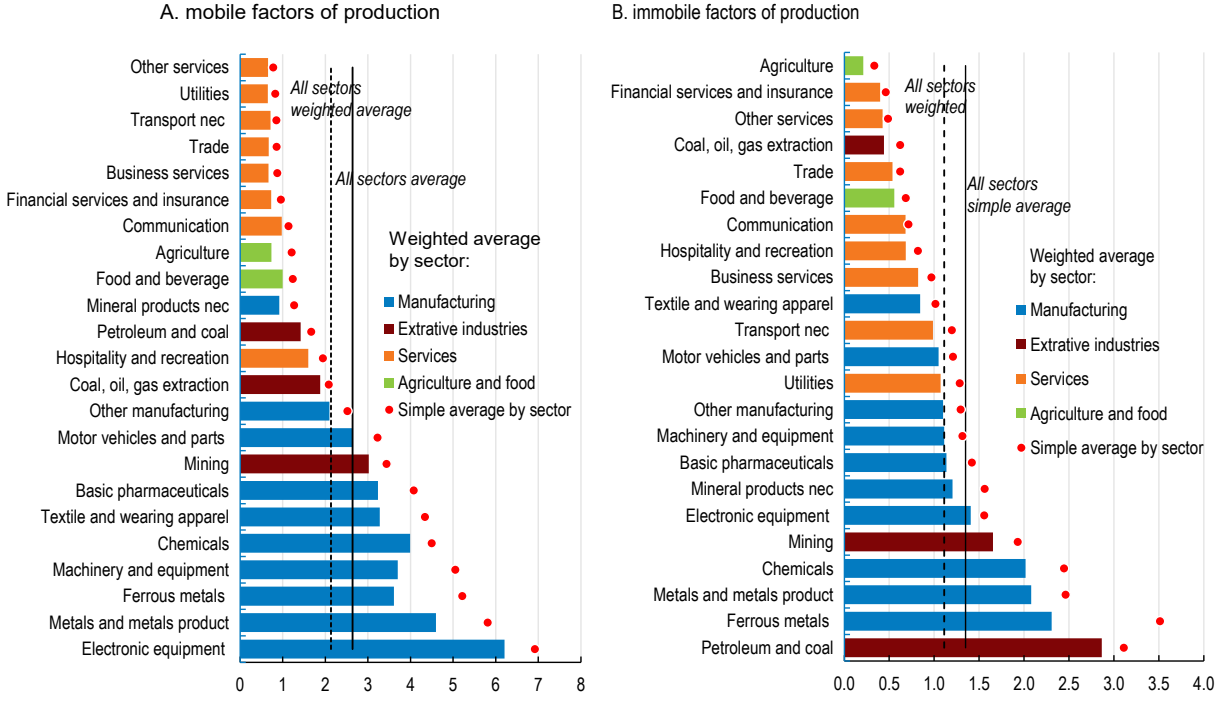
Note: Value of output at the starting point of the simulation are used as weights to produce weighted averages.
Source: OECD METRO model simulations.

There is more variation in the measures of exposure across sectors than there is across countries, suggesting potential for sectoral initiatives to address exposure to shocks. Manufacturing sectors are on average much more exposed to foreign output shocks than services sectors and agriculture and food because they are more internationalised in terms of destination of output as well as sourcing of intermediate inputs. For this reason, manufacturing of electronics, non-ferrous metals, iron and steel, machinery and equipment, and chemicals appear as the most exposed. When production factors are immobile, extractive industries, as well as the manufacturing sectors linked to them (metals, iron and steel, and chemicals) move towards the top of shock exposure rankings (Figure 1.7).

There are also important differences across countries and sectors in terms of which shocks contribute the most to exposure. For example, Germany's motor vehicles sector, while less exposed to GVC shocks than manufacturing of electronic equipment or metals,[9] tends to be relatively more exposed than that of the United States, and a bigger portion of this exposure can be attributed to shocks originating in China.

Services sectors, which in some countries employ large shares of labour resources (e.g. hospitality and recreation, retail trade, construction or warehousing and support activities), can be sources of shocks with relatively big impacts across the global economy. However, these tend not to be transmitted through constrained access to, or demand for, intermediate inputs, but rather through domestic economy-wide impacts involving factor markets. In the medium to long run, an output reduction in those sectors tends to be associated with a release of labour and capital that finds employment in other parts of the economy, which impacts other sectors. Shocks to business services, a sector which has strong upstream and downstream linkages to manufacturing sectors, are characterised by more classical transmission of vertical foreign shocks through GVCs.

Figure 1.7. Maximum exposure to GVC shocks across global sectors



Note: Value of output at the starting point of the simulation are used as weights to produce weighted averages.
Source: OECD METRO model simulations.

De-risking supply chains: Possible economic effects of policy-induced trade fragmentation scenarios

The discussion in the preceding sections demonstrates that some trade linkages appear relatively highly concentrated and that this may increase the probability of economic or other damage in the context of large, unexpected shocks or trade-related economic coercion. This confirms the merit in monitoring measures of trade concentration and anticipating impacts of possible shocks and disruptions. However, this might also suggest a greater scope for policymakers to induce trade diversification to de-risk certain trade linkages.

Most recently, concerns about trade dependencies and exposure to shocks, the growing role of strategic economic policies and raising geopolitical tensions have indeed resulted in a new wave of calls for deglobalisation, friendshoring, nearshoring, creation of trading blocks or re-localisation (e.g. Arriola et al. (2020[3]), Crowe and Rawdanowicz (2023[14])). Calls for economic security and strategic autonomy, and the associated pleas to limit dependency on foreign economies, are putting open markets and the rules-based trading system under pressure. At the same time, the calls to enhance economic security may also reflect a response to (sometimes very real) weaponisation of trade dependencies and other coercive practices, which undermine the rules-based trading system in the first place. There are also concerns that some of the policy responses which aim to minimise trade risks and improve supply chain resilience may not be well designed and may in fact unnecessarily undermine the benefits of international trade. Thus, the debate on de-risking international trade and supply chains needs to carefully consider the possible costs and benefits of different policy choices.

Until recently, there was no clear evidence of a major reorganisation of international supply chains towards reshoring or geoeconomic fragmentation. That said, the plateauing of the world trade-to-GDP ratio observed already since the 2008-09 GFC indicates a slowdown in economic globalisation. There are also signs that some of the newly implemented or considered policy responses are reshaping the regulatory landscape of supply chains and becoming key drivers of potentially long-term strategic decisions of firms. This can be seen, for example, in results of recent surveys on resilience-improving strategies of businesses (e.g., Accenture (2023[15]) and EconPol (2024[16])) and the reorientation of bilateral trade between China, and the United States and the European Union, as well as in the growing importance of third economies (OECD, 2024[17]).The emerging empirical evidence demonstrates a relatively high degree of trade interdependence. To the extent that fragmentation could involve undoing international supply chains, break the supply of critical raw materials and endanger technology transfers and the division of labour across countries at different levels of development, the economic costs of significant trade fragmentation are potentially high.

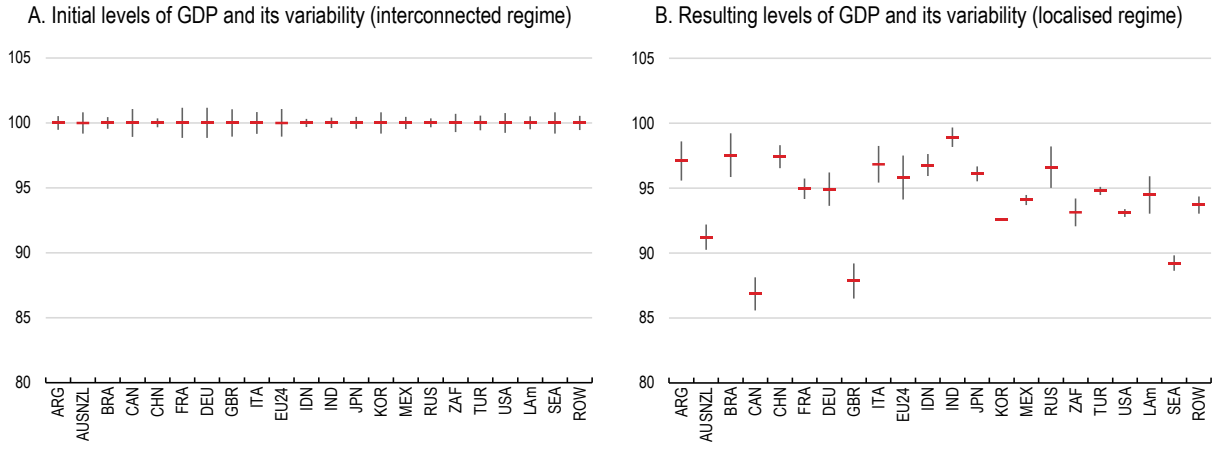
Model-based estimates of possible fragmentation scenarios can be informative but depend ultimately on assumptions about the extent and nature of fragmentation, ranging from scenarios of small increases in trade policy barriers, through discriminatory regional integration, to the formation of more or less autarchic geopolitical trading blocs. Model-based analyses of the costs of fragmentation have proliferated in the aftermath of the COVID-19 pandemic and, even more so, Russia's invasion of Ukraine. A summary of studies of trade fragmentation in the aftermath of Russia's invasion by IMF (2023[18]) concluded that the costs from the trade and technology diffusion channels range from close to zero to 12% of a country's or region's GDP.[10] They also suggest that developing and emerging market economies would lose the most (although, again, the estimated costs depend very much on uncertain assumptions).

An OECD METRO model-based analysis, motivated by the early COVID-19 supply chain disruptions and strong calls for re-localisation of supply chains at the time, compared simulated impacts on economic efficiency and the extent of international transmission of country-specific trade cost shocks under different assumptions about countries' openness and integration into GVCs. It showed that the policies that may result in more localised value chains are likely to be costly in terms of efficiency and do not necessarily

offer more stability in the face of shocks (Arriola et al., 2020[3]) (Figure 1.8). The localised economies regime, which assumed an implementation of a suite of hypothetical and stylised re-localisation policy responses where all countries decided to reduce their connectedness via GVCs through a combination of higher import tariffs, subsidies to domestic production and putting additional constraints on sourcing possibilities in GVCs, was estimated to decrease global trade by more than 18% and global real GDP by more than 5% relative to the interconnected regime, with individual countries losing between 1.1 and 12.2% of GDP depending on the extent and nature of their GVC integration. In addition, when the effects of a stylised set of "supply chain" shocks were modelled,[11] contrary to some of the claims in the general debate on risks in GVCs, in the localised regime, shocks did not result in a significant increase in the stability of GDP, production and consumption relative to the interconnected regime. In fact, for more than half of the economies, the stability of GDP decreased in the localised regime. This is because openness and geographical diversification of the sources of inputs and destinations of output in GVCs can offer possibilities of adjustment to disruptions.

Figure 1.8. GDP level and variability a more localised supply chain scenario

Simulated impact on GDP of selected OECD and MOE economies of a supply chain localisation scenario



Note: All changes in variables are relative to the level of the interconnected regime base scenario, which is set to equal 100. Blue dots show the base in the given regime relative to the interconnected base and whiskers show average deviations for negative and positive trade cost shocks
Source: Arriola et al. (2020[3]), "Efficiency and risks in global value chains in the context of COVID-19", OECD Economics Department Working Papers, No. 1637, OECD Publishing, Paris, https://doi.org/10.1787/3e4b7ecf-en.

A recent OECD study (Arriola et al., 2024[8]) of the economy-wide dimensions of trade dependencies considered possible economic implications of a hypothetical and highly stylised scenario that partially reduced trade between the OECD and major non-OECD economies (MOEs).[12] The scenario assumed that all goods and services trade flows between each of the OECD countries and each of the MOEs are reduced by 10% (hereafter a trade reduction shock or a trade shock). All other trade flows were assumed to remain directly unaffected, but they could be affected indirectly, for example through interruption of indirect links involving OECD-MOE trade if such links exist, or through redirection of trade and other economic adjustments.

This scenario was analysed using the OECD Inter-Country Input-Output tables (ICIO) and Input-Output analysis methods[13] and the OECD's CGE trade model METRO. Albeit allowing for different levels of country and industry detail and putting different emphases on various economic adjustment mechanisms, both the ICIO and the CGE approaches allow for assessment of economy-wide implications of trade dependencies. They also take a broader supply chain perspective and capture not only those trade

dependencies that are due to direct import-export relationships but also those that may result from indirect trade links (e.g. when a product exported from one country to another embeds a component produced in a third country). Importantly, these methodologies enable analysis of direct and indirect dependencies in the services sectors.

Overall, the results of this analysis (Arriola et al., 2024[8]) confirm a high degree of trade interdependence of the two groups of countries (and especially between OECD countries and China) and illustrate some of the economic costs that may be involved in the currently debated strategies of de-risking supply chains:

- Most OECD and MOE countries lose in the trade reduction scenario; that said there is significant inter-country variation and the estimated impacts depend on the modelling approach used. Depending on the modelling framework used and country considered GDP declines range from nil to about 1.7%.
- OECD countries and sectors with stronger trade linkages with MOEs rather than with other OECD economies fare worse, while stronger linkages within the OECD help mitigate the impacts of the trade shock. The OECD countries in the Asia Pacific, in particular Korea and Australia, are affected the most while the OECD countries in Europe are affected moderately and those in North America remain largely unaffected.
- Across all OECD regions, the main driver of these GDP reductions is the decrease in trade with China, even though some OECD countries also have noticeable exposures to other MOEs. This is not surprising, given that China accounts for almost two-thirds of the MOEs' overall trade with the OECD.
- The considered trade shock is found to impact the GDP of some MOE countries even more than for OECD countries. This is because the export and import links disrupted in this scenario represent a larger share of the economy in MOEs.

In any given country, not all sectors of the economy are exposed to the considered trade shock to the same degree.[14] The list of the most impacted industries varies from one country to another, but it is reasonably common to find the highest levels of exposure in the primary sector and, more specifically, in the mining and quarrying cluster. This is because the trade shock constrains several important flows of mineral resources between OECD and MOEs.

Conclusions

Results of recent exploratory OECD empirical analyses attempting to quantify the historical evolution and economic significance of trade dependencies illustrate some of the concerns that lie beneath the debate on trade. Global production of at least some products has become increasingly concentrated, and increasingly clustered around some countries and regions. Therefore, shocks related to climate change, changes in economic policy or geopolitical conflicts, arguably may have a higher potential to disrupt commercial links and cause economic or societal damage. Concentration can also give rise to concerns about policy-induced issues with security of supply, such as economic coercion.

While the growing concentration of trade may be shaped by market economic factors, such as natural endowments, comparative advantage, economies of scale, or GVC fragmentation, it may also have been influenced by non-market policies and notably by government support. There is thus interest in a better understanding of the reasons for the growth of concentration. In particular, the contributions of natural and policy-related factors, including policies which may have involved market distortions or targeted non-economic objectives, need to be better understood.

While trade concentration has grown on average, large – if not dominant – portions of global and national trade remain relatively well diversified overall. As suggested by the concentration profile of global trade flows, international product markets also are generally characterised by a reasonable degree of

competition and limited control over supply or price formation of specific importers or exporters. Moreover, it is difficult to distinguish those concentrated trade links that could cause problems from advantageous trade linkages. There are legitimate concerns that policy responses which aim to minimise trade risks and improve supply chain resilience may not be well designed and may unnecessarily undermine the benefits of international trade.

In this context, the current debate on de-risking international trade needs to consider carefully the possible costs and benefits of different policy choices. The different methodologies used to produce evidence all demonstrate a relatively high degree of trade interdependency between the OECD and MOE countries (and especially between OECD countries and China) as well as potentially high economic costs of significant trade fragmentation.

References

Accenture (2023), Resiliency in the making: Turning adversity into advantage for engineering, supply, production and operations, Accenture. [15]

Antras, P. and R. Staiger (2012), "Offshoring and the Role of Trade Agreements", American Economic Review, Vol. 102(7), pp. 3140–3183. [4]

Arriola, C. et al. (2024), "Towards demystifying trade dependencies: At what point do trade linkages become a concern?", OECD Trade Policy Papers, No. 280, OECD Publishing, Paris, https://doi.org/10.1787/2a1a2bb9-en. [8]

Arriola, C. et al. (2020), Efficiency and risks in global value chains in the context of Covid-19, https://doi.org/10.1787/18151973. [3]

Baker, S., N. Bloom and S. Davis (2016), Measuring Economic Policy Uncertainty, https://www.policyuncertainty.com/media/EPU_BBD_Mar2016.pdf. [6]

Baldwin, R. (2011), "Trade and Industrialization after Globalization's Second Unbundling: How Building and Joining a Supply Chain Are Different and Why It Matters", NBER Working Papers, Vol. Working Paper No.17716, https://www.nber.org/papers/w17716. [1]

Berthou, A., A. Haramboure and L. Samek (2024), "Mapping and testing product-level vulnerabilities in granular production networks", OECD Science, Technology and Industry Working Papers, No. 2024/02, OECD Publishing, Paris, https://doi.org/10.1787/9bcde495-en. [13]

Bonneau, C. and M. Nakaa (2020), "Vulnérabilité des approvisionnements français et européens", Trésor-Éco n° 274, Ministère de l'Économie, Des Finances, et De La Relance, France, https://www.tresor.economie.gouv.fr/Articles/511478e4-5fb3-48a6-afbc-edc5186be04c/files/e1968df8-f94a-4718-bbeb-992db19864e6. [10]

Caldara, D. and M. Iacoviello (2022), "Measuring Geopolitical Risk", American Economic Review, Vol. 112(4), pp. 1194–1225, https://doi.org/10.1257/aer.20191823. [7]

Crowe, D. and L. Rawdanowicz (2023), Risks and Opportunities of Reshaping Global Value Chains, OECD Publishing, https://doi.org/forthcoming. [14]

EconPol (2024), Reconfiguration of Supply Chains: What Are the Priorities of German Firms?, [16]
https://www.econpol.eu/publications/policy_brief_56/reconfiguration-of-supply-chains.

European Commission (2022), EU strategic dependencies and capacities: second stage of in-depth reviews. Commission Staff Working Document SWD (2022) 41, [11]
https://www.europeansources.info/record/eu-strategic-dependencies-and-capacities-second-stage-of-in-depth-reviews/.

IMF (2023), Geoeconomic Fragmentation and the Future of Multilateralism, International Monetary Fund, https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2023/01/11/Geo-Economic-Fragmentation-and-the-Future-of-Multilateralism-527266. [18]

Kowalski, P. et al. (2015), "Participation of Developing Countries in Global Value Chains: Implications for Trade and Trade-Related Policies", OECD Trade Policy Papers, No. 179, OECD Publishing, Paris, https://doi.org/10.1787/5js33lfw0xxn-en. [20]

Lafrogne-Joussier, R. (2021), Supply shocks in supply chains: Evidence from the early lockdown in China, https://cepr.org/active/publications/discussion_papers/dp.php?dpno=16813. [2]

Miller, R. and P. Blair (2022), Input-output analysis: foundations and extensions (3rd edition), Cambridge University Press. [19]

OECD (2024), Risks and Resilience in Global Trade: Key Trends in 2023-2024, OECD Publishing, Paris, https://doi.org/10.1787/1c66c439-en. [17]

Schwellnus, C. et al. (2023), "Global value chain dependencies under the magnifying glass", OECD Science, Technology and Industry Policy Papers, No. 142, OECD Publishing, Paris, https://doi.org/10.1787/b2489065-en. [9]

Staiger, R. (2022), A World Tradeing System for the Twenty-First Century, Massachusetts Instutute of Technology. [5]

Vicard, V. and P. Wibaux (2023), EU Strategic Dependencies: A long view. CEPII Policy Brief No. 41 June 2023, http://www.cepii.fr/PDF_PUB/pb/2023/pb2023-41.pdf. [12]

Notes

[1] OECD Trade and Agriculture Directorate.

[2] In policy debates, "moving up the value chain" has been often understood as – either commercially-driven or government-induced – transition to activities characterised by relatively "high value added" (for example at product design and marketing stages rather than assembly or manufacturing stages) or even as the

need to capture a growing share of domestic value added in exports. This view of upgrading, however, misses the point that the volume of the activity also matters and if a country or a firm has an advantage of performing assembly or manufacturing at scale, it may obtain more economic benefits from focusing on these supply chain activities (Kowalski et al., 2015[20]).

[3] Considered from a longer historical perspective, the level of geopolitical risk in the early 2020s, as measured by this methodology, was higher than that in the late 1990s. However, it was still markedly lower than during previous episodes of geopolitical tensions, for example around the Gulf War, Korean War and, particularly, World War I and World War II (Caldara and Iacoviello, 2022[7]).

[4] There have been cases where trade interdependencies have been exploited for the purposes of interfering with the legitimate sovereign policy choices of another country. While there is no internationally agreed definition, such instances have been characterised as "economic coercion" (OECD, 2024[17]).

[5] The analysis covers all countries which report internationally comparable trade data but in examining the nature and evolution of trade dependencies it focuses on OECD and major other economies (NOEs), where the latter grouping is composed of Brazil, China, India, Indonesia, Russia and South Africa.

[6] Products are here defined at the Harmonised System 6-digit (HS6) level of product aggregation.

[7] This work analysed simulated responses of output of national economic sectors to production shocks occurring in other domestic and foreign sectors connected vertically through supply chains and horizontally through competition in product markets. In addition to assessing the overall magnitude and nature of shock transmission, the analysis identified countries and broad sectors which may be particularly vulnerable to shocks or could be a more significant source of risk.

[8] That said, the differences in impacts under different factor mobility assumptions vary across sectors and depend also on whether the impacted sector has a significant weight in domestic labour and capital markets.

[9] For instance, the country's exposure to GVC shocks in the electronics industry is approximately twice as high. For more on industry and country exposure see Arriola, Kowalski and Tongeren (Arriola et al., 2024[8]).

[10] There are also the migration and cross-border capital flows and financial integration channels which are less explored.

[11] The spectrum of shocks included equally probable and spatially uncorrelated increases and decreases in the cost of bilateral trade (for both imports and exports) between each country or region included in the model and all its trading partners.

[12] The MOE grouping includes Brazil, China, India, Indonesia, Russia and South Africa. This focus is purely analytical and is without prejudice to the relationships between the OECD or any of its members and any of the individual countries of the MOE grouping.

[13] The principal method used in this analysis is called 'hypothetical extraction' (Miller and Blair, 2022[19]). The hypothetical extraction method evaluates the economic significance of certain economic connections

by calculating what would happen if those connections were removed or reduced while preserving the rest of the global trade and economic activity structure. For more details, see (Arriola et al., 2024[8]).

[14] In several cases, the sectors identified as the most heavily dependent on OECD-MOE trade represent only small shares of their country's economy. On the other hand, the list of highly impacted industries also includes those of great significance from both a domestic and a global point of view.

2. Special focus : Semiconductor value chains

Antton Haramboure, Guy Lalanne, Lea Samek and Angela Attrey[1]

Semiconductors are fundamental building blocks of digital technology. They not only play a crucial role in fields such as artificial intelligence (AI) and quantum computing, but also are embedded in a myriad of everyday products. For example, a modern car might contain up to 3,000 semiconductor chips, which control everything from battery management and fuel injection to infotainment systems (Ewing and Boudette, 2021[1]). The semiconductor shortages that occurred following the COVID-19 pandemic underscored that access to these critical components cannot be taken for granted. In this context, a number of countries have recently adopted policy initiatives to strengthen domestic production of semiconductors (Box 2.1).

Box 2.1. Selected recent policy initiatives to enhance semiconductor supplies

The US CHIPS and Science Act

The CHIPS and Science Act, introduced in the United States in 2022, aims at strengthening US competitiveness, innovation, national security in the semiconductor sector and increasing a science, technology, engineering and math (STEM) workforce. The main measures involve tax credits for investment in manufacturing, sectoral research and development (R&D) funding, and funding for education and skills. The act appropriated around USD 53 billion (0.2% of GDP) over five years for these objectives, including around USD 39 billion of incentives for building semiconductor plants and around USD 13 billion for supporting R&D and workforce in this area. It provided a 25% tax credit for building and equipping the plants initiated before 2027. The credit is estimated to cost USD 24.3 billion over ten years. It also significantly increased authorised spending for federal science and technology R&D programmes, administered by multiple federal agencies (amounting to around USD 174 billion through fiscal year 2027, equivalent to 0.7% of 2022 GDP).

The CHIPS and Science Act also involves measures to hinder the expansion of semiconductor manufacturing in China or any other countries that pose a threat to US national security. With limited exceptions, it prohibits recipients of its funding and investment tax credits from expanding semiconductor manufacturing in countries posing national security threat for ten years. The act also includes several provisions related to research security.

At the same time, the United States has implemented measures to regulate the export of advanced semiconductors and chipmaking equipment to China. In October 2022, export controls were introduced to prohibit the transfer of cutting-edge chips and manufacturing tools to Chinese firms with government

ties. These restrictions were expanded in 2023 and 2024 to close gaps, limit sales to data centres, and target additional companies.

The European Chips Act

The European Chips Act came into force in September 2023. It aims at fostering semiconductor production in the European Union, reducing external dependencies, and doubling the EU's global market share to 20% in 2030. The act is based on a three-pillar structure: the "Chips for Europe" initiative which seeks to support research, development and innovation in the EU chips ecosystem and improve the transition "from lab to fab"; the second pillar focusing on improving supply security with a new framework to attract large-scale investments in production capacities; and the last pillar aiming at setting up a co-ordination mechanism between member states and the Commission to monitor market developments and anticipate crises. The act provides derogations to state aid rules for key facilities, reallocates EUR 3.3 billion (0.02 % of GDP) from existing EU funds to relevant projects, complemented by EUR 2.9 billion, and seeks to rationalise investment by member states. The European Commission intends to mobilise EUR 43 billion (0.3% of GDP) in public and private funds through the act, with EUR 11 billion coming from repurposing existing funds. EU subsidies are provided for investment in new, first-of-their kind facilities.

Japan's "Strategy for Semiconductor and the Digital Industry"

In June 2021, the government announced a new "Strategy for Semiconductor and the Digital Industry", seeking to increase domestic development and production of advanced semiconductors as well as other advanced technologies critical for the digital and green transitions. The revised strategy (in June 2023) has a goal to reach more than JPY 15 trillion sales of domestically produced semiconductors by 2030. The strategy relies on tax breaks and subsidies for companies investing in semiconductors, data centres or other critical technologies, but does not provide precise budget costing of these measures. In the context of this strategy, Japan supported the creation of a new chip venture called Rapidus Corp, with public financial support worth JPY 330 billion.

This special focus aims to shed light on the semiconductor industry's position in global value chains (GVCs) and to identify some of the critical features of the semiconductor value chain itself. It makes use of the OECD semiconductor-augmented Inter-Country Input-Output (ICIO) tables built by Haramboure et al. (2023[2]). Together with highly detailed trade data, they help to map various stages of semiconductor value chains, revealing potential vulnerabilities from the fragmentation of this complex large-scale production process.[2]

The analysis shows that the semiconductor industry is positioned well upstream in GVCs, with its production highly concentrated in a few key economies, predominantly in Asia. A granular description of the semiconductor value chain reveals its considerable fragmentation, wherein various countries exhibit strong leadership at different stages of production. This configuration creates substantial interdependencies across countries, introducing potential vulnerabilities. Disruptions in any leading economy within this value chain could lead to widespread shortages, significantly impacting numerous downstream industries and economies worldwide.

The resilience of semiconductor GVCs can be enhanced through increased diversification, particularly by establishing new manufacturing facilities. This expansion will require substantial investments and rely on the availability of a skilled workforce and robust infrastructure. The OECD supports policies to develop semiconductor talent and address worker shortages through enhanced science, technology, engineering and mathematics (STEM) education and industry-education collaboration. It also helps design public policies to support the semiconductor industry by ensuring access to ultraclean water, reliable energy sources, and robust transport infrastructure for seamless production and distribution.

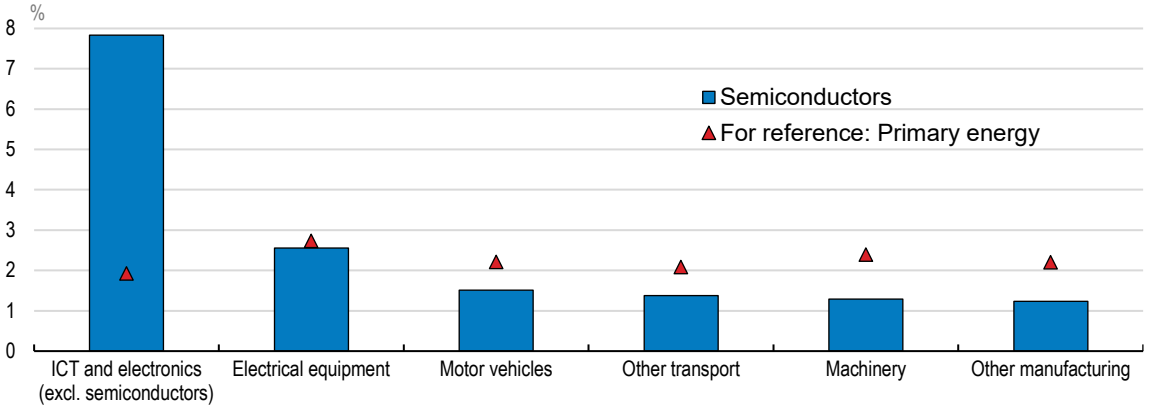
Semiconductors are a key upstream sector, with production concentrated in Asia

Metrics from the OECD semiconductor-augmented ICIO tables underscore the unique position of semiconductors in GVCs. ICIO tables provide detailed economic data on the interconnections between industries and countries and facilitate the analysis of GVCs. Semiconductors are key inputs for many industries, with their production situated upstream and heavily concentrated in Asia across all semiconductor types.

The semiconductor industry is a critical supplier for several key manufacturing sectors (Figure 2.1). Semiconductors are at least as important as primary energy in the production of manufacturing sectors such as ICT and electronics, motor vehicles and machinery manufacturing sectors. For instance, electrical equipment production requires the same amount of value added from the semiconductor industry as from primary energy. The manufacturing of ICT and electronics is particularly reliant on semiconductors, with semiconductor value added accounting for 8% of final demand, significantly exceeding the 2% contribution from the primary energy sector. This suggests that a disruption in semiconductor supply could have significant negative effects on the ICT and electronics industry and semiconductor supply should be considered as important (if not more) than primary energy supply. Moreover, unlike energy, semiconductors are highly heterogeneous and often specific to the product or application of the electronic device, reducing their substitutability.

Figure 2.1. Semiconductors are a crucial input into a range of industries

Share of semiconductor and primary energy value added in final demand, 2018



Note: The sample is restricted to the leading semiconductor purchasing economies: Brazil, Canada, China, France, Germany, Hong Kong (China), Ireland, Italy, Japan, Korea, Malaysia, Mexico, the Netherlands, the Philippines, Singapore, Switzerland, Chinese Taipei, Thailand, the United Kingdom and the United States. Primary energy includes coal, oil and gas.
Source: Haramboure et al. (2023[1]) based on OECD semiconductor-augmented ICIO tables.

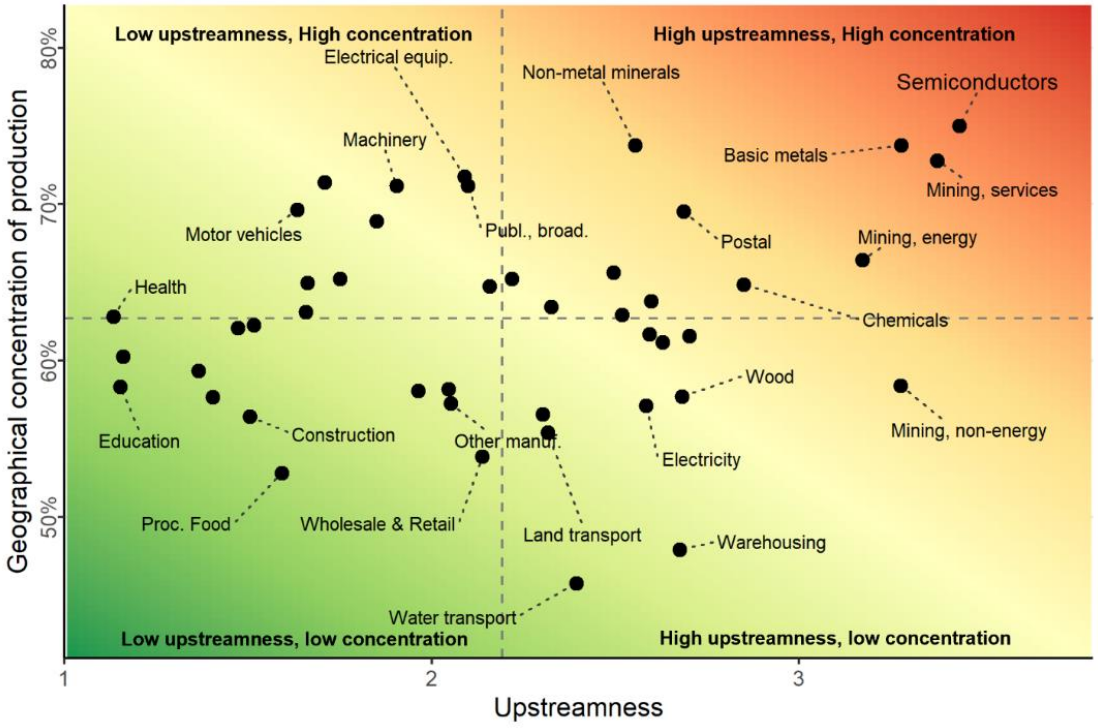
The semiconductor industry is the most upstream industry in the ICIO database (Figure 2.2). Once manufactured, semiconductors are integrated as intermediary inputs that can pass through numerous intermediary production stages before being incorporated into final consumer products, comparable to industries which supply raw materials, like mining and basic metals. Because semiconductors are a highly upstream input, disruptions in semiconductor production could impact a multitude of downstream industries that directly or indirectly depend on chips.[3]

The semiconductor industry is also the most geographically concentrated industry in the semiconductor-augmented ICIO tables, with approximately 75% of its value-added generated by five

economies – four of which are in Asia (Figure 2.2 and Figure 2.3). This significant concentration in Asia stems from a gradual redistribution of value-added generation since 1995, moving from Japan and the United States to China, Korea and Chinese Taipei. This shift notably coincided with many US semiconductor companies adopting a "fabless" production model, whereby foundry and packaging tasks are outsourced, and the fabless firm focuses on chip design. Additionally, the increasing importance of economies of scale has driven greater industrial and geographical concentration within the sector. Consequently, a few leading firms, mainly operating in a few economies, account for a larger share of the industry's profits (McKinsey & Company, 2021[3]).

Figure 2.2. Semiconductor production is highly upstream and highly concentrated

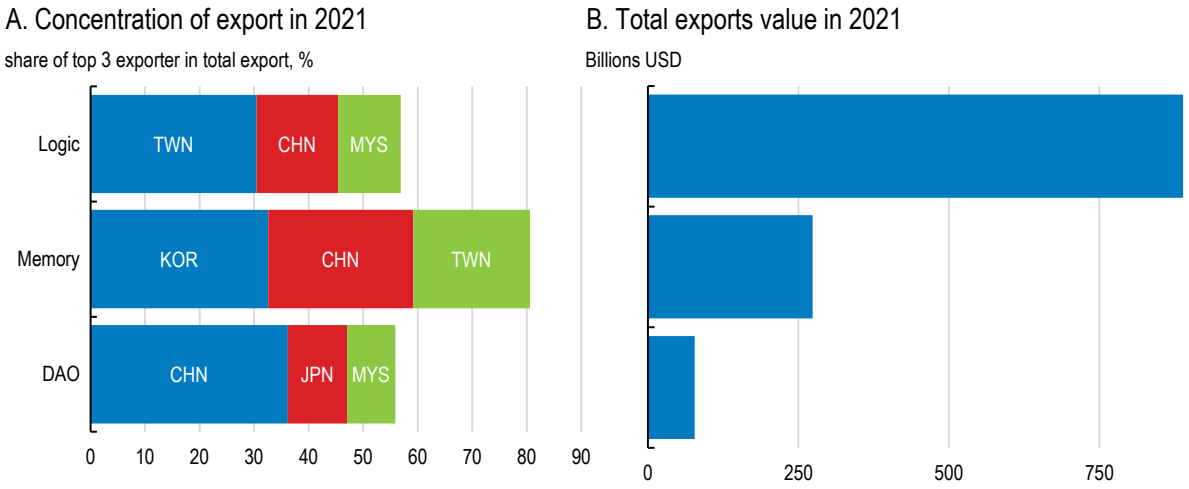
Concentration (share of top five economies in global value added) and upstreamness (distance to final demand), 2018



Note: Geographical concentration of production is measured as the share of the top five economies in global value added of an industry. Upstreamness of an industry is measured as the distance to final demand (Antràs et al., 2012[4]).
Source: Haramboure et al. (2023[1]) based on OECD semiconductor-augmented ICIO tables.

In addition, semiconductor chips are diverse, serving different purposes, and are produced using different manufacturing processes. As a result, concentration is even higher for some specific types of semiconductors, as illustrated by trade data for 2021 in Figure 2.3, which separately measures export value and concentration for logic, memory and DAO ("Discrete, Analog and Others") chips.[4] Memory chips, which account for about a fifth of semiconductor export value, exhibit a particularly high concentration, with the top three exporting countries – all located in Asia – capturing over 80% of the exports. Although the top three exporting economies differ by semiconductor type, they are also located in Asia and account for over 55% for logic and DAO chips. Concentration is particularly high among the most advanced logic chips, which are crucial for AI development. According to 2022 data, these chips are only produced by Samsung in Korea and TSMC in Chinese Taipei (BCG and SIA, 2024[5]).

Figure 2.3. China, Korea and Chinese Taipei lead different segments of the semiconductor industry

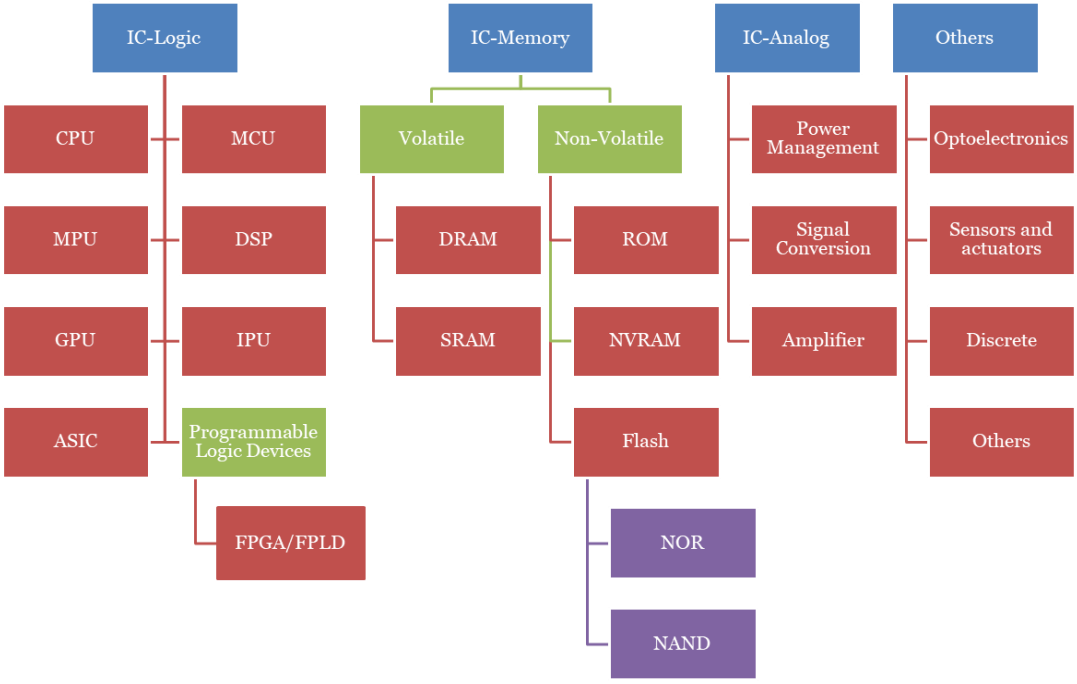


Note: Logic, memory and DAO semiconductor segment group goods under headings 8541 and 8542 of the Harmonised Systems.
Source: Haramboure et al. (2023[1]) based on COMTRADE, and OECD calculations.

Altogether, these features demonstrate that, while semiconductors are widely used across many industries, their production is concentrated in a narrow set of economies. This underscores a significant vulnerability: a disruption in semiconductor production within a single leading economy could precipitate widespread shortages affecting diverse downstream industries and economies worldwide.

More comprehensive data are required to better understand the complex value chain for semiconductors, including potential bottlenecks, vulnerabilities and substitutability. A technical paper by the OECD (2024[6]) sets out a common taxonomy for semiconductor types, distinguishing between four broad categories, namely: Logic, Memory, Analog and Others, as well as sub-categories based on their prevalence and specific functions (Figure 2.4). The taxonomy also characterises semiconductor front-end facilities by the detailed category of chips produced and the technologies and equipment available. This taxonomy provides the basis for a living semiconductor production database to better understand the wider landscape of semiconductor production.

Figure 2.4. A taxonomy of semiconductor types



Note: IC stands for integrated circuit; CPU central processing unit, MCU microcontroller unit; MPU microprocessor unit; DSP digital signal processors; GPU graphics processing unit; IPU intelligent processing unit; ASIC application-specific integrated circuits; FPGA field programmable gate array; FPLD field programmable logic device; DRAM dynamic random-access memory; ROM read-only memory; SRAM static random-access memory; NVRAM non-volatile random-access memory; NAND *Not And;* NOR *Not Or*.
Source: OECD (2024[6]).

The segmented semiconductor value chain creates interdependencies among leading economies

A structured definition of the semiconductor industry can clarify essential interdependencies within the industry itself, as well as with the key inputs, technologies and capital goods necessary for the semiconductor production.

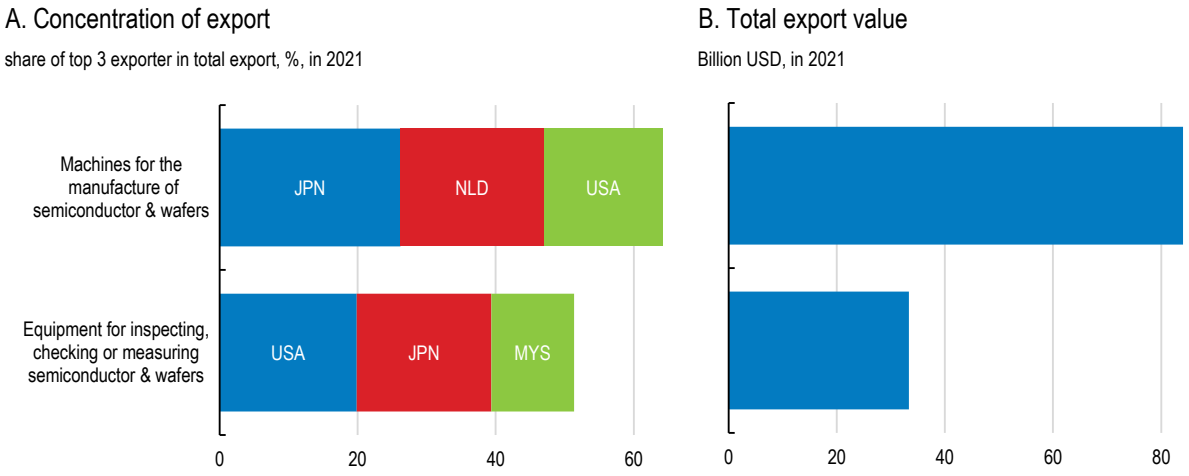
In the OECD semiconductor-augmented ICIO tables, the semiconductor industry is delineated into three fundamental stages of production: chip design, wafer fabrication, and assembly, test and packaging (ATP). The industry showcases a variety of business models, with certain firms integrating all production stages, while others specialise in only one. Countries have specialised in distinct segments according to their comparative advantages. As already mentioned, US firms have, for example, retained a substantial share of the design activities (McKinsey and Company, 2022[7]; BCG and SIA, 2024[5]). This specialisation has fostered significant complementarities between leading economies, notably between US fabless firms and Chinese Taipei's pure-play foundries (McKinsey and Company, 2022[7]).[5]

The interdependencies within the semiconductor industry extend beyond its three core production stages, reaching upstream steps. Alongside dominating the design of chips, US firms also hold a substantial lead in the technologies that enable this process. More precisely, in the Electronic Design and Automation (EDA) tools and Intellectual Property (IP) market, US headquartered firms held a substantial 72% of global sales in 2020 (McKinsey and Company, 2022[7]) and 68% of global revenue in 2022 (BCG and SIA, 2024[5]).

There is also a strong concentration in the exports of raw materials and capital goods necessary for the production and fabrication of semiconductors. Exports of silicon, for instance, are highly concentrated, with

the United States, Germany and China playing the leading roles. Trade data also show that both exports of machines to manufacture semiconductors and the fabrication of wafers are more concentrated than exports of most types of semiconductors (Figure 2.5.). Anecdotal evidence suggests an even greater concentration for machines required to manufacture leading-edge chips (less than 10 nm feature size).[6] The United States, Japan and Malaysia lead the exports of other equipment tools used for the inspection and testing of semiconductors and wafers. However, the level of aggregation of Figure 2.5 obscures that although not among the leading economies in semiconductor production, some economies like Czechia, Israel, and the Netherlands are leading exporters of various specialised equipment used to manufacture and check semiconductor and wafers (Haramboure et al., 2023[2]). This highlights a niche area of expertise and significant export capability within these countries despite their smaller role in broader semiconductor production.

Figure 2.5. Exports of semiconductor machinery are even more geographically concentrated than exports of semiconductors



Note: The plot represents the share of top three exporters in total exports for several goods of the semiconductor value chain.
Source: Haramboure et al. (2023[2]) based on COMTRADE, and OECD calculations.

Disruptions may have different effects depending on which part of the value chain is affected. Disruption at the production stage may result in significant short-term negative impacts on many industries, as semiconductors are not easily substituted, and adjusting supply is slow and costly. Increasing manufacturing capacity requires large upfront investments, long lead times and access to a highly specialised talent pool, implying slow supply adjustment. Building a manufacturing plant for leading-edge semiconductors, for instance, requires an upfront investment of USD 10-20 billion (Shih, 2021[8]). In contrast, disruption in the supply of machines may take more time to affect semiconductor production.

The semiconductor value chain is characterised by high segmentation and specialisation of countries in some production stages following their comparative advantage. As a result, no country is currently involved in all the steps of the value chain, nor is it able to produce all types of semiconductors needed by downstream industries. This combined segmentation and concentration not only expose leading semiconductor economies to vulnerabilities from potential disruptions affecting other participants in the value chain, but also create a high level of interdependence. This pattern is especially significant for the production of the most advanced semiconductors.

Enhancing resilience of semiconductor value chains through international collaboration: the OECD's Semiconductor Informal Exchange Network

With an increasing number of policy actions targeting semiconductors around the world (Box 2.1), sharing information, identifying best practices, and enhancing international dialogue and collaboration will be key to increasing the resilience of semiconductor value chains. Accordingly, the OECD convened the Semiconductor Informal Exchange Network (SIEN) in June 2023, bringing together senior policymakers in the semiconductor industry to promote information and data exchange and policy dialogue. The SIEN led to, among other things, the adoption of the common taxonomy described earlier (2024[6]). It is also working on enhancing transparency across different segments of the value chain to establish a mechanism for anticipating and managing value chain disruptions. In addition, it aims to bring together policymakers to share their experiences with semiconductor policies, including lessons learned and best practices.

The OECD also supports the design of policies that foster the emergence of local semiconductor ecosystems, thus contributing to a more diverse and resilient global semiconductor value chain. Recognising the significant investment required for new manufacturing capabilities, particularly in advanced chip production which can often reach tens of billions of dollars (Shih, 2021[8]), several OECD countries are introducing ambitious incentives such as subsidies and tax breaks to stimulate industry investments.

The success of new manufacturing facilities depends heavily on the availability of a skilled workforce and access to critical infrastructure. The OECD supports policies to develop skills and semiconductor talent to address the growing shortage of qualified workers (Deloitte, 2023[9]; McKinsey & Company, 2024[10]). The global shortage in semiconductor skills, requires renewed efforts in STEM education from an early age, together with enhanced collaboration between industry and education institutions to design appropriate curricula for both higher education and vocational education and training institutions. Finally, the OECD helps design public policies that support the semiconductor industry by ensuring access to critical infrastructure, including water, reliable and clean energy, as well as robust air and sea transport infrastructure.

References

Antràs, P. et al. (2012), "Measuring the Upstreamness of Production and Trade Flows", *American Economic Review*, Vol. 102/3, pp. 412-416, https://doi.org/10.1257/aer.102.3.412. [4]

BCG and SIA (2024), *Emerging resilience in the semiconductor supply chain*. [5]

Deloitte (2023), *The global semiconductor talent shortage*. [9]

Ewing, J. and N. Boudette (2021), *A Tiny Part's Big Ripple: Global Chip Shortage Hobbles the Auto Industry*. [1]

Haramboure, A. et al. (2023), "Vulnerabilities in the semiconductor supply chain", *OECD Science, Technology and Industry Working Papers*, No. 2023/05, OECD Publishing, Paris, https://doi.org/10.1787/6bed616f-en. [2]

Martins Guilhoto, J., C. Webb and N. Yamano (2022), "Guide to OECD TiVA Indicators, 2021 edition", *OECD Science, Technology and Industry Working Papers*, No. 2022/02, OECD Publishing, Paris, https://doi.org/10.1787/58aa22b1-en. [11]

McKinsey & Company (2024), *How semiconductor companies can fill the expanding talent gap*. [10]

McKinsey & Company (2021), *Value creation: How can the semiconductor industry keep outperforming?*. [3]

McKinsey and Company (2022), *Strategies to lead in the semiconductor world*. [7]

OECD (2024), "Chips, nodes and wafers: A taxonomy for semiconductor data collection", *Technical paper series* OECD Publishing, Paris. [6]

Shih, W. (2021), *Why the global chip shortage is making it so hard to buy a PS5*, https://www.theverge.com/2021/8/31/22648372/willy-shih-chip-shortage-tsmc-samsung-ps5-decoder-interview (accessed on 25 February 2022). [8]

Notes

[1] OECD Directorate for Science, Technology and Innovation.

[2] The ICIO tables measure economic interrelatedness for 67 countries and 45 industries between 1995 and 2021 (Martins Guilhoto, Webb and Yamano, 2022[11]) . They are the main building block to the Trade in Value Added (TiVA) data. In the basic ICIO tables, manufacturing of semiconductors is part of a larger "Computer, electronic and optical equipment" industry (D26 in ISIC Rev.4). Relying on bilateral trade data and five domestic input-output tables that are sufficiently granular to identify semiconductors, Haramboure et al. (2023[2]) estimate a semiconductor-augmented ICIO table, where the industry is split into two sub-industries, namely "Semiconductors" and "ICT and electronics (excluding semiconductors)". The augmented data are derived from the 2021 version of the ICIO tables and cover the 1995-2018 period.

[3] A direct dependency in an industry refers to the direct purchase of semiconductor inputs. Indirect dependency, on the other hand, accounts for semiconductors purchased by the industry's suppliers and embedded within the intermediate goods supplied to the industry.

[4] Export concentration only measures inter-country flows concentration and does not consider domestic production.

[5] A pure-play foundry focuses its activities on manufacturing semiconductor devices designed by other companies.

[6] These advanced lithography machines are almost exclusively produced by a single Dutch firm, which relies on specialised optical instruments from one German firm, as reported by BCG and SIA (BCG and SIA, 2024[5]).

3. Special focus : Critical raw materials supply chains

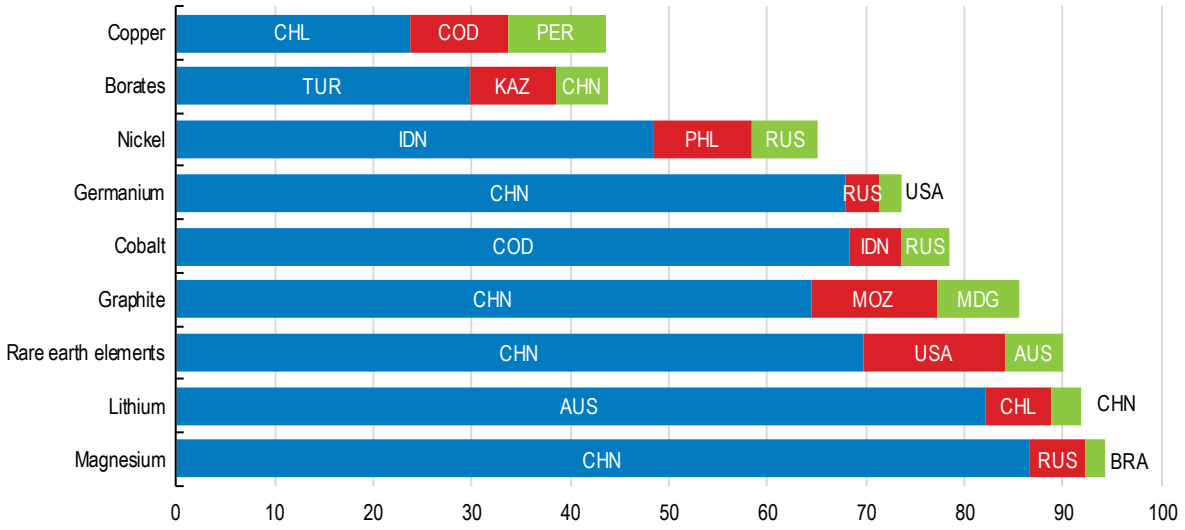
Przemysław Kowalski[1] and Benjamin Katz[2]

Critical raw materials production is highly concentrated in a small number of locations, which dominate global supply

Trade of industrial raw materials is critical for transforming the global economy from one dominated by fossil fuels to one led by renewable energy technologies or for advancing digitalisation (hereafter critical raw materials – CRMs). Extraction and processing of raw materials has traditionally been highly concentrated not only in geographic terms but also in terms of ownership. This is mainly because the economic viability of the raw material industry requires extraction and processing to take place where these materials are the most naturally abundant, or where the geological and climatic conditions and available technology and resources make the extraction and processing the most economically viable. However, these natural characteristics of the raw materials industry also provide incentives for market participants and governments to leverage market power dynamics to purse economic and non-economic objectives. For example, export restrictions on unprocessed forms of cobalt, lithium and nickel have been used by some of the main producers with the aim of promoting the development of domestic processing industries (Andrenelli et al., 2024[1]). Other forms of state intervention, such as special regulations, state ownership, investment restrictions and subsidies are also pervasive in the sector.

Production and international trade of CRMs has become increasingly concentrated amongst a handful of extracting and processing locations which account for the bulk of global supply (Kowalski and Legendre, 2023[2]). For example, the three top producing countries in 2023 accounted for more than two thirds of the global production of cobalt (78%), lithium (92%), nickel (65%) and rare earth elements (90%) (Figure 3.1). Concentration of exports is particularly significant for unprocessed forms of cobalt, manganese, borates, chromium, magnesium and lithium (Figure 3.2).

Figure 3.1. Share of top three producing countries in global production in 2022



Note: For lithium data refer to 2021.
Source: OECD based on US Geological Survey.

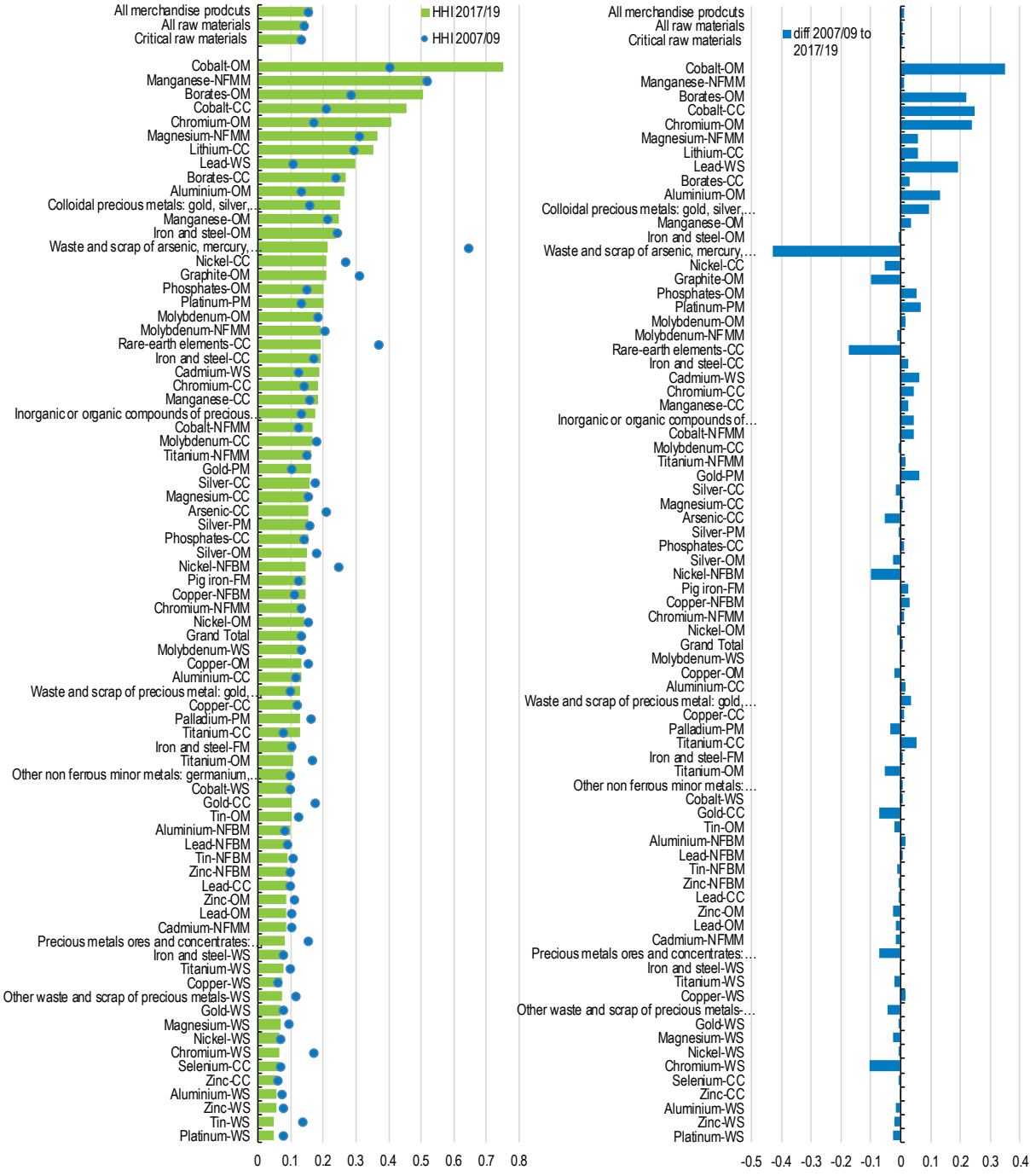
Growing demand for CRMs is prompting governments to adopt CRM-focused policies

Demand for several of these highly geographically concentrated resources has grown rapidly as they have become CRMs for green and digital transformation industries.[3] The sluggish growth of mining and processing capacities which require significant long-term investment and typically face extended approval periods, and the fact that deposits are not available everywhere, indicates that international trade and investment will continue to play a key role in securing raw materials for the foreseeable future. Consequently, policies of individual producer countries may continue to have important international spillover effects. Moreover, expansion of demand for industrial raw materials is taking place against a backdrop of growing geopolitical tensions and strategic rivalries (Box 3.1).

Restrictions on exports of raw materials which have the objective of favouring downstream domestic users to the detriment of foreign users are some of the most contentious forms of state intervention. Undermining the economic viability and thereby decreasing the output of domestic extractive industries hampers the global supply of the concerned materials. In addition, if the exporter controls a large share of the market, export restrictions increase world market prices, creating incentives for other exporters to impose similar measures,[4] amplifying negative effects on international markets.

Figure 3.2. Concentration of global exports of CRMs across all exporting countries

Global HHI index of export concentration across exporting countries and critical raw material products and sectors



Note: The different sectors to which the specific critical raw materials products may belong are labelled with the following acronyms: PM – precious metals and stones; OM – ores and minerals; CC - chemicals and compounds; NFMM – non-ferrous minor metals; NFBM – non-ferrous base metals; WS – waste and scrap; and FM - ferrous metals.
Source: OECD calculations using the BACI data.

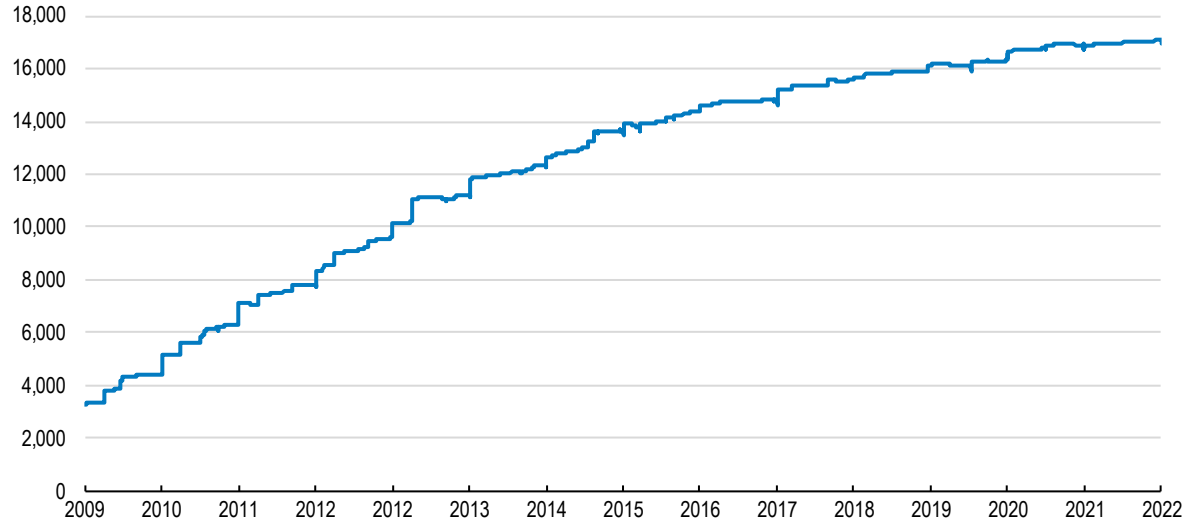
The most recent release of the *OECD Inventory of Export Restrictions on Industrial Raw Materials* which covers the period 2009-22 shows that export restrictions on industrial raw materials have seen more than

a five-fold increase during this period (Figure 3.3). In the period 2020-22, approximately 13% of global trade in non-waste and scrap industrial raw materials was facing at least one export restriction measure.

Export restrictions on ores and minerals, in essence the raw materials located upstream in CRM supply chains, increased faster than restrictions in other segments of the CRM supply chain. This correlates with the broad trend of increasing concentration of production, imports and exports of upstream products, and is broadly consistent with the logic of supporting domestic downstream industries via restrictions on exports of upstream products.

The use of quantitative export restrictions, such as *export prohibitions* or *quotas*, has also been increasing, particularly in the most recent years covered by the Inventory. Remarkably, the incidence of *export prohibitions*, the strongest type of export restrictions, has increased significantly since 2020 and were the most used type of export restriction introduced in 2022.

Figure 3.3. Number of exported raw material products subject to at least one export restriction measure



Note: The count of all types of measures in place across all covered raw materials and all implementing countries takes into account the stock of measures in place at the beginning of the period, as well as new additions and eliminations.
Source: OECD (2024[3]), *OECD Inventory on Export Restrictions on Industrial Raw Materials*.

The growing use of export restrictions, which are becoming at once increasingly prevalent and prohibitive, suggests a rising influence of these measures on international markets and on the availability and pricing of industrial raw materials, with possible negative spillover effects cascading down GVCs.

Recent case studies on selected economic effects of export restrictions on cobalt, lithium and nickel introduced by the Democratic Republic of Congo (DRC), Argentina, Zimbabwe and Indonesia show that the (actual or perceived) positive domestic effects in restriction-using countries are likely to occur at the expense of trading partners. The bans introduced by the DRC and Indonesia appear to have resulted in a significant re-direction of exports of primary forms of cobalt and nickel from international markets towards domestic processing and were correlated with investments in domestic downstream capacity leading to larger downstream production. However, there were also limitations in terms of the impact of these measures. While export restrictions may have played a role in helping the DRC and Indonesia shift away from exports of primary products, the downstream impacts tended to be concentrated in the immediate next processing stages and involved mainly Chinese investors who already controlled large parts of these

segments of the value chain. Argentina's export taxes appear to have helped the country raise the tax revenue, but they also seem to have resulted in diminished exports.

These case studies also illustrate some of the mechanisms which led to China's dominance in extraction and processing of several CRMs. The investments in downstream processing in both the DRC and Indonesia were dominated by Chinese investors. Export bans on primary lithium by Zimbabwe were also accompanied by announcements of increased Chinese investments in downstream processing. China already had a strong presence as an owner of mining facilities (in DRC) and a key importer and processor of raw materials (from DRC, Indonesia and Zimbabwe) prior to the bans, and Chinese investors were therefore natural candidates for participation in downstream industry expansions. In addition, investments in downstream processing activities were very large and, due to the high commodity price volatility, very risky. Representatives of the mining sector argue that typical commercial financial institutions in OECD countries face greater challenges in the financing of such sizeable and risky projects than state-supported Chinese actors.[5] Some assessments also suggest that only a part of the value added from the expansion of downstream activities accrued to the host economies, and that some of these projects had mixed Environmental, Social and Governance (ESG) results (Andrenelli et al., 2024[1]). In addition, such policies may discourage investments in sectors which do not rely on country's natural resources (Economist, 2024[4]).

Responsible sourcing requirements, trade dependencies and security of supply for CRMs

The experience of the tantalum supply chain illustrates the complex interplay between responsible sourcing requirements, trade dependencies and security of supply for CRMs (Box 3.1). The ability of companies sourcing minerals and their due diligence programmes to parse their supply chains – mitigating risks where feasible and only disengaging from specific business relationships when necessary – is paramount. Such due diligence programmes comprise industry, civil society or government-backed initiatives supporting companies in facilitating risk identification or traceability upstream or conducting audits of smelters or refiners. When effective, due diligence aims to help companies identify and mitigate supply chain risks at an early stage before they escalate, or to help them disengage more surgically in the case of more severe risks without cutting off entire countries, regions or types of supply.

Meaningful due diligence can also help alert the market and decision-makers on supply risks, whether real or potential. For example, a company seeking to assess the risk of illicit tantalum trade in the Great Lakes region in Central and East Africa is likely to observe that the absence of reliable, disaggregated data renders an independent evaluation of national tantalum production and exports nearly impossible. Addressing such knowledge gaps is of utmost importance both for supply chain risk mitigation and to safeguard a stable supply of tantalum over time.

Due diligence can also help bring greater transparency to risks linked to beneficial ownership of mines or other nodes along the supply chain, of increasing interest to policymakers concerned about trade dependencies. The increased trade flows and formality of the tantalum supply chain from the Great Lakes region associated with the emergence of due diligence programmes since 2010 may also be instructive for how to foster a more stable supply of other critical raw materials with similar risk profiles.

In the absence of strong due diligence, companies confront an undesirable choice between potentially contributing to conflict financing and accruing legal compliance risks on the one hand or trade disruptions on the other. In addition, concerns have arisen about the lack of a level playing field when not all companies are subject to, or endeavour to meet, due diligence expectations. With geopolitical tensions on the rise, natural resources often being a factor in conflicts around the world, and regulatory and market requirements on responsible business conduct expanding, this challenge is likely to become more acute. Strengthening the policy environment for effective due diligence may therefore be of interest to

policymakers seeking to better absorb short-term shocks and help stabilise the supply of critical raw materials from diverse sources of supply over the medium and longer terms.

The *OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas* (hereafter the "OECD Guidance") recognises the role that due diligence programmes play in pooling resources and leverage to support due diligence, but that companies in the supply chain bear ultimate responsibility for due diligence. In light of this, the current situation calls for companies to be more active and engaged, and less perfunctory, with their due diligence. For instance, in particular smelters, instead of relying on due diligence programmes alone to filter their supply, should use information such programmes generate to raise questions with their suppliers. Only an active approach will position smelters to engage and, if necessary, disengage in a targeted way instead of from the entire region. Due diligence programmes, with the support and direction of governments and companies using them as relevant, could strengthen mineral tracking to be more impervious to smuggling. In some cases, making programmes' own governance to be more inclusive, transparent and responsive would build confidence and provide more paths towards addressing shortcomings, particularly since some are primarily industry-driven and lack timely updates on programme information.

Box 3.1. Balancing responsible sourcing and security of supply of a critical raw material: The example of tantalum

Conflict financing, human rights abuses and governance risks have been a backdrop to the supply of tantalum from the African Great Lakes region in Central and East Africa for over 25 years. Tantalum is important for the world's electronics, aerospace and nuclear power industries. Its recent addition to US and EU lists of critical minerals underlines the strategic significance of tantalum. However, security of supply still tends to be seen as distinct from responsible sourcing expectations, despite high disruption risks in producing areas. Tantalum's supply is highly concentrated in a region rife with conflict and instability. The Democratic Republic of Congo (DRC) alone accounts for 41% of mined production. The Great Lakes region, of which DRC is a part, account for well over half of global supply (Padilla and Nassar, 2023[5]) with 62% of global production in 2023 (USGS, 2024[6]).

The mineral's exposure to conflicts has already affected production and trade in the past. The DRC banned production and exports in late 2010 for six months due to the involvement of armed groups (De Koning, 2011[7]). A recent analogue is the ban of tin exports by the United Wa State Army in Myanmar, officially to improve governance of a mining sector with similar governance and environmental risks. The highly informal nature of the supply chain also appears to have constrained investment, production and trade during the peak period of involvement of armed groups prior to 2010.

The mining ban in the DRC, however, was arguably a response to – rather than a feature of – conflict tied to the tantalum supply chain. It coincided with efforts to break the link between the trade in tantalum and conflict, human rights abuses and corruption. These efforts culminated in regulations in the DRC, Rwanda and the United States (and eventually the European Union), regional agreements between member states of the International Conference on the Great Lakes Region in addition to international norms on responsible business conduct (RBC) like the OECD Guidance. The London Metal Exchange (LME) similarly requires due diligence based on the OECD Guidance for tin, which is often mined from the same ore as tantalum in the Great Lakes region, in addition to six other non-ferrous metals including major commodities like cobalt, copper and nickel. While these initiatives aimed at fostering responsible trade in support of prosperity and stability in high-risk areas, they also called for disengagement from specific business relationships as a last resort in several situations. They include failed attempts at preventing or mitigating severe impacts; when adverse impacts are irremediable; where there is no

reasonable prospect of a change; and when severe adverse impacts or risks are identified and the entity causing the impact does not take immediate action to prevent or mitigate them.

In the case of tantalum, responsible sourcing when carried out well appears to contribute to security of supply. However, when companies address responsible sourcing expectations without a risk-based approach, and when they nuance or do not have ability to distinguish between different business relationships, the risk of disruption grows. The quality of due diligence may be determinative in this regard, in particular how effectively companies in the supply chain can navigate regulatory and market expectations on RBC while avoiding blanket disengagement. In the period during which due diligence programmes were established and scaled up to help companies meet RBC requirements following the 2010-11 DRC ban, tantalum production from the Great Lakes region surged to several times its pre-2010 levels. In addition, even if reliable data on reserves are scarce and they tend to be under-explored and poorly documented (Schütte and Näher, 2020[8]; BGR, 2021[9]), official production data since 2010 have better reflected the DRC having the largest observed production in the region.

The emergence of due diligence programmes has also coincided with the region gaining a significantly larger share of global supply, the distribution of official production within the Great Lakes region becoming more diverse, and higher accuracy of trade data despite some crucial gaps. Analysis of tantalum trade statistics have also shown that "the market structure of smelter countries sourcing tantalum from the region [shifted] from a China-dominated monopsonistic situation prevailing from 2006 to 2012 towards a less concentrated international market in 2013-17" (Schütte, 2019[10]). Over the medium to long term, due diligence appears to be associated with a more stable supply of tantalum. This may stem from improved monitoring and transparency, increasing formality and investment, fewer reputational concerns or reducing the chances that events linked to conflict or political disputes constrain supply unpredictably.

When companies are unable to mitigate risks effectively, they may determine that it is unfeasible to remain engaged responsibly and feel compelled to withdraw entirely from countries or regions to avoid falling afoul of regulations or market expectations on RBC. This represents a potentially more disruptive scenario for responsible sourcing expectations. It merits recalling that initially, following the introduction of responsible sourcing requirements by the United States in 2010, the sourcing of tantalum and other minerals by OECD countries from the region plummeted in what some have termed a *de facto* "embargo". Although due diligence programmes have helped the global tantalum sector source responsibly from the region since then, such programmes have been strained by a resurgence of conflict, with concerns mounting over companies' ability to use them effectively to mitigate related risks in their supply chains. In particular, the recent expansion of rebel group M23 and other non-state armed groups into large swathes of territory in North Kivu province of the DRC has put global markets under renewed pressure to demonstrate responsible sourcing of tantalum, in addition to tin, tungsten and gold.

One major challenge is the lack of comparable and precise data, especially regarding intra-regional trade at different steps of the supply chain. This issue is further complicated by the absence of information on tantalum content in mixed mineral production. The International Conference on the Great Lakes Region has a mandate to establish a database about smuggling practices. International diplomacy could step up efforts to operationalise this database and improve public access to production and trade data. Diplomacy and trust-building measures will also be central to addressing the root causes of the conflict.

Concerns about the strains that due diligence is showing in the face of increased conflict and smuggling risks in the Great Lakes region underline the need to address existing challenges (US State Dept., 2024[11]). The control by non-state armed groups over a number of highly productive artisanal mining sites and trading centres in tantalum-rich areas has prompted upstream due diligence programmes to suspend due diligence and traceability efforts in 2023 and 2024. Such disengagement may have been the only option to manage risks, but it has disrupted formal trade in tantalum and led to an increase in

smuggling (UN Security Council, 2024[12]). The prevalence of smuggling has also raised concerns about potential infiltration of minerals connected to conflict or other risks into legitimate channels of trade in the region. It is conceivable that, in the short term, the more smuggling flourishes, the less likely it is that due diligence weaknesses will cause trade shocks, since trade will continue under a veneer of legitimacy. This would lead to uncertainty in the market persisting, though, with unpredictable results. Tantalum smelters are already voicing doubts about the viability of continued sourcing from the Great Lakes region while complying with regulatory and market requirements, which hints at the possibility of a more serious shock.

One scenario that could increase the risk of a shock might stem from greater fragmentation in sourcing from the Great Lakes region. If companies facing more regulatory or reputational pressure to source responsibly disengage, while less scrupulous peers or suppliers carry on without meaningfully addressing the risks, market concentration and supply chain vulnerabilities could increase and the leverage of companies trying to source responsibly could decline. This dynamic could trigger a race to the bottom in sourcing tantalum and other critical minerals, while also making coercive economic behaviour involving critical raw materials like tantalum easier.

Emphasising RBC standards that advocate proportionate responses to the risks, progressive improvement and adapting risk mitigation to the circumstances may help companies remain engaged in high-risk areas without compromising their competitiveness. Promoting broad buy-in to and co-operation on international norms on responsible sourcing will be important for maintaining a level playing field. This may include extolling the benefits of RBC for mineral producing countries with a range of risk profiles through diplomacy on critical raw materials and integrating provisions on RBC into emerging and prospective agreements on the supply of critical minerals.

Countries increasingly adopt policy initiatives to enhance security of CRMs supply

Concentration of production and trade of several CRM is a growing cause of concern, making governments consider several types of policy responses. First, with no country having all the minerals needed for all purposes and given the global ramifications of a potentially impeded green transition, there is a strong case for plurilateral or multilateral co-operation to restrain the use of export restrictions. Among others, such co-operative solutions for mitigating harmful export restrictions will require a better understanding of the motivations of countries using them as well as their impact on their trading partners and of how the different interests could be reconciled in an effective multilateral agreement.

Second, several countries are pursuing different national, bilateral or plurilateral policy initiatives. For example, both the United States Inflation Reduction Act and the European Union's Critical Raw Materials Act aim to support a diversification away from foreign towards domestic (or trading allies') sources of CRMs (Box 3.2). In addition, the emerging inter-governmental partnerships, which can also involve the private sector, such as the Minerals Security Partnership and the European Union's raw materials diplomacy partnerships, are initiatives which aim to secure stable supply of CRMs from reliable foreign sources. A relatively new element of these approaches is their explicit acknowledgement that the stable and resilient supply of critical minerals should occur hand-in-hand with value addition and wider economic development in resource-rich countries.

More broadly, greater investment, including in mining and processing infrastructure and in line with high ESG expectations, including by implementing OECD standards on RBC in the minerals sector, can help deliver the economic benefits of greater domestic value addition without compromising the stability of global markets.

Box 3.2. Selected recent policy initiatives aiming to enhance security of CRM supplies

The US Inflation Reduction Act

The Inflation Reduction Act, established in 2022 in the United States, attempts to comprehensively reshape the US power sector by supporting the decarbonisation of electricity generation and electric vehicles industries with several measures. The main measures are production and investment tax credits for clean electricity and energy storage, and tax credits for the purchase of a new electric or hydrogen vehicle conditional on meeting several conditions. With the aim of reducing dependencies on critical mineral supplies, the IRA requires that a minimum share of the critical minerals comes from North America (or a country with which the United States have a free-trade agreement) to benefit from the tax credit.

The EU Critical Raw Materials Act

In March 2023, the European Commission proposed a Critical Raw Materials (CRM) Act, as part of the EU Green Deal Industrial Plan. This Act, which came into force in April 2024, aims at developing a European value chain for selected raw materials identified as key inputs for the green and digital transitions and facing high supply risks. It proposes several measures, in particular to streamline permitting processes and strengthen international engagement.

References

Andrenelli, A. et al. (2024), Trade and domestic effects of export restrictions: insights from exploratory case studies of cobalt, lithium, and nickel, https://doi.org/(forthcoming). [1]

BGR (2021), Tantalum - Sustainability Information, https://www.bgr.bund.de/EN/Gemeinsames/Produkte/Downloads/Informationen_Nachhaltigkeit/tantal_en.html;jsessionid=14823F18901B02EE2834349369ECF9EF.internet001?nn=1548104. [9]

De Koning, R. (2011), Conflict Minerals in the Democratic Republic of the Congo: Aligning Trade and Security Interventions, Stockholm International Peace Research Institute, https://www.sipri.org/sites/default/files/files/PP/SIPRIPP27.pdf. [7]

Economist (2024), The false promise of Indonesia's economy, https://www.economist.com/finance-and-economics/2024/02/08/the-false-promise-of-indonesias-economy. [4]

IEA (2021), Net Zero by 2050: A roadmap for the energy sector, International Energy Agency, https://www.iea.org/reports/net-zero-by-2050 (accessed on 8 December 2021). [13]

Kowalski, P. and C. Legendre (2023), "Raw materials critical for the green transition: Production, international trade and export restrictions", OECD Trade Policy Papers, No. 269, OECD Publishing, Paris, https://doi.org/10.1787/c6bb598b-en. [2]

OECD (ed.) (2024), OECD Inventory on Export Restrictions on Industiral Raw Matierials, https://www.oecd.org/en/topics/export-restrictions-on-critical-raw-materials.html. [3]

Padilla, A. and N. Nassar (2023), "Dynamic material flow analysis of tantalum in the United States from 2002 to 2020", Resources, Conservation and Recycling, Vol. 190, https://doi.org/10.1016/j.resconrec.2022.106783. [5]

Schütte, P. (2019), "International mineral trade on the background of due diligence regulation: a case study of tantalum and tin supply chains from East and Central Africa", Resources Policy, Vol. 62, https://doi.org/10.1016/j.resourpol.2018.11.017. [10]

Schütte, P. and U. Näher (2020), "Tantalum supply from artisanal and small-scale mining: A mineral economic evaluation of coltan production and trade dynamics in Africa's Great Lakes region", Resources Policy, Vol. 69, https://doi.org/10.1016/j.resourpol.2020.101896. [8]

UN Security Council (2024), Final report of the Group of Experts on the Democratic Republic, https://documents.un.org/doc/undoc/gen/n24/118/80/pdf/n2411880.pdf. [12]

US State Dept. (2024), Statement of Concern Related to Certain Minerals Supply Chains from Rwanda and Eastern Democratic Republic of the Congo Contributing to the Ongoing Conflict, https://www.state.gov/statement-of-concern-related-to-certain-minerals-supply-chains-from-rwanda-and-eastern-democratic-republic-of-the-congo-contributing-to-the-ongoing-conflict/. [11]

USGS (2024), Mineral Commodity Summaries 2024; Tantalum, https://pubs.usgs.gov/periodicals/mcs2024/mcs2024-tantalum.pdf. [6]

Notes

[1] OECD Trade and Agriculture Directorate.

[2] OECD Directorate for Financial and Enterprise Affairs.

[3] For example, see IEA (2021[13]).

[4] Incentives to introduce own export restrictions would reflect concerns about the economic viability of downstream domestic users of CRMs for which inputs are becoming more expensive. That said, in some countries and industries, there may be a countervailing incentive for other exporters to seize the opportunity of higher global prices to export more.

[5] This issue has been identified as one of the main challenges for Western firms active in the CRM mining and processing industries during recent discussions at the OECD Forum on Critical Supply Chains held in March 2024.

4. The imperative of energy security: Old concerns, new challenges

Keisuke Sadamori[1]

Introduction

The International Energy Agency (IEA), an autonomous body within the OECD system, was created in 1974 to ensure secure and affordable energy supplies. At first, heavy focus on oil, but over time the IEA's mandate has extended to all types of energy and technologies. The IEA is at the heart of global dialogue on energy. It publishes analysis, data, policy recommendations and real-world solutions to help countries to benefit from secure and sustainable energy and safely advance transition to clean energy. IEA's mandate to ensure energy security is not only about having uninterrupted access to energy, but it is also about securing energy supplies at affordable prices. Affordability of energy has long been a concern, but it surged to the forefront of the policy agenda following the global energy crisis triggered by large-scale Russia's invasion of Ukraine.

Today, 50 years on from the first oil shock that led to the founding of the IEA, the world once again faces a moment of high geopolitical tensions and uncertainty for the energy sector. There are parallels between then and now, with oil supplies in focus amid a crisis in the Middle East – but there are also key differences. The global energy system has changed considerably since the early 1970s, and rapid changes continue to unfold. Clean energy transitions, geopolitical tensions and the growth of cyber threats have expanded the scope of what constitutes energy security today.

Energy security issues become increasingly entangled with the rapidly progressing clean energy transitions. Energy transitions offer the chance to build a safer and more sustainable energy system that reduces exposure to fuel price volatility and reduces energy bills, but there is no guarantee that the journey will be a smooth one. The transitions to clean energy systems marks a change of unprecedented magnitude and will require a proactive approach by governments to address the risks associated with the introduction of a clean energy economy in a timely and effective manner. As the concept of energy security is multidimensional and complex (Box 4.1), this chapter focuses both on the traditional aspects of energy security and aspects related to clean energy transitions.

Box 4.1. Defining and measuring energy security

Securing affordable energy supply is paramount for modern economies and societies. Energy is a key input for production, whose efficiency and scale are linked to the availability and costs of energy resources. It is also vital for improving living standards. Energy enables the provision of basic amenities, contributing to health, education and overall societal progress. It is also interlinked with the efforts to combat climate change.

Energy security is usually defined in broad terms as making available enough quantity of energy in a reliable and affordable way. The IEA defines energy security as the uninterrupted availability of energy sources at an affordable price (IEA, 2022[1]). The Nuclear Energy Agency (NEA) adopted a definition of energy supply security as the resilience of the energy system to unique and unforeseeable events that threaten the physical integrity of energy flows or that lead to discontinuous energy price rises, independent of economic fundamentals (OECD/NEA, 2010[2]).

Energy security can be analysed in two different time perspectives. In the short term, it primarily deals with ability to react promptly to sudden changes in the supply-demand balances. In the long term, energy security deals with timely investments to supply energy in line with economic developments, technological changes and environmental needs. Energy security could cover broad issues related to nation-wide energy systems or focus more narrowly on specific energy products or regional issues.

Assessing energy security is complex, requiring analysing technical, economic, environmental and political considerations.

- Technical issues relate to the technology of energy production and transmission, which determines physical risks, substitutability between different sources of primary energy, as well as needs and duration of investment.
- Economic aspects revolve around the level and volatility of energy costs, linked with the affordability of energy and market regulation. They also deal with financing of energy investment and encouraging innovation to improve reliability and affordability and to minimise environmental impact.
- Energy security should be also analysed in the context of climate change. Extreme weather events, which are set to become increasingly frequent and more devastating with global warming, impact physical security of energy production and transmission directly. At the same time, greening energy production, which is necessary to counter climate change, may affect future energy security.
- Political aspects pertain to risks of domestic political and social instability in case of energy disruptions, geopolitical risks for imported energy sources, and international co-operation to boost resilience and sustainability of energy supply.

The IEA has for long been reviewing and assessing countries against common energy security indicators, recommending policy actions to enhance security and resilience. It regularly conducts Emergency and Security Reviews of its member countries and beyond. Major indicators used by the IEA to help rank countries on their energy security performance include (for oil and gas):

- Import dependency (share of imports in total consumption)
- Supply diversity (Herfindahl-Hirschman index)
- Storage and stocks (total storage capacity/stocks in days of average consumption/peak demand)
- Continuity of supply and economic importance (N-1 indicator; share in total demand).

Electricity requires a slightly different set of indicators, and the IEA has also established a catalogue of

indicators to assess countries' electricity security against the same measurements:

- Import dependency (share of imports in total consumption)
- Generation adequacy (peak load as a share of installed dispatchable generation capacity)
- Continuity of supply (stand-by black-start reserve capacity as a share of installed dispatchable generation capacity)
- Grid reliability (System Average Interruption Duration/Frequency / indices)
- Integration of variable renewable energy (VRE) (share of VRE in total electricity generation)
- Economic importance (value of lost load).

Given the rapidly changing electricity system, the IEA has started work towards a modern, comprehensible and actionable security framework for power systems. It will combine all three major elements of security: operational security, system adequacy, and governance and market arrangements. The IEA will measure them against several indicators, including instantaneous VRE penetration, critical resource size coefficient and price differentials.

Energy security and clean transitions

As the world changes, so do the challenges around energy security. While risks around the availability of oil and natural gas show no signs of abating, new ones are emerging. These risks could significantly hinder energy transitions and undermine the resilience of energy systems, if not addressed promptly and effectively. This calls for new and enhanced approaches to energy security – fit for today and the decades ahead – to ensure uninterrupted access to affordable energy. As underlined by the IEA's report Net Zero by 2050: A Roadmap for the Global Energy Sector, energy security becomes even more important on the way to net zero.

Russia's invasion of Ukraine provided a stern test of the resilience of today's energy system to geopolitical shocks. The price spikes that followed cuts to gas supply from Russia were certainly very damaging, but the attempt by Russia to use gas supply for political leverage failed. Russia has lost its largest customer, shredded its reputation as a reliable exporter and created incentives for consumers to consider alternatives to natural gas.

The crisis has highlighted how geopolitical events can directly impact the energy sector. However, the relationship is reciprocal. Shifts in energy markets can also shape geopolitical dynamics. As clean energy transitions advance, they are altering the demand for different fuels and sources of electricity, changing the global energy landscape in profound ways.

For much of the fossil fuel era, geopolitics and energy have been tightly interwoven. Importing nations have long depended on exporters for crucial energy supplies, while exporters have relied on importers for revenue. This interdependence has driven the ebb and flow of political and commercial relationships between producers and consumers, helping to manage these delicate dependencies.

However, the risks have often been mitigated by open international energy markets. Initially, these markets centred on oil, but in recent years they have expanded to include natural gas. Well-functioning markets, alongside safety nets such as spare capacity from key producers and the IEA's co-ordinated system of oil reserves, have helped countries navigate supply and demand disruptions. This system proved its worth again in 2022, when two releases of oil stocks were co-ordinated by the IEA just after Russia's invasion of Ukraine.

The world faces a serious challenge with climate change, and energy and climate are inextricably linked. As global average temperatures break records year after year, the case for action has never been stronger.

The current energy system is a major driver of global warming, accounting for about 75% of total greenhouse gas emissions. This means transforming how we produce and consume energy is essential, with the world's ability to meet its climate goals hinging on the energy sector's ability to reach net zero emissions by the mid-century. The rapid growth of some clean energy technologies – including electric cars, solar photovoltaic (PV), batteries and heat pumps – has kept the door open to limiting the rise in the global average temperature to 1.5°C above pre-industrial levels, the target set by the Paris Agreement to avoid the worst impacts of climate change. Yet to meet this goal, a much faster progress is needed and on a much larger scale, according to IEA analysis. Extreme weather events, which are set to become increasingly frequent and more damaging with global warming, impact physical security of energy production and transmission directly. Addressing this will require even greater international co-operation and ambition from policymakers.

Governments and industry must boost preparedness and resilience in the face of new and more frequent threats, such as cyberattacks and extreme weather events, particularly with regard to electricity infrastructure. The establishment of reliable and cost-effective supply chains for clean energy and ensuring the adequacy of the global supply of critical minerals to meet the demand from ramping up clean energy technologies are key for energy transitions.

Even as demand for fossil fuels falls, energy security challenges will remain since the process of adjustment to changing demand patterns will not necessarily be easy or smooth. For example, the peaks in demand we see based on today's policies do not remove the need for investment in oil and gas supply, given how steep the natural declines from existing fields often are. At the same time, they underline the economic and financial risks of major new oil and gas projects, on top of their risks for climate change.

Clean transitions address energy security challenges

Traditional risks around fossil fuel supply evolve, but they do not disappear. Transition could be destabilising for fragile producing states that fail to diversify away from high dependence on hydrocarbon revenues. In the meantime, new geopolitical risks and dependencies arise in clean energy supply chains. And both traditional and new security risks are worsened in a more fragmented international system characterised by rivalries and the lack of co-operation. The world can ill afford these tensions if it wants to get on track to limit global warming to 1.5 C.

At the COP28 climate change conference in Dubai in December 2023, nearly 200 countries adhered to the view that the world needs to transition away from fossil fuels to avoid the worst consequences of global warming. However, while the world's dependence on oil is lessening, it remains deep-rooted, with oil demand continuing its growth, supply disruptions can still cause significant economic harm and have a substantial negative impact on people's lives. Natural gas demand is also growing. It should also be noted that the share of the Organization of Oil Exporting Countries (OPEC) in global supply rises over time as oil demand falls. But in exercising this influence they reduce it, because consumers have an increasing number of mature clean energy options at competitive prices.

The rising share of renewables in energy production not only reduces emissions, but also contributes to energy security. The energy shock created in the wake of Russia's invasion of Ukraine has led to a greater understanding of the problem of energy self-sufficiency, particularly in terms of electricity generation. And this can only be achieved by ensuring the largest possible share of domestic generation from domestic sources. There are some concerns about regional concentration of manufacturing capacities for clean energy technologies given that the vast majority of renewable energy generation is based on technologies and minerals controlled by China (see Special focus 2). Many countries are, therefore, trying to secure diverse and resilient supply chains for clean energy technology manufacturing including renewables. However, supply disruptions in solar panels, for instance, would not immediately affect power supply as

long as sun is shining. Thus, increasing renewable power generation should be considered as a way to increase self-sufficiency and thereby enhancing energy security.

Solar PV and wind are now the cheapest source of electricity generation in many countries in terms of levelised cost of energy. Nonetheless, stronger policies are still needed to support the growth of renewables. Accelerating the permitting process and providing the right incentives for more rapid deployment – for all renewables including flexible hydropower – are some of the most important actions governments can take to address today's energy security and future climate goals at once.

Oil security will continue to be critical during the clean energy transition

One of the IEA's core activities is ensuring the security of oil supplies by setting oil stockholding requirements for member countries. Each IEA country has an obligation to ensure it holds total oil stocks equivalent to at least 90 days of net oil imports. In case of a severe oil supply disruption, IEA members may decide to release these stocks to the market as part of a collective action.

An enduring focus on oil security is a consequence of the oil dependence for the transport sector (to fuel cars, trucks, ships and aircraft), which is expected to continue although the shift to a clean energy economy is gathering pace, with electric vehicle sales increasing, energy efficiency improving, and other clean energy technologies advancing rapidly. Based on today's policy settings, global oil demand is expected to plateau at the end of this decade.

However, the threat posed by oil supply disruptions will not disappear anytime soon. Even after demand starts declining, oil will remain an important part of the global energy mix for some time. There is also good reason to believe that oil supply disruptions are even more likely to occur in the coming decades than they are today. This is due to lower appetite for oil upstream investments with uncertain demand outlook, increasing supply concentration for both crude oil and oil products, a highly uncertain geopolitical outlook, and a plethora of additional risks including the growing threat of cyberattacks and the increasing frequency of extreme weather events.

Developments further along the oil value chain will also result in increased exposure to oil market risk for many countries. In the refining sector, a significant amount of capacity has been shut down in advanced economies over the past decade, particularly in Europe where some refiners have struggled to remain competitive following the completion of numerous large-scale, highly complex refineries in the Middle East and Asia. Faced with increased competition and a highly uncertain demand outlook in their main markets, more refineries in advanced economies are likely to close. This will leave many countries increasingly reliant on imports of oil products, such as diesel and jet fuel. As a consequence of their increased import dependence, these countries will become more vulnerable to disruptions in oil product markets.

The risks to oil security are manifold and wide-ranging, extending far beyond risks emanating from structural changes in global oil markets. Governments should take particular note of the threats posed by the increasingly uncertain geopolitical outlook, climate change and extreme weather events, and cyberattacks. In recent years, supply disruptions have been caused by events that fall into each of these categories.

Ultimately, reducing dependence on fossil fuels by promoting the uptake of clean energy solutions is the most effective means for any government to enhance energy security. Shifting to a clean energy economy should be seen as a golden opportunity to build a more sustainable energy system that minimises exposure to oil market volatility and decreases the prospect of supply shocks. However, the journey to a clean energy economy may not be a smooth one. For many years to come, oil supply disruptions will have the potential to cause significant economic harm and negatively impact people's lives. Maintaining a resolute focus on oil security and emergency preparedness will therefore be critical throughout clean energy transitions worldwide, and the IEA's emergency response capabilities will remain vital.

The oil and gas Industry must play their part in Net Zero Transitions

Structural changes in the energy sector are expected to lead to plateauing of oil and gas demand by the end of this decade under today's policy settings. Fossil fuel demand is not expected to decline quickly enough to align with the Paris Agreement and the goal to limit the increase in global temperature to 1.5°C. If governments were to deliver on their national energy and climate pledges in full and on time, oil and gas demand would be 45% below today's level by 2050 and the temperature rise could be limited to 1.7°C. 1.5°C trajectory would require net zero emissions from the global energy sector achieved by mid-century with oil and gas use falling by 75%.

The IEA's Oil and Gas Industry in Net Zero Transitions report explores what oil and gas companies can do to accelerate net zero transitions and what this might mean for an industry which currently provides more than half of global energy supply and employs nearly 12 million workers worldwide.[2] The implications of net zero transitions are far from uniform: the industry encompasses a wide range of players, from small, specialised operators to huge national oil companies. While attention often focuses on the role of the majors, which are seven large, international players, they hold less than 13% of global oil and gas production and reserves.

The oil and gas industry has so far played a marginal force in the world's transition to a clean energy system. Oil and gas producers account for only 1% of total clean energy investment globally. More than 60% of this comes from just four companies, out of thousands of producers of oil and gas around the world today.

While there is no single blueprint for change, there is one element that can and should be in all company transition strategies: reducing emissions from the industry's own operations. Less than half of current global oil and gas output is produced by companies that have targets to reduce these emissions. A far broader coalition – with much more ambitious targets – is needed to achieve meaningful reductions across the oil and gas industry. The production, transport and processing of oil and gas results in just under 15% of global energy-related greenhouse gas emissions. This is a huge amount, equivalent to all energy-related greenhouse gas emissions from the United States. To align with the 1.5°C scenario, these emissions need to be cut by more than 60% by 2030 from today's levels and the emissions intensity of global oil and gas operations must be near zero by the early 2040s. These are appropriate benchmarks for industry-wide action on emissions, regardless of the future scenario. The emissions intensity of the worst performers is currently five to ten times higher than the best. Methane accounts for half of the total emissions from oil and gas operations and is dozens of times more potent than CO2 for global warming. Tackling methane leaks is a top priority and can be done very cost-effectively – but it is not the only priority.[3]

Some 30% of the energy consumed in a net zero energy system in 2050 comes from low-emission fuels and technologies that could benefit from the skills and resources of the oil and gas industry. These include hydrogen and hydrogen-based fuels; carbon capture, utilisation and storage (CCUS); offshore wind; liquid biofuels; biomethane; and geothermal energy. Oil and gas companies are already partners in a large share of planned hydrogen projects that use CCUS and electrolysis. The oil and gas industry are involved in 90% of CCUS capacity in operation around the world. CCUS and direct air capture are important technologies for achieving net zero emissions, especially to tackle or offset emissions in hard-to-abate sectors. For the moment, only around 2% of offshore wind capacity in operation was developed by oil and gas companies. Plans are expanding, however, and the technology frontier for offshore wind – including floating turbines in deeper waters – moves this sector closer to areas of oil and gas company strength. In addition, industry skills and infrastructure, including existing retail networks and refineries, give the industry advantages in areas like electric vehicle charging and plastic recycling.

Companies that have announced a target to diversify their activities into clean energy account for just under one-fifth of current oil and gas production. The oil and gas industry invested around USD 20 billion in clean energy in 2023, some 2.5% of its total capital spending. For producers that choose to diversify

and are looking to align with the aims of the Paris Agreement, the IEA's bottom-up analysis of cash flows in the 1.5°C scenario suggests that a reasonable ambition is for 50% of capital expenditures to go towards clean energy projects by 2030, on top of the investment needed to reduce direct (scope 1) and indirect (scope 2) emissions. Not all oil and gas companies have to diversify into clean energy, but the alternative is to wind down traditional operations over time. Some companies may take the view that their specialisation is in oil and natural gas and decide that – rather than risking money on unfamiliar business areas – others are better placed to allocate this capital. But aligning their strategies with net zero transitions would then require them to scale back oil and gas activities while investing in emissions reductions.

Electricity security is a cross-sectoral matter and benefits from diversification

Secure power systems require secure fuel supplies to be able to feed the generation fleet. In many countries, gas-fired power plants are playing the critical role in covering peak demand periods and providing the flexibility to accommodate larger shares of wind and solar generation. As the world recovers from the COVID-19 pandemic and has to deal with the impacts of the Russian invasion of Ukraine, global gas markets have become very tight. This has had significant spillover effects on electricity systems dependent on gas. In many emerging economies, notably in Asia Pacific and Latin America, liquefied natural gas (LNG) supplies are the main source of flexible gas supply in the absence of pipelines and underground gas storage, which brings additional costs and supply risks. Coal-fired power generation is still the backbone of power supply in many Asian countries.

Energy system integration requires stronger co-ordination across sectors and among stakeholders, both in planning and operations. Power system planning needs to identify the investment required to ensure security of supply in the decades ahead. Integrated and co-ordinated planning frameworks should cover generation, transmission and distribution networks, demand, the electrification of end uses and dependencies on other sectors. Such frameworks are essential to identify appropriate options for the future power system, in the light of demand and technology uncertainty, and can help identify the need for interconnections at the national, regional and international level. Despite the progress in decentralisation, secure interconnected power systems are the backbone of energy security. In Europe and the United States, regional trade is a key source of flexibility, and the Association of Southeast Asian Nations (ASEAN) countries work to improve energy system interconnectivity and energy trade.

Regular adequacy studies and reviews of their underlying assumptions are key to ensure that all relevant outage risks are captured correctly and to inform policymaking. Probabilistic adequacy assessments give greater insight for systems with a high share of renewables as they allow many uncertainties to be evaluated together. Planning studies should include "low-probability high-impact" scenarios, including those related to extreme weather events and cybersecurity threats. Recent extreme weather events across the globe highlight the energy security risks that climate change brings.

Power systems are digitalising, bringing benefits at all levels, from the management of generation and grids to the rise of new capabilities and services from a wider set of resources. However, digitalisation comes with increased cybersecurity risks. A successful cyberattack could trigger the loss of control over devices and processes, in turn causing physical damage and widespread service disruption to electricity systems. A wealth of cyber risk management tools and frameworks have been deployed and policymakers play a central role in selecting and implementing them.

Whether physical or cyber, not all events can be prevented at reasonable costs, requiring a cost-benefit analysis. Policy setting and planning can be seen as an iterative process: the policy goals are key inputs to planning and, in turn, the planning exercises provide essential information on the options and corresponding costs to meet the policy objectives. The selected trajectory must strike a balance between the deployment of (costly) preventive measures and the consequences of various incidents occurring, ranging from expected outages to rare events. In their effort to strive for affordable and secure power,

policymakers should aim for a higher resilience, that is the ability of the system to absorb, accommodate and recover from short-term shocks (supply crisis, cyberattack or extreme weather events) and long-term, more gradual changes (adaptation to evolving needs and weather patterns).

Risk-preparedness plans help identify cost-effective resilience measures. For instance, greater diversity in the resource mix can ensure resilience against social, geopolitical, market, technical and environmental risks. With a deeper understanding of the risks, governments and regulators are equipped to design appropriate incentives for utilities to invest in a resilient power system in a timely manner.

Prioritising energy efficiency

Energy efficiency (i.e. using less energy for the same result) is central to achieving affordable clean energy transition that ensures equitable social development and economic growth. Decisive, ambitious and transformative action on energy efficiency is needed to improve the resilience, security and reliability of our energy systems, and improve access to sustainable and affordable energy services.

Without the efficiency improvements made since 2000, the world would be using 13% more energy today and energy-related carbon emissions would be 14% higher. Over half of the energy savings achieved can be attributed to efficiency measures in the industrial sector, about a third to efficiency in buildings and appliances, and a tenth to transport efficiency. These efficiency improvements have lowered energy bills for households and businesses, enhanced competitiveness and supported job creation.

Efficiency progress is also enhancing energy security and access to affordable, reliable energy. By cutting down overall energy demand, efficiency can significantly reduce overall reliance on fossil fuel imports, improve the balance of payments and reduce the likelihood of supply disruption. Efficiency gains since 2000 avoided the need for over 11 EJ of fossil fuel imports into IEA countries and other major economies in 2017, equivalent to 20% more. Reduced oil imports into IEA countries alone saved more than USD 30 billion.

Looking towards a net zero emissions future by 2050, there is still significant untapped potential: doubling the current rate of energy intensity improvement from 2% to 4% per year until 2030 means avoiding 95 EJ per year of final energy consumption – equivalent to China's current final energy demand. Achieving 95 EJ of annual energy savings by 2030 would also translate into significantly strengthened energy security, avoiding the demand for almost 30 million barrels of oil per day, about triple Russia's average production in 2021, and 650 bcm of natural gas per year, around four times EU imports from Russia in 2021. Reductions in electricity demand can also avoid the need for investment in new generating capacity, as well as in the required transmission and distribution infrastructure and storage facilities.

In emerging economies, efficiency gains are particularly important to ensure the reliability and quality of energy supply services, to allow currently suppressed demand to come online without overstraining existing electricity networks, and to allow economic development. Achieving multiple benefits from action on energy efficiency is particularly important in the context of rising and fluctuating energy prices, which disproportionally hurt the most vulnerable segments of the population, and the economies of developing and emerging economies. People-centred and inclusive approaches and the prioritisation of energy efficiency are means to boost affordability and ensure that we are not reversing progress towards universal access to electricity.

Following the pathway set out in the IEA Net Zero Scenario, the global economy could grow by 40% by 2030 and support around 800 million more people with access to electricity, all with a 5% lower final energy demand. Compared to the IEA Stated Policies Scenario, energy efficiency and related measures in the Net Zero Scenario would reduce annual CO2 emissions by 5 Gt in 2030. Over 80% of these additional efficiency gains result in overall net cost savings to consumers, helping to lower energy bills and cushion the effects of price volatility.

Achieving 95 EJ of annual energy savings could contribute to lowering household energy bills by at least USD 650 billion per year by 2030. This calls for strong and early action on energy efficiency by 2030. Governments play an essential role in ensuring the necessary front-loading and prioritisation of energy efficiency action. Recognising the value of early action on energy efficiency as a means of cost-effectively accelerating progress towards net zero energy targets, and increasing energy security and resilience, over 40 governments at the 8th IEA Annual Global Conference on Energy Efficiency in June 2023 signed a joint statement calling on all governments and other actors to strengthen their action.

Recommendations from the Global Commission for Urgent Action on Energy Efficiency call for well-designed and comprehensive policy packages with ambitious targets, clear implementation strategies and strong monitoring frameworks. These policy recommendations can be implemented quickly and in different contexts to boost efficiency improvements globally, improve energy security, offset increasing energy demand and curtail CO2 emissions growth. To maximise effectiveness in both the short and long term, existing best practice policies, cost-effective technologies and sustainable business models need to be scaled up quickly, drawing on knowledge of what has worked and what has not.

Governments have a significant role to play in this transition, not only in leading by example but also as significant final consumers of energy services. Governments can lead this process by implementing whole-of-government approaches that align priorities and actions, thereby capturing all the benefits of energy efficiency and achieving greater impacts. For example, due to its high importance for overall energy consumption and quality of life, energy-efficient cooling is driven by government national action plans in India and China.

The greatest efficiency gains are achieved by comprehensive policy packages that include a mix of regulation, information and incentives, while enabling innovation, investment and digitalisation. Using regulation such as minimum energy performance standards to exclude the worst-performing appliances, equipment, vehicles and buildings from the market and to drive up average efficiency levels has led to the greatest improvements in efficiency historically. This concerns cooling and lighting in particular (by 2050 around two-thirds of the world's households could have an air conditioner, and China, India and Indonesia together account for half of the total number).

Regulation can be supported by bulk procurement programmes, such as the UJALA (Unnat Jyoti by Affordable LEDs for All) programme for 350 million LED bulbs in India, helping technologies become more affordable and accessible. These initiatives speed up the replacement of old inefficient technologies. Governments can lead by example through green procurement rules and specifications like those implemented in the European Union, which set minimum energy and environmental standards for buildings and government procurement. The US Federal Energy Management Program, as a further example, sets energy and water-reduction goals for federal agencies, and supports implementation by providing guidance, training and technical assistance. In Indonesia, government regulation 70/2009 requires all companies with an annual energy consumption exceeding 6 000 tonnes of oil equivalent to appoint an energy manager, develop an energy conservation plan, perform an energy audit and report energy consumption to the government. Discussions about lowering the industry threshold to 4 000 tonnes of oil equivalent and introducing sector specific thresholds are underway.

Conducting comprehensive stakeholder engagement and leveraging behavioural insights can ensure that efficiency programmes are based on the actual needs and behaviours of end users, and also appropriately consider vulnerable groups. Energy efficiency policies that incorporate behavioural insights in both the design and implementation stages have proven to be more effective, as seen in the strengthening of the EU appliance energy labels. Putting people at the core of these policy actions and making better information available with the right narratives can have far-reaching impacts on the public attitudes and beliefs that drive consumption and mobility patterns – and can catalyse the much-needed behaviour change. Furthermore, redesigning policies and products to make energy savings the default option simplifies consumer choices. For instance, India has mandated that the default set-point temperature of

room air conditioners be set at 24°C, which still leaves consumers with the free choice of temperature but achieves savings by default – through many consumers simply never changing the settings.

Governments can also incentivise efficiency improvements through financial mechanisms such as direct stimulus funding, investment in public buildings, facilities and infrastructure, preferential finance, and market-based mechanisms.

Efficiency action can be rapidly scaled up by boosting demand for efficient products and services through a range of financial and non-financial incentives, and by enabling greater levels of market activity through supply-side incentives such as finance or tax benefits for manufacturers. Standards and labelling, and dedicated end-user incentives for equipment replacement are effective examples. The replacement of 1 million inefficient refrigerators in Colombia, for instance, lowered energy bills for consumers, reduced the need for subsidies to low-income households and created 12 000 jobs.

Other options include enhancing industrial efficiency through targeted fiscal incentives or large-scale programmes that can combine a range of policy measures. India's Perform, Achieve, Trade (PAT) Scheme offers a market-based approach to driving energy efficiency investment. PAT is a multi-cycle programme to reduce specific energy consumption in the most energy-intensive industries by setting consumption targets and enabling businesses who beat their target to trade the Energy Saving Certificates (ESCerts) that they are issued with.

Implementation of energy efficiency policies and programmes needs to take place at all levels of society, and at national and sub-national levels, to maximise impact. For example, to enhance energy efficiency in buildings, local governments in Mexico and India developed the implementation action required to achieve national standards.

Energy efficiency can rapidly create sustainable employment and support long-term economic growth. Job creation potential exists in construction and manufacturing, with key opportunities in building retrofits and technology replacement programmes. Drawing from international experience, the Make in India and Made in China programmes focus on creating high-quality manufacturing jobs through training and capacity building, while at the same time improving appliance efficiency and therefore making them more affordable for end users.

International collaboration can assist governments to implement energy efficiency policy more rapidly and effectively. The broad exchange of best practices allows countries to share and learn about successful and unsuccessful approaches to instilling energy efficiency in their economies. Of note is the IEA's Energy Efficiency Hub, a platform for global collaboration on energy efficiency.

Mobilising finance for clean energy deployment will be key to advancing the clean transition and ensuring energy security

According to the IEA's *World Energy Investments 2024*, global energy investment is set to exceed USD 3 trillion for the first time in 2024, with USD 2 trillion going to clean energy technologies and infrastructure. Investment in clean energy has accelerated since 2020, and spending on renewable power, grids and storage is now higher than total spending on oil, gas and coal combined.

The annual World Energy Investment report has consistently warned of energy investment flow imbalances, particularly insufficient clean energy investments in emerging market and developing economies (EMDE) outside China. There are tentative signs of a pick-up in these investments: in the IEA's assessment, clean energy investments are set to approach USD 320 billion in 2024, up by more 50% since 2020 in EMDE outside China parts of the world. This implies similar growth to the one seen in advanced economies (+50%), although below investment growth in China (+75%). The gains primarily come from higher investments in renewable power, now representing half of all power sector investments in these

economies. Progress in India, Brazil and parts of Southeast Asia and Africa reflects new policy initiatives, well-managed public tenders, and improved grid infrastructure. Africa's clean energy investments in 2024, at over USD 40 billion, are nearly double those in 2020. Yet much more needs to be done. In most cases, this growth comes from a very low base and many of the least-developed economies are being left behind (several face acute problems servicing high levels of debt).

In 2024, the share of global clean energy investment in EMDE outside China is expected to remain around 15% of the total. Both in terms of volume and share, this is far below the amounts that are required to ensure full access to modern energy and to meet rising energy demand in a sustainable way. Power sector investment in solar PV technology is projected to exceed USD 500 billion in 2024, surpassing all other generation sources combined. Though growth may moderate slightly in 2024 due to falling PV module prices, solar remains central to the power sector's transformation. In 2023, each US dollar invested in wind and solar PV yielded 2.5 times more energy output than a dollar spent on the same technologies a decade before.

In 2015, the ratio of clean power to unabated fossil fuel power investments was roughly 2:1. In 2024, this ratio is set to reach 10:1. The rise in solar and wind deployment has driven wholesale prices of electricity down in some countries, occasionally below zero, particularly during peak periods of wind and solar generation. This lowers the potential for spot market earnings for producers and highlights the need for complementary investments in flexibility and storage capacity. Investments in nuclear power are expected to have picked up in 2024, with its share (9%) in low-carbon power investments rising after two consecutive years of decline. Total investment in nuclear is projected to have reached USD 80 billion in 2024, nearly double the 2018 level, which was the lowest point in a decade. Grids have become a bottleneck for energy transitions, but investment is rising. After stagnating around USD 300 billion per year since 2015, spending is expected to have hit USD 400 billion in 2024, driven by new policies and funding in Europe, the United States, China and parts of Latin America. Advanced economies and China account for 80% of global grid spending. Investment in Latin America has almost doubled since 2021, notably in Colombia, Chile, and Brazil, where spending doubled in 2023 alone.

However, investment remains worryingly low elsewhere. Investments in battery storage are ramping up and are set to have exceeded USD 50 billion in 2024. But spending is highly concentrated. In 2023, for every dollar invested in battery storage in advanced economies and China, only one cent was invested in other EMDE. Investment in energy efficiency and electrification in buildings and industry has been quite resilient, despite the economic headwinds. But most of the dynamism in the end-use sectors is coming from transport, where investment is set to reach new highs in 2024 (+8% compared to 2023), driven by strong electric vehicle (EV) sales.

The rise in clean energy spending is underpinned by emissions reduction goals, technological gains, energy security imperatives (particularly in the European Union), and an additional strategic element: major economies are deploying new industrial strategies to spur clean energy manufacturing and establish stronger market positions. Such policies can bring local benefits, although gaining a cost-competitive foothold in sectors with ample global capacity like solar PV can be challenging. Policymakers need to balance the costs and benefits of these programmes so that they increase the resilience of clean energy supply chains while maintaining gains from trade. In the United States, investment in clean energy increases to an estimated more than USD 300 billion in 2024, 1.6 times the 2020 level and well ahead of the amount invested in fossil fuels. The European Union spends USD 370 billion on clean energy today, while China is set to spend almost USD 680 billion in 2024, supported by its large domestic market and rapid growth in the so-called "new three" industries: solar cells, lithium battery production and EV manufacturing.

How critical minerals can unlock a cleaner and more secure energy future?

An energy system powered by clean energy technologies differs profoundly from one fuelled by traditional hydrocarbon resources. Critical minerals such as copper, lithium, nickel, cobalt and rare earth elements are essential components in many of today's rapidly growing clean energy technologies – from wind turbines and electricity networks to electric vehicles (see Special focus 2). Demand for these minerals is growing quickly as clean energy transitions gather pace.

IEA Global Critical Minerals Outlook 2024 report finds that, on a path to 1.5°C climate target, demand for critical minerals quadruples by 2040. Solar PV plants, wind farms and electric vehicles generally require more critical minerals to build than their fossil fuel-based counterparts. A typical electric car requires six times the mineral inputs of a conventional car and an offshore wind plant requires 13 times more mineral resources than a similarly sized gas-fired plant. Since 2010, the average amount of mineral resources needed for a new unit of power generation capacity has increased by 50% as the share of renewables in new investment has risen.

Demand for critical minerals experienced strong growth in 2023, with lithium demand rising by 30%, while demand for nickel, cobalt, graphite and rare earth elements all saw increases ranging from 8% to 15%. Clean energy applications have become the main driver of demand growth for a range of critical minerals. EVs consolidated their position as the largest consuming segment for lithium, and increased their share considerably in the demand for nickel, cobalt and graphite.

Availability of critical minerals are one of key determinants of the speed of energy transitions, as well as crucial element to enable stable operations of manufacturing sectors. IEA is now working on how IEA member countries can share their policy measures and best practices for ensuring critical mineral supply security and also on analysis on critical minerals market developments to help ensure market transparency.

As further detailed in Special Focus 2 of this report, critical mineral supply remains however highly concentrated and there has been limited progress in terms of diversification over the past three years. Concentration of supply has even intensified in some cases. China is by far dominant in extraction of graphite (70%) and rare earth elements (69%). China's share is close to 100% in processing of the two, and key in processing cobalt (74%), lithium (65%), and copper (45%).

The geographical concentration of mining operations is set to rise further or remain high throughout to 2040. These high levels of supply concentration represent a risk for the speed of energy transitions, as it makes supply chains and routes more vulnerable to disruption, whether from extreme weather, trade disputes or geopolitics.

The "N-1" analysis is a typical measure of the resilience of any system and reveals significant vulnerabilities. If the largest supplier and its demand is excluded, then available "N-1" supply of all key energy transition minerals would fall significantly below material requirements. The situation is most pronounced for graphite where the available "N-1" supply covers only 10% of the N-1 material requirements – significantly below the minimum non-single-origin threshold of 35% proposed in the EU Critical Raw Materials Act. This indicates that without urgent efforts to expedite the development of projects, achieving announced diversification goals will be highly challenging.

Lower prices have been good news for consumers and for affordability, bringing clean technology costs back on a downward trajectory, including the 14% reduction in battery prices in 2023. However, falling prices also make spending to ensure reliable and diversified supply less appealing to investors. This price effect has had the biggest consequences in new and emerging resource-holders; in the case of nickel, three-quarters of operating or potential projects that are at risk are outside the top three producers.

The IEA Global Critical Minerals Outlook includes a new risk assessment framework for key energy transition minerals, across four major dimensions – supply risks, geopolitical risks, barriers to respond to

supply disruptions, and exposure to environmental, social and governance (ESG) and climate risks. Most minerals are exposed to high environmental risks. For example, today's refining operations occur in places where grids tend to have a higher carbon intensity, relying mostly on coal-based electricity. Meeting energy security and decarbonisation needs

Repurposing energy infrastructure for lower-carbon fuels

In the current context of high price volatility in global energy markets, governments are reducing their exposure to and dependency on fossil fuels by diversifying supply routes and sources, and by enabling the use of low-carbon fuels in existing energy infrastructure. Sourcing low-carbon fuels from several locations and from various technologies increases security of supply and protects against shocks in demand and supply. Creating new infrastructure requires high levels of investment and brings the risk of delay from the need to obtain different permits and approvals. The repurposing of existing infrastructure offers the prospect of accelerating the transition. For instance, existing thermal assets can provide the flexibility that variable renewable energy sources call for, complementing other sources, such as transmission, storage and demand response, while securing emission reduction benefits if they are run on lower-carbon fuels.

Low-carbon gases (including biomethane, low-emission hydrogen, synthetic methane and methane subject to CCUS) are set to play a key role in decarbonisation pathways. In the IEA Net Zero Scenario, low-carbon gases account for close to 75% of total gaseous fuels in total final energy consumption in 2050, and for the majority of gaseous fuels consumed in the power sector. In turn, low-carbon gases keep the share of gaseous fuels in total final energy consumption close to today's levels and play a key role in the hard-to-abate sectors, including industry, long-haul transport and seasonal energy storage. In the power sector, low-carbon gases are set to provide flexible back-up supply in a system dominated by variable renewable sources of electricity supply.

The existing gas infrastructure can fast-track the deployment of low-carbon gases, by providing network access, reducing transport costs and ultimately facilitating their integration into the broader energy system. At the upstream level, natural gas and condensate fields, depleted gas reservoirs and their related above-ground infrastructure could be used for CO2 storage, enabling the deployment of CCUS-based solutions as in the production of hydrogen from methane. The vast system of gas transmission and distribution pipelines can be repurposed to carry low-carbon gases.

Biomethane and synthetic methane are perfectly interchangeable with conventional methane due to their almost identical chemical and physical properties. Nevertheless, they will require the development of standards to ensure uniform gas quality across interconnected gas systems and diminish any risk of deviating from them. Biomethane is mainly fed into distribution networks due to the decentralised nature of its production. In the longer term, the high penetration of biomethane at the distribution level will necessitate closer integration between transmission and distribution networks. Bidirectional compressor stations would enable reverse flows from distribution to the transmission network, facilitate daily balancing and provide access to biomethane for seasonal gas storage sites (which are most often connected to the transmission system).

In the case of low-emission hydrogen, blending can provide a temporary solution until dedicated hydrogen transport systems are developed. Depending on the characteristics of the gas transmission system, hydrogen can be blended at rates of 2-10% H2 by volume without substantial retrofitting of the pipeline system. The hydrogen tolerance of polymer-based distribution networks is typically greater, potentially allowing blending of up to 20% with minimal or possibly no modifications to the grid infrastructure. Natural gas pipelines can also be repurposed to serve as hydrogen distribution. Pipeline repurposing can be substantially less costly and the lead times much shorter compared to new-build hydrogen networks.

The decommissioning of existing infrastructure can cause economic disruption for local communities that are dependent on it for employment and revenues. Leveraging existing strengths to identity new uses for existing infrastructure during the transition can bring many benefits. Notably, repurposing or converting existing infrastructure allows for the preservation of large parts of the value of the infrastructure, while retaining jobs and tax bases in communities where the infrastructure is located. For instance, a number of current oil and gas producing countries are currently developing or looking to develop CCUS, hydrogen and offshore wind energy industries, using existing skillsets and knowledge bases from oil/gas production, including offshore. Policymakers should assess the opportunities for scaling up the deployment of low-carbon fuels using today's energy infrastructure before giving the owner consent to reclaim or demolish existing infrastructure along the entire value chain. Such a forward-looking and people-centred approach to existing energy infrastructure could lead to substantial cost savings and improve the resilience of the energy system.

Repurposing coal infrastructure also can accelerate just and secure energy transitions. The most interesting asset in the coal value chain is generally the coal power plant and its associate infrastructure, in particular the connection with the electricity transmission grid. There is currently over 2 000 GW of coal power generation capacity that could be converted into low-carbon assets in different ways, providing adequacy, flexibility and stability to the electricity grid. The first option is to retrofit the plants with CCUS. Another option is to use low carbon fuels, such as sustainable biomass, or ammonia produced from renewable hydrogen or fossil fuels in combination with CCUS. Conversion to biomass has already been done in some plants around the world, and the project of ammonia co-firing is making good progress such as the Gresik Thermal power plant in Indonesia. In addition, technological development of co-firing high shares of ammonia and ammonia single-fuel firing is progressing as well. Biomass has an additional advantage in that, when combined with CCUS, it can turn coal power plants, currently the largest source of CO2 emissions, into a source of negative emissions. Other possibilities like conversion to a nuclear facility, thermal storage or a combination of the two should not be overlooked. The conversion or retrofitting of existing coal power plants offers many advantages, in particular the prospect of faster permitting processes and use of an existing electricity grid connection, two important bottlenecks identified in clean energy transitions.

Conclusions

Key recommendations to help buttress energy security in the transition, when the clean energy and fossil fuel systems co-exist and are both required to deliver reliable energy services are:

- Synchronise scaling up a range of clean energy technologies with scaling back of fossil fuels. Investing in clean energy is key to avoid future crises while reducing emissions. In the Net Zero Emissions by 2050 (NZE) Scenario, around USD 9 is spent on clean energy by 2030 for every USD 1 spent on fossil fuels. Cutting investment in fossil fuels ahead of scaling up investment in clean energy would lead to energy price escalations, and undermine people's support to energy transitions.
- Tackle the demand side and prioritise energy efficiency. The energy crisis highlights the crucial role of energy efficiency and behavioural measures in helping to avoid mismatches between demand and supply. Since 2000, efficiency measures have reduced unit energy consumption significantly, but the pace of improvement has slowed in recent years. Policies that accelerate the rate of retrofits are crucial as over half of the buildings that will be in use in 2050 have already been built.
- Collaborate to bring down the cost of capital in emerging market and developing economies**.** The cost of capital for a solar photovoltaics (PV) plant in 2021 in key emerging economies was between two- and three-times higher than in advanced economies and China. Tackling related risks and

lowering the cost of capital in emerging and developing economies by 200 basis points reduces the cumulative financing costs of getting to net zero emissions by USD 15 trillion through to 2050.

- Manage the retirement and use existing infrastructure carefully. Some parts of the existing fossil fuel infrastructure perform functions that will remain critical for some time, even in rapid energy transitions. They include gas-fired plants for electricity security – in the European Union peak requirements for natural gas rise to 2030 even as overall demand goes down by 50% – or refineries to fuel the residual internal combustion engine car fleet. Unplanned or premature retirement of this infrastructure can have negative consequences for energy security.
- Tackle the specific risks facing producer economies. Diversification will be crucial to mitigate risks. Some countries are investing part of their current windfall oil and gas profits in renewables and low-emissions hydrogen. Potential export earnings from hydrogen are no substitute for those from oil and gas, but low-cost renewables and carbon capture, storage and utilisation (CCUS) can provide a durable source of economic advantage by attracting investment in energy-intensive sectors.
- Invest in flexibility to strengthen electricity security. Reliable electricity is central to transitions as its share in final consumption rises from 20% today 50% in the IEA's Net Zero Scenario. Increasing variability in electricity supply and demand means that the requirement for flexibility quadruples by mid-century in both scenarios. Battery storage and demand-side response become increasingly important, each providing a quarter of the flexibility needs in 2050.
- Ensure diverse and resilient clean energy supply chains. Critical minerals demand for clean energy technologies is set to quadruple by 2050, with annual revenues reaching USD 400 billion. High and volatile critical mineral prices and highly concentrated supply chains could delay energy transitions or make them more costly. Minimising this risk requires action to scale up and diversify supplies alongside recycling and other measures to moderate demand growth.
- Foster the climate resilience of energy infrastructure. The growing frequency and intensity of extreme weather events presents major risks to the security of energy supplies. IEA analysis of the risks facing four illustrative assets shows that the potential financial impact from flooding could amount to 1.2% of their total asset value in 2050, and in one case would be four-times higher than this without flood defences in place. Governments need to anticipate the risks and ensure that energy systems have the ability to absorb and recover from adverse climate impacts.
- Provide strategic direction and address market failures, but do not dismantle markets. Governments need to take the lead in ensuring secure energy transitions by tackling market distortions as well as correcting for market failures. However, transitions are unlikely to be efficient if they are managed on a top-down basis alone. Governments need to harness the vast resources of markets and incentivise private actors to play their part. Some 70% of the investments required in transitions need to come from private sources.

References

IEA (2022), *World Energy Outlook 2022*, OECD Publishing, Paris, https://doi.org/10.1787/3a469970-en. [1]

OECD/NEA (2010), *The Security of Energy Supply and the Contribution of Nuclear Energy*, Nuclear Development, OECD Publishing, Paris, https://doi.org/10.1787/9789264096356-en. [2]

Notes

[1] International Energy Agency.

[2] Since 2018, the annual revenues generated by the oil and gas industry have averaged close to USD 3.5 trillion. Around half of this went to governments, while 40% went back into investment and 10% was returned to shareholders or used to pay down debt.

[3] Two key characteristics determine the impact of different greenhouse gases on the climate: the length of time they remain in the atmosphere and their ability to absorb energy. Methane has a much shorter atmospheric lifetime than carbon dioxide (CO2) – around 12 years compared with centuries – but absorbs much more energy while it exists in the atmosphere. There are various ways to combine these factors to estimate the effect on global warming and express a tonne of a methane in CO2 equivalent terms (CO2-eq). The most common is the global warming potential (GWP), although different conversion factors can be applied. Some consider the impact of methane over a 20-year timeframe (GWP20), with one tonne of methane equivalent to 82-87 tonnes of CO2. Others look at its impact over a 100-year timeframe (GWP100), with one tonne of methane equivalent to around 30 tonnes of CO2. Alternative metrics, such as the Global Temperature Potential, can be used to more closely link methane emissions to the temperature increase expected in a future year.

5. Managing security implications of international investment

Ana Novik, Joachim Pohl and Nicolás Rosselot[1]

Introduction

Foreign investment brings benefits to home and host countries and societies. It contributes to spurring growth, employment and development. However, recent geoeconomic and geopolitical developments and rapid technological advances have drawn greater attention to security implications of certain foreign investments. To manage these implications, many governments, especially in advanced economies, have adjusted their investment policies.

Investment security is a component of governments' broader efforts to strengthen their economic security and aligns closely with more recent efforts to address risk associated with international economic interactions. Historically, investment-related tools have been in place in many countries for decades, well before the more recent surge in economic security concerns triggered policy changes in other areas such as supply-chain resilience and the like. As a forerunner, instruments developed to manage security concerns for investment may inspire and inform economic security initiatives in other areas.

As an area of economic security where developments began early and progressed swiftly, investment security may provide important insights for policy considerations in other areas where economic security considerations emerge. Experiences may be transferable to areas such as research co-operation and international researcher exchanges, outward investment, as well as some aspects of trade.

This chapter traces how investment security tools have developed and endeavours to project how they may evolve. The chapter documents the important role that internationally agreed policy principles, such as the OECD 2009 Guidelines on Investment Policies related to National Security, and peer-learning play in developing policies that reconcile the continued imperative of openness to international investment with the growing priority to manage security implications of this openness. Experience gathered in this pioneering field may also allow governments to anticipate emerging needs and consider other components of holistic economic security policies.

The emergence and evolution of investment security instruments

Foreign investment contributes to prosperity in all stages of economic development, and governments continue their decades-long endeavour to open their economies to foreign capital. As a result, remaining barriers to international capital flows are progressively being reduced, and today, few restrictions to international investment remain.[2]

This drive for greater openness coexists with the need for governments to address risks that may be associated with certain foreign investments and that may threaten their security interests. For the most

part and until recently, policies to manage this risk existed merely on the books and in most economies played a negligeable role in practice.

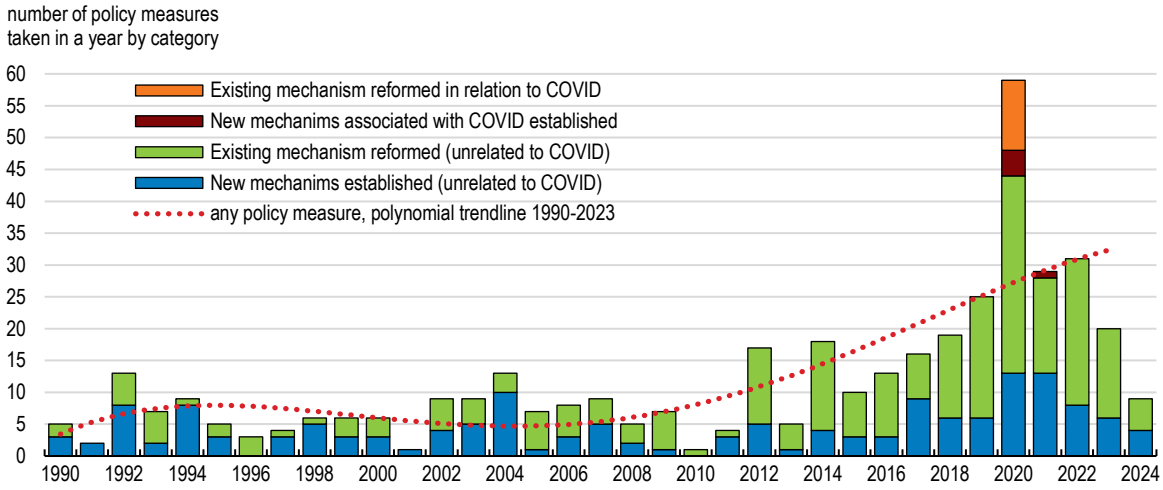
Several factors have driven a historically unprecedented change of heart and policy in this area in the past decade. Geopolitical and geoeconomic developments have increased concerns about security implications of foreign investment. A growing role of state-driven or state-supported investors that participate in international investment, explicit programmes to acquire know-how in sensitive sectors, more assertive attitudes in economic and military dimensions in some regions, and global crises have all contributed to greater risk-awareness by demonstrating the consequences of dependencies and vulnerabilities. The rapid development of certain technologies, their potential for military applications, and the massive expansion of sensitive, personalised data have also fuelled concerns that foreign investments may occasionally entail substantial risk. These include traditional aspects of espionage and sabotage that a foreign presence in the country could facilitate in certain circumstances, especially in border areas or near sensitive sites; the potential outflow of sensitive technologies or information that could be exploited by malign actors or to advance foreign countries' military capabilities; and dependencies from certain foreign economies, especially in strategic sectors.[3]

Many governments, especially in OECD economies, have nuanced their stance of hitherto almost unconditional openness to international investment in light of these developments. They have introduced new policies to manage security risks and have strengthened existing policies considerably. Even countries that felt little exposure only a few years ago have taken a closer look at the security implications of certain foreign investment projects. These efforts continue in many advanced economies but there is considerable variation across the OECD area and beyond, with some governments showing greater reluctance to introduce measures to manage investment related security risks.

In most OECD countries, investment-related risks continue to play a central role in economic security strategies. Such strategies document the preoccupation with the presence of foreign investors in sensitive locations such as border areas[4] or significant shareholdings in sensitive enterprises such as those operating critical infrastructure where it could facilitate espionage or sabotage, or grant leverage over host-state governments.[5] Economic security strategies also point to access to sensitive data in host countries as well as unwanted technological leakages,[6] and to the potential generation of economic and financial dependencies.[7]

Figure 5.1 documents the dynamic development of policy changes in 72 advanced, emerging market and developing economies.[8] The figure shows annual aggregates of the introduction of new and reform of existing policies to manage investment-related risk beginning in 1990, documents a significant acceleration after 2014 and the continued dynamism of policymaking. Announcements of reforms in the economies included in the sample suggest that the reform drive will remain important, at least in the near future.[9]

Figure 5.1. Introduction and reform of investment policies to safeguard national security interests



Note: Sample includes 72 advanced, emerging, and developing economies from within the subset of 83 economies. More than one measure may be counted for a given country in a year. A new mechanism or reform is associated with COVID-19 if the government explicitly justified its introduction, at least in part, with the pandemic or its fallout.
Source: OECD.

Recent crises have shaped the developments in foreign inward investment policy to different degrees. The Global Financial Crisis of 2008/09 had little immediate impact on developments in this area and, if anything, occupied investment policymakers with managing the immediate fallout of that crisis rather than management of security implications. The COVID-19 pandemic in turn has triggered a substantial number of policy changes that were explicitly linked to the crisis (OECD, 2020[1]).[10] Russia's war of aggression against Ukraine has also been associated with some new policy changes in 2022, but has overall affected policy dynamics to a lesser extent (OECD, 2022[2]). This is likely because the war caused fewer economic disruptions in a limited number of countries, policies had just been strengthened and remained in place from the preceding crisis, and sectors associated with military conflict were already covered by investment policies related to national security interests in most countries.[11]

Policy developments did not take place in all countries at the same time. While most advanced and major emerging economies have introduced new policies or carried out reforms in this area since 2014, emerging and developing economies began to carry out similar reforms as of 2020 (e.g. Moldova, the Philippines, South Africa and Viet Nam). Reforms are currently under consideration in Bosnia and Herzegovina and North Macedonia, for example.

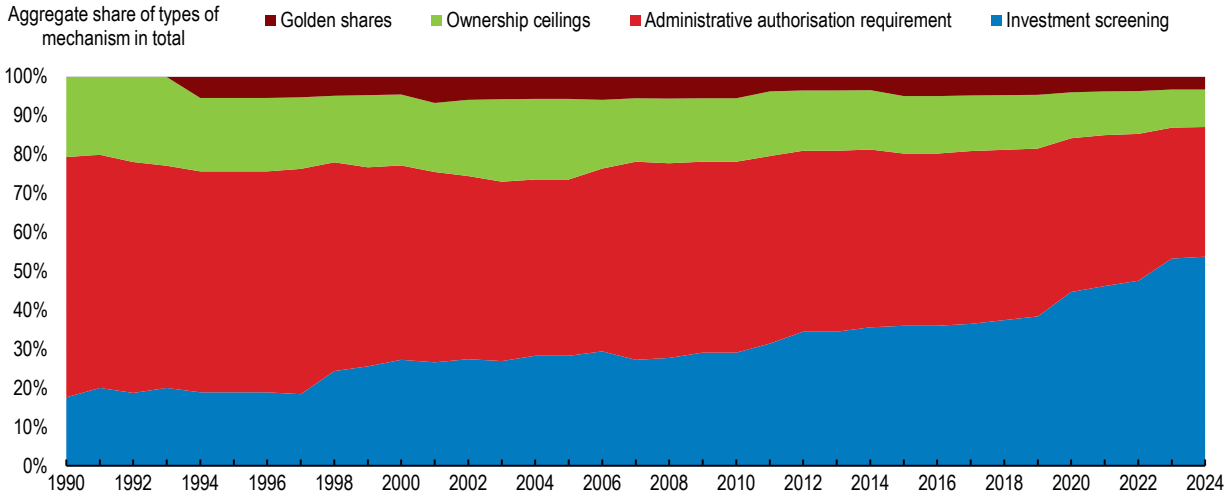
In OECD countries, investment screening has become the most common means to manage security implications associated with foreign investment

The question how investment-related risks is best managed has found different responses in different jurisdictions and at different times. In earlier decades, instruments to manage security risks showed great diversity in approaches and had idiosyncratic features. Such instruments include golden shares, foreign ownership ceilings, administrative authorisation requirements for acquisitions in designated asset groups, security assessments at the establishment or registration of enterprises, and investment screening mechanisms (OECD, 2020[3]). In addition to such instruments that seek to manage risks by controlling acquisition of ownership of sensitive assets, some jurisdictions maintain licensing requirements for

sensitive activities (e.g., for the provision of certain services or distribution of certain products), restrictions related to participation in public procurement, or ineligibility for aids and subsidies for security reasons.

The relative frequency of uses of different instruments is evolving as new mechanisms are brought into effect, and older mechanisms are phased out or replaced. Figure 5.2 shows the evolution of the relative distribution of four of the most frequent approaches to manage security risks associated with foreign investment in OECD members over last three decades. It documents an earlier dominance of administrative authorisation requirements and, to a lesser extent, foreign ownership ceilings. Golden share arrangements have played and continue to play only a marginal role. Administrative authorisation requirements and foreign ownership ceilings combined accounted for about three quarters of all mechanisms in operation during most parts of the 1990s. Recent policymaking efforts have led to a relative decline of the share of these types of policies, and investment screening is now the single-most frequently used type of policies to address national security concerns that are associated with certain international investments in OECD countries.

Figure 5.2. Relative frequency of mechanisms to manage security implications of foreign investment



Note: Data for OECD members, showing relative frequency of approaches, counting individual mechanisms separately; "100%" corresponds to the total number of distinct mechanisms of one of the four categories in force in a given year. One economy may have several mechanisms contemporaneously.
Source: OECD.

International exchanges at the OECD as well as guidance enshrined in the 2009 OECD Guidelines for Recipient Country Investment Policies relating to National Security (2009 Guidelines) have led to a greater similarity of the instruments' designs and implementation overall. Investment screening, understood as implying a case-specific review from a class of potentially problematic transactions, has become the most frequently used instrument to address risks associated with inward investment.

In OECD countries, almost all newly introduced investment policies related to national security employ investment screening approaches. More than four out of five OECD members now operate investment screening mechanisms, up from 55% at the end of 2020 and from only just over 42% a decade ago. The preference for investment screening has likely been shaped by recommendations set out in the 2009 Guidelines and the principles of non-discrimination, transparency, predictability, proportionality and accountability, which has also inspired EU rules – the Regulation (EU) 2019/452 of the European

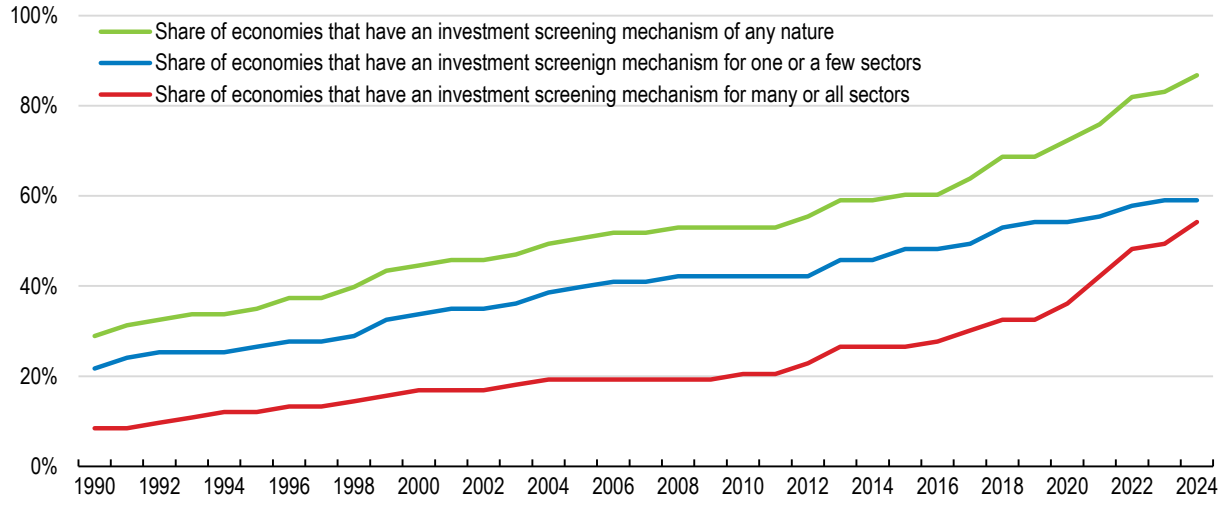
Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union (EU Regulation 2019/452).

Preferences for the use of certain instruments and approaches to manage security implications continue to evolve. New approaches are introduced, reflecting evolutions in investor strategies and behaviour, changing risk perception, and evolving economic realities. For example, many advanced economies now focus their review mechanisms on mergers and acquisitions, while some emerging economies are more focused on the security risks associated with newly established or registered enterprises.

The scope of application of investment policies related to national security has significantly broadened

Evolutions in the geopolitical and geoeconomic environment and a changing assessment of sources of risk and needs have also brought about a change in the scope of application of investment review mechanisms. While in earlier decades, most mechanisms used to be sector-specific or limited to a few sectors, cross-sectoral or multi-sectoral mechanisms have recently become more common. Cross-sectoral mechanisms consider security implications of investment in any sector, while multi-sectoral mechanisms, apply to many economic sectors that are considered sensitive. Single-sector mechanisms often remain in force besides mechanisms that apply to multiple or all sectors. The trend towards cross or multisectoral application of policies, observed since the early 1990s, has recently further accelerated, and that well beyond OECD members (Figure 5.3).

Figure 5.3. Spread of investment policies related to national security interests and broadening of their scope of application



Note: Data shows investment review mechanisms in effect in a subset of 61 economies from within the 72 economies considered overall.
Source: OECD.

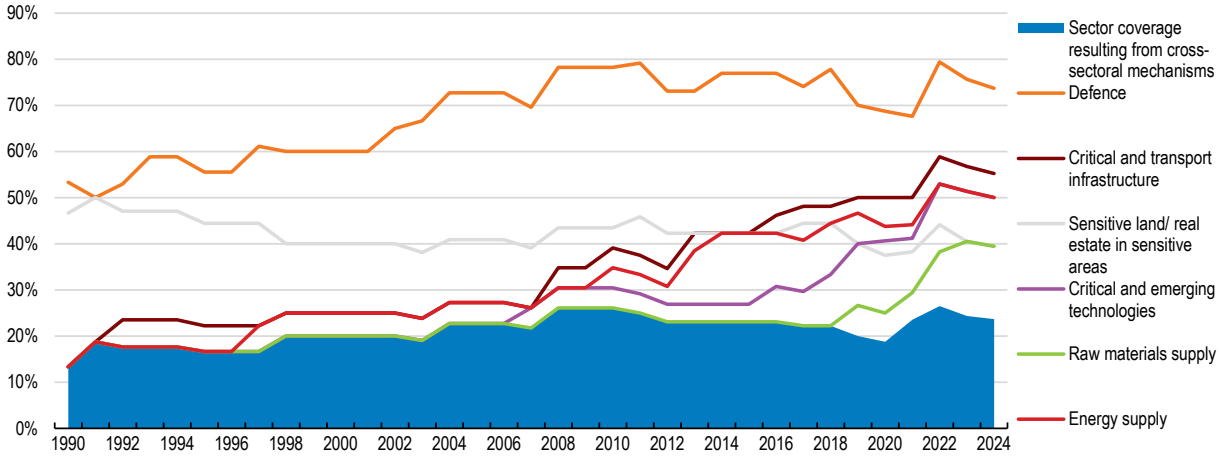
The evolution of sectoral coverage of investment review mechanisms has led to significant changes in the composition of sectors that can attract scrutiny. Until the 1990s, policies almost exclusively focused on defence industries and real estate in sensitive locations, often addressed in single-sector mechanisms. The sectoral coverage has diversified markedly since. Critical infrastructures – where not covered by some economy-wide screening mechanisms – were explicitly included in the scope of some mechanisms since the beginning of the 1990s, and critical and emerging technologies appeared separately towards the end

of the 1990s. More recently, transactions in the energy and raw materials sectors have increasingly been subject to investment screening (Figure 5.4).

While some of the sectoral additions absorb risks that result from longer-term processes such as privatisation of critical infrastructure, other changes reflect responses to newly identified risks. For example, health infrastructure and biotechnologies were rapidly included in the scope of mechanisms to manage security implications of foreign investment in many economies in 2020 when severe shortages of vaccines and medical equipment appeared during the COVID-19 pandemic (OECD, 2020[1]).

Figure 5.4. Sector coverage of policies to manage security implications of foreign investment

Sector covered (share of economies that operate any mechanisms in a given year)



Note: Graphs show aggregate occurrence of coverage of the indicated sector in investment policies related to national security interests in a given year in OECD members. Legislation may frame these sectors in different terms, and aggregations were made to enhance readability. The grey area shows the proportion of economy-wide mechanisms which cover the indicated sectors but do not mention them specifically.
Source: OECD.

Recent crises brought attention to sensitivities of additional sectors

Recent global crises focused governments' attention on enterprises operating in certain critical sectors and globally integrated industries. This led to greater scrutiny of acquisitions of enterprises operating in critical and emerging technologies (CET) and those that supply certain critical inputs, such as critical raw materials, energy and food, and where this was not previously the case, has brought these under the scope of investment screening mechanisms.

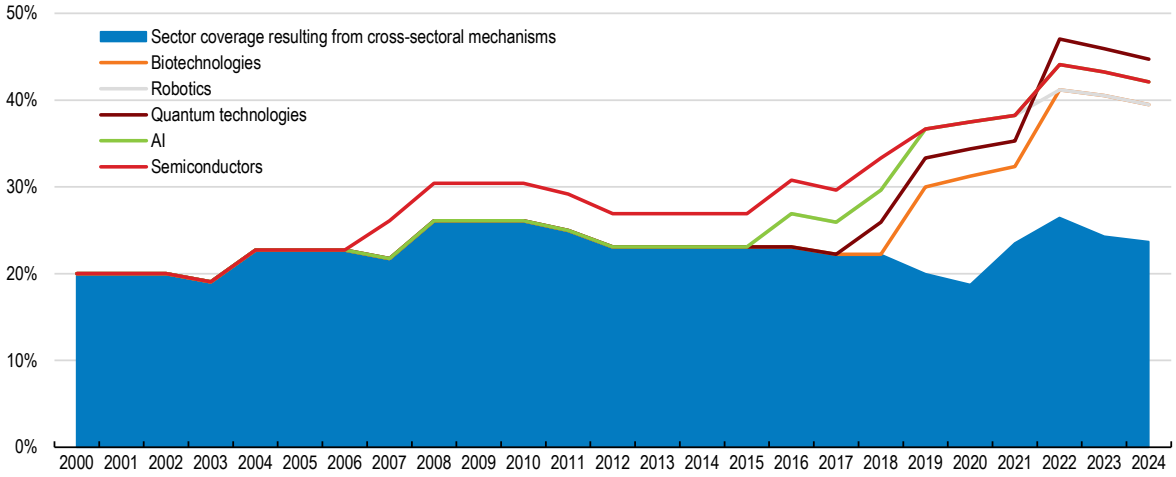
Foreign investment in critical and emerging technologies

The sensitivity of CET-related enterprises has been recognised for decades and considerations whether to control their acquisition date back to the 1980s. In some countries, the sector was covered under economy-wide mechanisms, and already in the early 2000s, CET sectors were mentioned explicitly in the scope of mechanisms to manage security implications of foreign investment, a trend that has markedly accelerated since 2015. Artificial Intelligence (AI), a foundational technology with dual-use applications, has most recently entered the list of sectors that are explicitly covered by screening mechanisms (OECD, 2021[4]). Several individual subsectors of CET such as semiconductors, quantum technologies, and robotics are now covered by around 40% of OECD countries' mechanisms that have any such policies,

and in many countries, these sectors are singled out specifically. Figure 5.5 shows a breakdown by subsector and the historical evolution since 2000.

Figure 5.5. Critical and emerging technologies: coverage under policies to manage security implications of foreign investment

Sector covered (share of economies that operate any mechanism in a given year)



Note: Data for OECD members show aggregate occurrence of coverage of the indicated sector in investment policies related to national security interests in the subset of jurisdictions that have any policy in that year. Legislation may frame these sectors in different terms and aggregations were made to enhance readability. The grey area shows the proportion of cross-sectoral mechanisms which cover the indicated sectors but do not mention them specifically.
Source: OECD.

Supply and access to CETs are also the focus of initiatives at national and international levels. These include, at domestic level, initiatives to identify and anticipate future technologies that warrant foreign investment control or related measures,[12] that subject advanced technologies to more stringent review,[13] or subject these technologies to specific rules and mechanisms altogether.[14] These initiatives add to efforts to establish or strengthen international co-operation to regulate access to these technologies where they may have national security implications.[15]

Growing concerns about foreign access to CETs is also reflected in caseload statistics[16] and in particular in the share of in-depth scrutiny and risk mitigation measures.[17]

Resilience of supply chains

Shocks to supply chains have focused governments' attention since 2020, when the COVID-19 pandemic led to shortages of essential products and services whose availability had hitherto been taken for granted. Russia's war of aggression against Ukraine heightened concerns further. Foreign investment has an ambivalent relationship with the resilience of supply chains: It can reduce dependencies by broadening the supplier-base but can also lead to concentrations of supplies with fewer suppliers or bring supply under control of potentially unreliable enterprises. Several countries have thus begun to adjust their investment policies to mobilise investment screening and similar instruments in favour of greater resilience of their supply chains.

The concern is not new as such, as the historical focus on defence production documents. Several countries have had restrictions on foreign participation in defence production for this reason. What is new is the expansion of the list of industries whose inclusion in the scope of screening is motivated by concerns

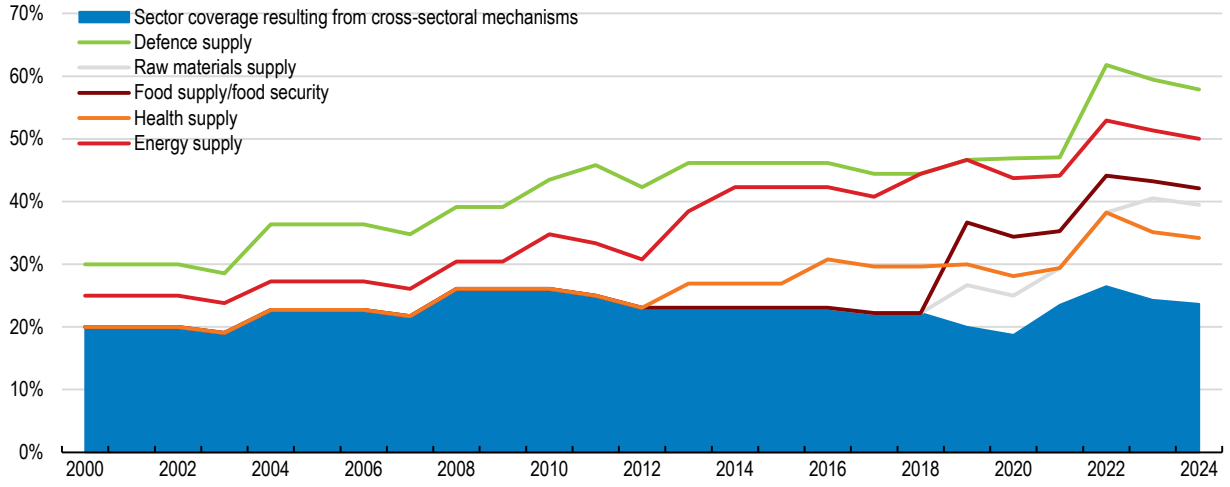
about supply chain resilience which now include, among others, the supply of critical raw materials, energy, food and health-related goods and services. Figure 5.6 documents the relative frequency of selected areas in the coverage of mechanisms to manage security implications of foreign investment between 1990 and 2024.

A further change that concerns about supply chain resilience has brought about is its explicit recognition as a risk factor during investment review processes. Screening authorities are now expected to consider factors such as the resulting concentration of ownership or control by foreign investors in critical supply chains, the presence of alternative suppliers at national and international levels, and the security implications for supply relationships with other critical industries or government entities affected by the transaction.

Recent screening legislations in Estonia, Luxembourg, Malta or Slovakia for example explicitly include the consideration of supply of critical inputs as being a factor for authorities to consider in the assessment of the security risks of a given transaction. The United States and Japan, among others, have issued policy statements or guidelines to include these considerations and to provide additional guidance on the factors that reviews need to consider. The number of screened transactions in which critical inputs played a role has risen markedly over the past years, according to official government figures.[18]

Figure 5.6. Critical inputs: coverage under policies to manage security implications of foreign investment

Sector covered (share of economies that operate any mechanism in a given year)

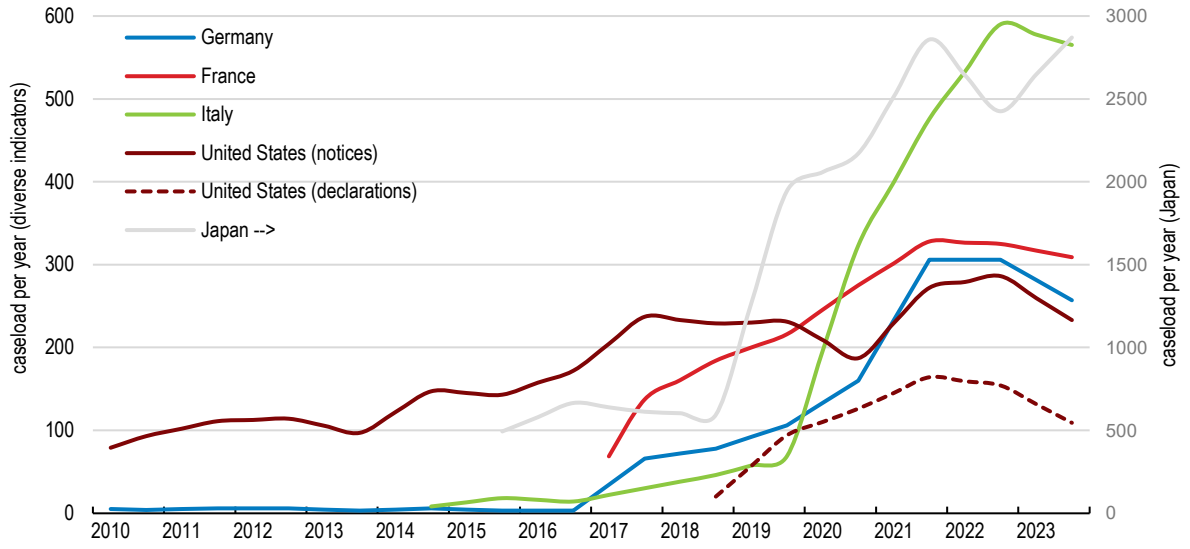


Note: Data for OECD countries show aggregate occurrence of coverage of the indicated sector in investment policies related to national security interests in the subset of jurisdictions that have any policy in that year. Legislation may frame these sectors in different terms, and aggregations were made to enhance readability. The grey area shows the proportion of cross-sectoral mechanisms which cover the indicated sectors but do not mention them specifically.
Source: OECD.

The number of screened transactions has significantly increased in recent years

The number of transactions that have been screened has grown significantly since 2017, especially in Europe but also in Japan and Canada (Figure 5.7). This was partly because of the introduction of new mechanisms and the expansion of their scope. However, in several jurisdictions, the number of transactions has recently plateaued, potentially due to declining global FDI flows in 2022 and 2023 (OECD, 2024[5]).

Figure 5.7. Caseload under investment screening mechanisms



Note: Time-series reflect official data made available by governments by February 2025. Indicators differ and depend on data availability and are not comparable across jurisdictions. They also depend on designs of review mechanisms. Data as reported for calendar years for all countries, including those where data are reported for fiscal years that run from July to June. For better readability, data for Japan are plotted on the right axis. Data for Germany refer to reviews under either of its two mechanisms under the Foreign Trade and Payments Act (AWG) and Ordinance (AWV) – §§ 55-59 and 60-62 AWV, respectively; for France, to applications filed; for Italy, to notifications; for the United States, to notices and declarations; for Japan, to the total number of prior notifications.
Source: OECD based on data reported by governments.

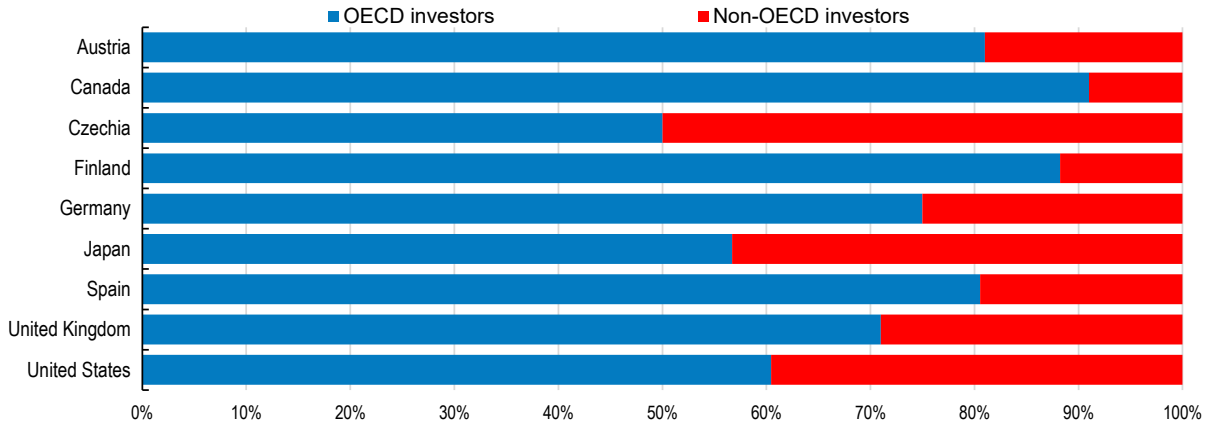
The proportion of transactions subject to review as a share of all inward investment transactions has also grown in some jurisdictions for which such data are available. For example, in Finland, the share of investment proposals subject to review in overall inward investment proposals has increased sixfold between 2017 and 2023, from 3.7% of all investment projects in 2017 to 22% in 2023.[19] France has reported a twofold increase between 2017 and 2020 (from 11% to 23%), before this indicator plateaued in 2021 at 20%.[20]

Governments have identified several reasons for this overall upward trend. These include: the broader scope of mechanisms,[21] greater knowledge of notification obligations among investors and associated greater compliance,[22] as well as exposure of some assets to foreign takeovers under the conditions of the COVID-19 pandemic.[23] In EU Member States, the information-sharing under the co-operation mechanism under EU Regulation 2019/452 has also been cited as a source of growing case numbers.[24]

More granular information on transactions notified to and reviewed by authorities are becoming available for ever more jurisdictions (OECD, 2021[6]). Data for 2022 show that investments originating in OECD countries account for the largest share of reviewed transactions (Figure 5.8), which is likely the result of the large share of transactions by OECD investors in transactions overall. Most of these cases appear to be cleared by authorities with no further intervention; denial and mitigation remain rare in most OECD jurisdictions.[25]

Figure 5.8. Investor origin of reviewed transactions

Share of country groups in total transactions subject to review in 2022



Note: Indicators vary and depend on the format and content of data aggregation by reporting countries: Austria: origin of investor in reviewed case; Canada: origins of investment filings; Finland: origin of notifications; Japan: prior notifications; the United Kingdom: eligible transactions; the United States: notices and declarations. Data on origins of investors for Canada, Germany, Japan and Spain exclude investors from unspecified EU and EEA countries due to the unavailability of disaggregated data. The numbers for the United Kingdom exclude domestic investors that are subject to the National Security Investment Act 2021. Data for Austria and Japan explicitly refer to the beneficial ownership of investors. The data are not normalised for the number of transactions originating in the country-groupings, a factor that likely contributes to the distribution.
Source: OECD based on official data reported by governments.

OECD policy tools help promote good practice in design and implementation of investment screening mechanisms

Policy dialogue at the OECD and disciplines developed by its policy community have played an important role in shaping investment policies related to national security and ensuring designs that are effective in managing security concerns while keeping markets open for international investment. These mechanisms were particular important in a field where most countries had limited prior experience and where developments took place at a high pace.

The 2009 Guidelines for Recipient Country Investment Policies relating to National Security (OECD/LEGAL/0372, 2009 Guidelines) encourage governments that are introducing investment policies to safeguard security interests to apply the principles of non-discrimination, transparency, predictability, proportionality and accountability. These principles are recognised for their usefulness as a benchmark for policy design. Exchanges of experience among policymakers, facilitated by the OECD, can also help governments to adopt best-practice solutions, drawing on a large set of examples and reforms in this area. Analytical, comparative studies on different aspects of policy design and regular updates on policy developments complement the guidance and policy dialogue among governments.

Conclusions

In the past decade, geopolitical and geo-economic changes have led many governments to reconsider the implications of foreign investment and foreign ownership in sensitive parts of their economies. This process has led to a historically unprecedented policy making activity in this area. Governments have introduced mechanisms to review individual investment proposals, expanded the scope of application of these

mechanisms, and have progressively tightened the rules governing the review. The number of transactions that are subject to review and potentially intervention has grown manifold in the space of only a few years.

An assessment of the impact of these mechanisms on international investment in general, on specific sectors or specific economies is difficult and will remain difficult due to lack of fine-grained information, absence of valid indicators, and limited information – given the parties interest in discretion and the sensitive nature of the considerations that underpin government decisions, little is known or can be deducted as to the implementation practice across jurisdictions.

Despite the growth of security concerns in a complicated geopolitical environment and a succession of crises, governments remain interested in attracting foreign capital and in openness to foreign investment. International co-operation on policy design as hosted by the OECD as well as policy guidance and standards help governments reconcile the need to manage security implications of certain foreign investments with their continued stance to openness.

References

OECD (2024), *FDI in Figures*, https://www.oecd.org//content/dam/oecd/en/topics/policy-sub-issues/fdi/FDI-in-Figures-April-2024.pdf [5]

OECD (2022), *International investment implications of Russia's war against Ukraine*, https://doi.org/10.1787/a24af3d7-en [2]

OECD (2021), *OECD Business and Finance Outlook 2021: AI in Business and Finance*, OECD Publishing, Paris, https://doi.org/10.1787/ba682899-en [4]

OECD (2021), *Transparency, Predictability and Accountability for investment screening mechanisms*, https://www.oecd.org/en/publications/transparency-predictability-and-accountability-for-investment-screening-mechanisms_61175d59-en.html.. [6]

OECD (2020), "Acquisition- and ownership-related policies to safeguard essential security interests: Current and emerging trends, observed designs, and policy practice in 62 economies"*, OECD Working Papers on International Investment*, No. 2020/1, OECD Publishing, Paris, https://doi.org/10.1787/61a64a3b-en [3]

OECD (2020), *Investment screening in times of COVID-19 and beyond*, https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/07/investment-screening-in-times-of-covid-19-and-beyond_c3324953/aa60af47-en.pdf [1]

Notes

[1] OECD Directorate for Financial and Enterprise Affairs, Investment Division.

[2] See for country-specific information the OECD FDI Regulatory Restrictiveness Index (FDI RRI) at https://www.oecd.org/en/data/indicators/fdi-restrictiveness.html

[3] More details about these developments and the emerging concerns are available in (OECD, 2020[3]).

[4] Lithuania's National Security Strategy (as amended in 2021) recognises the need to "develop and to effectively implement a system of control over foreign investments and transactions in strategic (…) and their protection zones come only from investors who (…) have passed the national screening mechanism."

[5] The European Economic Security Strategy underlines concerns associated with certain foreign investment that can generate "Risk of disruptions or sabotage of critical infrastructures, such as pipelines, undersea cables, power generation, transportation, electronic communication networks, that undermine the secure and reliable provision of goods and services or data security in the EU." Similarly, the Netherland's 2023 Security Strategy highlights needs to "Strengthen the protection of critical infrastructure against unwanted foreign takeovers, mergers and investments by bringing newly designated critical providers under the scope of the Investments, Mergers and Acquisitions Security Screening Act".

[6] The Swedish 2024 National Security Strategy recognises the need to increase "awareness of intelligence-related threats and the risks of undesirable investments, acquisitions and unlawful technology transfers is an important instrument to strengthen economic security".

[7] As an example, in the context of a recent reform of its investment screening legislation, Canadian authorities announced that: "The Government of Canada has committed to promoting economic security and combatting foreign interference by modernizing the ICA [the Investment Canada Act] to strengthen the national security review process and better mitigate economic security threats arising from foreign investment." Similarly, Lithuania's National Security Strategy (as amended in 2021) mentions: "The influence of foreign states in creating and maintaining economic and energy dependence and the threats that such dependence poses to national security remain relevant, and their management requires particular attention in terms of assessing compliance with national security interests."

[8] This chapter is based on policy observations in 83 economies: Andorra, Argentina, Australia, Austria, Belgium, Brazil, Bosnia and Herzegovina, Bulgaria, Brunei Darussalam, Cambodia, Canada, Chile, P.R. China, Colombia, Costa Rica, Croatia, Czechia, Denmark, Ecuador, Egypt, El Salvador, Estonia, Fiji, Finland, France, Germany, Greece, Guatemala, Honduras, Hungary, Iceland, India, Indonesia, Ireland, Israel, Italy, Japan, Jordan, Kazakhstan, Korea, Kosovo, Lao PDR, Latvia, Lithuania, Luxembourg, Malaysia, Malta, Mauritius, Mexico, Moldova, Morocco, Myanmar, the Netherlands, New Zealand, North Macedonia, Norway, Panama, Paraguay, Peru, the Philippines, Poland, Portugal, Romania, Saudi Arabia, Serbia, Singapore, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Chinese Taipei, Thailand, Timor-Leste, Tunisia, Türkiye, Ukraine, the United Kingdom, the United States, Uruguay, Viet Nam, European Union. For certain aspects, a subset of jurisdictions is chosen.

[9] For instance, in Croatia, Greece, Iceland, Korea, Norway and Switzerland.

[10] On 25 March 2020, the EU Commission published a Communication that provides guidance to Member States on how to achieve adequate protection of assets that are crucial for European security and public order in the context of the economic shock caused by the COVID-19 pandemic. For instance, France, Germany, Japan, Poland and Spain made permanent changes to their investment screening mechanisms in response to the new situation.

[11] Without always making explicit changes to rules and legislation, some countries announced that they would pay careful consideration to foreign acquisitions by investors controlled by or subject to influence by Russia or Belarus when implementing their investment screening mechanisms (and perhaps even more so in sectors that are currently particularly vulnerable to security risks, including the defence sector, the energy sector and dual-use technologies). Canada published a Policy Statement on 8 March 2022 in that regard and the European Commission called on all EU Member States to pay particular attention to these threats in a Communication of 6 April 2024.

[12] For instance, lists of critical and emerging technologies presenting potential security risks were made public in the United States and in the European Union.

[13] Under the Investment Safety Assessment Act, mergers and acquisitions (VIFO Act), the Netherlands introduced a screening framework that applies more stringent rules to operations resulting in direct or indirect possession or control of no less than 10% of the voting rights in companies active in a list of "highly sensitive technologies" annexed to the Decree on the scope of application of sensitive technology.

[14] Korea maintains rules under its Act on the Prevention of Divulgence and Protection of Industrial Technology which include a technology-specific mechanism to oversee foreign acquisitions of certain emerging and critical technologies. Under Executive Order 14105, the United States has established a new national security programme that prohibits certain transactions and requires notification of certain other transactions by US persons into certain entities located in or subject to the jurisdiction of a country of concern and involved in semiconductors and microelectronics, quantum information technology, and artificial intelligence.

[15] For instance, the EU-US Trade and Technology Council, which includes foreign direct investment screening as an area of co-operation, serves as a transatlantic forum for the EU and the United States to collaborate and co-ordinate different approaches on key technology issues.

[16] For example, Italy saw a thirty-fold increase of notifications related to CETs between 2014 and 2022, with only four such transactions notified in 2014, against 122 in 2022. For Italy, CETs include those categorised in its annual reports to the Italian Parliament as: defence technology; communications; aviation and aerospace; telecommunication engineering; defence industry components; 5G technologies; pharmaceuticals and biotech; laser technologies; engineering technologies; cybersecurity; drone manufacturers; robotics; and cloud computing.

[17] In Canada, the number of cases resulting in Section 25.3 orders grew from seven cases in 2016 to 33 cases in 2022. For Canada, its Annual Reports categorize its investments as: communications equipment manufacturing; architectural, engineering and related services; scientific research and development services; investigation and security services; and computer systems design and related services, some of which include CET investments.

[18] Developments in Spain are illustrative of this trend: The government recorded just one notification related to a company involved in the supply of critical inputs in 2020, but over 50 in 2023. For Spain, critical inputs include those categorised as "fundamental inputs" ("*insumos fundamentales*"). Recorded declarations and notices for the United States in critical inputs sectors as designated by the OECD's formulation more than doubled from 20 in 2019 to 49 in 2022. For the United States, the OECD identified "critical inputs" to include the following sectors in CFIUS' annual reports: oil and gas extraction; non-metallic mineral mining and quarrying; electric power generation, transmission and distribution; mining (except oil and gas); petroleum and coal products manufacturing; and other non-metallic mineral product manufacturing. In Canada, the number of cases related to metal ore mining and non-metallic mineral mining and quarrying that were subjected to increased scrutiny under the Section 25.3 orders rose from five in 2016 to 28 in 2022. Critical minerals fall into the category 'metal ore mining and non-metallic mineral mining and quarrying', but which of the recorded cases relate to critical minerals cannot be identified in the publicly available deducted from the reported case numbers.

[19] Parliament of Finland, "The Government's proposal to Parliament to amend the Act on the Monitoring of Foreign Acquisitions" (2020), p.5. Data for 2023 calculated based on Finnish Ministry of Economic Affairs and Employment "Screening of foreign corporate acquisitions in Finland – Annual report 2023", 14 June 2024.

[20] Ministère de l'Économie et des Finances, "Les chiffres clés des IEF en 2020", 24 March 2021. The share in total investment projects, not communicated by the Ministry in the context of the key figures is revealed in France Stratégie (2021), "Comité de suivi et d'évaluation de la loi PACTE-Deuxième Rapport", p.103. It is not clear how the overall annual number of FDI transactions is assessed, that is, which criteria need to be fulfilled to include a given transaction in the count of the base number of annual transactions.

[21] For France, Fiche d'impact générale on the Décret relatif aux investissements étrangers soumis à autorisation préalable (ECOT18167RD) (October 2018). Germany: Draft 1st Amendment of the Foreign Trade and Payments Act (AWG) (2020), p.3. The Government of Italy noted that the inclusion of certain communications assets under the scope of the review mechanism has contributed to increasing caseload (Relazione concernente l'attività svolta sulla base dei poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni (Anno 2019), p.18).

[22] E.g. Italy (Relazione concernente l'attività svolta sulla base dei poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni (Anno 2019), p.19).

[23] E.g. Italy, Presidenza del Consiglio dei Ministri, "Relazione sulla politica dell'informazione per la sicurezza 2020" (February 2021), p.47.

[24] Bundesministerium Digitalisierung und Wirtschaftsstandort, "Schramböck: Erste positive Bilanz nach einem Jahr Investitionskontrollgesetz und neun Monaten EU-Kooperationsmechanismus", media release, 9 August 2021.

[25] In 2022, the overwhelming majority of transactions subject to scrutiny appear to be authorised without obligations or conditions in most jurisdictions that report data on the implementation practice of their screening regimes (e.g., 98% in Germany, 92% in Italy, 86% in Spain and 98% in the United Kingdom). In some jurisdictions, the share of transactions to which obligations are attached is significantly higher (e.g., France reports a share of 44% for 2023, Direction Générale du Trésor, "Contrôle des Investissements Étrangers en France – Rapport annuel 2024"). Different designs of screening policies are likely to contribute to different outcomes, which are thus not directly comparable.

6. Building stronger defences for a digital future: The role of cybersecurity

Laurent Bernat and Lauren Crean[1]

Introduction

Protecting cybersecurity is of growing importance as digital technologies become increasingly complex and integral to critical sectors across the economy, raising the costs of their disruptions, and cyberattacks becoming more frequent. Ransomware and other cyberattacks present a growing threat, notably for public institutions, services and infrastructure. In 2021, for example, a cyberattack forced the shutdown of the largest pipeline in the United States for six days, leading to fuel shortages across the East Coast. While the number of cybersecurity incidents and their economic impact is notoriously difficult to determine, it appears to be growing. On average, a third of individuals (aged 16-74) across OECD countries reported in 2022 having experienced a security incident.[2] According to some estimates, the number of cyberattacks has almost doubled since before the COVID-19 pandemic. Since 2020, the aggregated reported direct losses from cyber incidents have amounted to almost USD 28 billion (in real terms) globally, with billions of records stolen or compromised. Total direct and indirect costs of these incidents are most likely substantially higher, with estimates ranging significantly from 1 to 10% of global GDP.[3]

Governments play an important role in cybersecurity. Companies often lack incentives to invest sufficiently in cybersecurity, and complex supply chains make it difficult to determine who is responsible. The rapid pace of technology development means that cybersecurity is a constantly moving target requiring close and continued attention. Market forces alone are insufficient to address the risks and threats. Because these are inherently global challenges, to address them effectively countries need to take coherent, co-ordinated policy action based on internationally recognised principles.

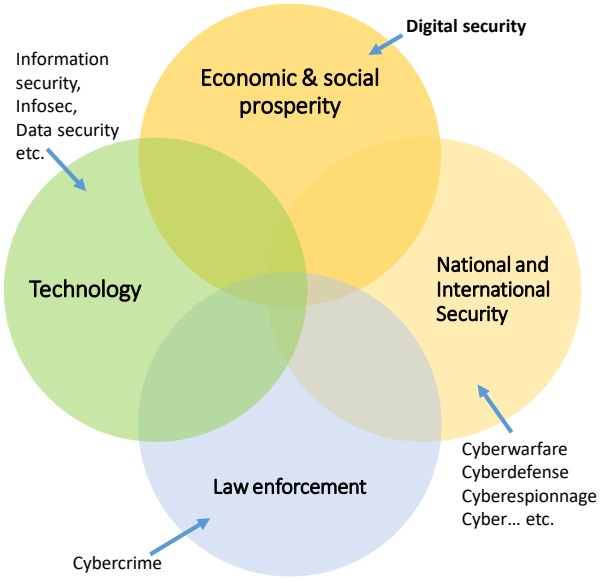
Over the last 30 years, the OECD has developed cybersecurity policies focused on economic and social prosperity. This approach is reflected in a set of Council Recommendations introduced in the *OECD Policy Framework on Digital Security: Cybersecurity for Prosperity* (OECD, 2022[1]). This chapter introduces this Framework and the related Recommendations. It also provides an overview of OECD work on the digital security of critical activities (OECD, 2019[2]; Bernat, 2021[3]) and the security of communication networks (OECD, 2023[4]).

Digital security: Economic and social dimensions of cybersecurity

The OECD defines digital security as the set of measures taken to *manage digital security risks* for economic and social prosperity (OECD, 2022[1]). As a global public policy priority, cybersecurity underpins several key areas, which often overlap and are interrelated (Figure 6.1):

- Technical operations, i.e. ensuring that information systems work as intended. This aspect, which includes human errors, represents the origins of cybersecurity, initially perceived as a technical issue managed by technical experts, commonly referred to as computer security, information security (infosec), and data security.
- Prosperity, i.e. ensuring that security supports broader economic and social objectives. This dimension shifts the focus from protecting the digital environment itself to safeguarding the economic and social activities that depend on it. The OECD refers to this as digital security or digital security risk management.
- Criminal law enforcement, i.e. enforcing cybercrime laws to reduce threats. Cybercrime can include security aspects introduced below, but also crimes such as the exploitation of children online.
- National and international security, i.e. establishing confidence-building and other measures to prevent and de-escalate the extension of armed conflicts in cyberspace. This dimension is often called cyberdefense, cyberwarfare or cyberespionage.

Figure 6.1. Economic and social aspect of cybersecurity



Source: OECD.

Governments have adopted various institutional frameworks to develop and implement policies related to each of these dimensions, leveraging different domestic agencies, with variable degrees of centralisation and co-ordination with other government bodies. At the international level, each dimension is generally addressed by different international organisations, in line with their respective mandates. For example, the OECD addresses digital security policy in line with its mandate in economic and social affairs, including science, technology and innovation policy; standards development organisations such as the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), Internet Engineering Task Force (IETF), European Telecommunications Standards Institute (ETSI), or International

Telecommunications Union ITU-T Study Group 17 develop technical standards; the Council of Europe, the United Nations Office of Drugs and Crime (UNODC) and Interpol (at a more operational level), focus on cybercrime; and the United Nations Group of Governmental Experts (GGE) and Open Ended Working Group (OEWG) address international security issues. Building on OECD expertise, the rest of this chapter focuses more specifically on digital security policy. Box 6.1 introduces the key concepts related to digital security.

Box 6.1. Digital security fundamentals

Digital security risk is the detrimental effect that digital security *incidents* can have on economic and social activities (OECD, 2020[5]; OECD, 2022[6]). In line with general risk management approaches, digital security risk is represented in terms of the *likelihood* and potential *impact* (i.e. severity) of incidents. The definition of risk in OECD digital security Recommendations is inspired by ISO/IEC risk management (ISO/IEC, 2022[7]) and information security standards.

Digital security incidents are events that disrupt the availability, integrity and/or confidentiality (*AIC triad*) of data, software, hardware and networks and, as a consequence, negatively affect economic and social activities that rely on these assets:

- Availability: assets are not accessible and usable on demand by authorised users;
- Integrity: assets have been altered in an unauthorised manner;
- Confidentiality: unauthorised entities have access to the assets.

Incidents are caused by *threats* exploiting *vulnerabilities*. Threats can be intentional (i.e. attacks) or unintentional (e.g. human errors, fires, power cuts, etc.). They include malicious actors ("threat sources") willing to exploit vulnerabilities to cause harm, and the tools and techniques ("threat vectors") they use to carry out attacks (e.g. "malware"). Malicious actors range from relatively unskilled individuals to organised criminal groups and state-sponsored actors, with considerable resources, often called Advanced Persistent Threats (APTs). State-sponsored attacks are generally pursuing geopolitical goals, while cybercriminals tend to aim for financial gains. Some actors also pursue ideological objectives (e.g. "hacktivists"). In many cases, it can be extremely difficult to accurately attribute attacks to specific individuals, groups or their sponsors, solely on the basis of their mode of operation or forensic evidence, in part because well-resourced threat actors can mimic other threat actors' modes of operation. Threats exploit *vulnerabilities* in people (e.g. lack of training and awareness), processes (e.g. no backup procedures or systematic vulnerability management) and technologies (e.g. vulnerabilities in software code).

Digital security risk focuses on *economic and social* risks resulting from digital security *incidents*. These may include financial losses, loss of opportunity, reputational damages, intellectual property theft, privacy and human safety damages. For example, when a ransomware hits a hospital and spreads across the network, some infected information systems may become unavailable and others have to be shut down to mitigate the incident (technical risk). As a result, patients being operated upon during the incident may be in danger because medical equipment may be disabled, scheduled surgeries may have to be postponed (economic and social risk), and personal data may be breached.[1]

Digital security risk management involves addressing digital security risk while maximising economic and social opportunities. Risk management is the assessment of the risk, followed by its treatment, i.e. a decision on what to do with the risk: reduce, avoid, transfer or take it (further introduced below). Risk is managed all the time. For example, in everyday life, to cross a street, people watch for cars or bicycles to *assess* the risk before deciding what to do. If it is a highway, they do not cross it to *avoid* the risk which his too high. To *reduce* risk they use pedestrian crossings, and they have an insurance policy to

transfer the risk, "just in case". If they simply cross the street without other action, they simply *accept* the risk, and will have to face the consequences. *Risk assessment is absolutely central for security*, including digital security. It marks the difference between accepting a risk after a careful and systematic evaluation and blindly accepting it without further consideration.

Digital security risk management roots security decisions in the economic and social reality of the activity at stake. It drives the selection of security measures which are appropriate to, and commensurate with, the risk and activity at stake. In so doing, it ensures that the security measures will support the economic and social activities at stake, and will not undermine them, for example, by inappropriately closing the environment or reducing functionality in a manner that would limit the possibility of taking advantage of ICTs to innovate and increase productivity. Digital security risk management prevents decisions from being made in isolation, from a separate technical or sole security point of view (security as an end in itself).

Digital security risk is a sub-category of digital risk, which itself is one among many other risks that a person or organisation may face when using digital technologies. All risks are interrelated and therefore risk management should not be approached in a silo. Other digital risks include crimes such as fraud (e.g. business email compromise) and the exploitation of children online. While there may be intersections between digital security risk and other digital risks, it is important to avoid confusion and not conflate these distinct categories, in particular when addressing digital security risk at the international level.

[1] According to a 2021 survey by the research firm Ponemon, 21% of IT and IT security professionals in healthcare delivery organisations agreed that a ransomware attack increases mortality rates (https://ponemonsullivanreport.com/2023/01/survey-ransomware-attacks-impact-patient-outcomes-at-half-of-healthcare-facilities/).

Digital security risk management

The OECD *Recommendation on Digital Security Risk Management* (OECD, 2022[6]) provides high-level principles to help develop an effective economic and social approach to cybersecurity. These principles are central to fostering a *culture of digital security* among public policymakers, as well as leaders and decision-makers in public and private organisations. They help the stakeholders to protect activities that rely on the digital environment from cyber threats, without inhibiting these activities, hindering innovation, impeding digital transformation and undermining human rights. Additionally, this protection must account for the dynamic nature of technologies, economic activities that rely on them and the threat landscape.

The general principles apply to all stakeholders, while the operational principles apply to leaders and decision-makers in organisations (Table 6.1).

Table 6.1. OECD Digital Security Risk Management Principles

General principles	
1. Digital Security Culture: Awareness, skills and empowerment	All stakeholders should create a culture of digital security based on the understanding of digital security risk and how to manage it.
2. Responsibility and liability	All stakeholders should take responsibility for the management of digital security risk based on their roles, the context and their ability to act.
3. Human rights and fundamental values	All stakeholders should manage digital security risk in a transparent manner and consistently with human rights and fundamental values.
4. Co-operation	All stakeholders should co-operate, including across borders.
Operational principles	
5. Strategy and governance	Leaders and decision-makers should ensure that digital security risk is integrated in their overall risk management strategy, and managed as a strategic risk requiring operational measures.
6. Risk assessment and treatment	Leaders and decision-makers should ensure that digital security risk is treated on the basis of continuous risk assessment.
7. Security measures	Leaders and decision-makers should ensure that security measures are appropriate to and commensurate with the risk.
8. Innovation	Leaders and decision-makers should ensure that innovation is considered.
9. Resilience, preparedness & continuity	Leaders and decision-makers should ensure that a preparedness and continuity plan based on digital security risk assessment is adopted, implemented and tested, to ensure resilience.

Note: The italicised text is a short extract from the Recommendation on Digital Security Risk Management.
Source: OECD (2022[6]), *OECD Recommendation on Digital Security Risk Management.*

General principles

A culture of digital security is essential to manage digital security risk (Principle 1). It is the mindset with which stakeholders should approach digital security, whether to develop and implement public policy, or protect their organisation, personal assets and safety, without inhibiting benefits, opportunities and human rights. A culture of digital security encompasses the understanding that such risk exists, and the need to acquire appropriate skills – through education, training, experience and/or practice – to make responsible decisions (empowerment). While the possible consequences of a car crash are intuitive, the complexity of the digital environment blurs the link between an incident and its consequences. For example, many people are aware that a virus may infect their equipment, but do not understand the potential consequences such as identity theft, financial fraud or theft of trade secrets. Consequences beyond the immediate individual implications are even less visible.

Individuals all share responsibility for their digital security decisions, or the lack thereof (Principle 2). However, the nature and levels of responsibility vary according to stakeholders' *role.* For example, the responsibility of the user of a digital device is different from the responsibility of that device's vendor, manufacturer, third-party developers of software components embedded in the device, cloud providers hosting data processed by the device, etc. Responsibility with respect to others is at the core of the OECD risk-based due diligence recommendations contained in the OECD MNE Guidelines (OECD, 2011[8]) and OECD Due Diligence Guidance for Responsible Business Conduct (OECD, 2018[9]).

Human rights and fundamental values need to be protected in the digital environment (Principle 3). Depending on how they are used, security measures can *support or undermine* human rights and fundamental values. For example, some security measures can enhance privacy protection, provide anonymity to whistle-blowers and protect human rights activists from authoritarian surveillance. They can also enable the illegitimate surveillance of citizens or employees or prevent access to activists' content.

While the global interconnectedness of the digital environment enables considerable economic and social benefits, it also increases complexity, facilitates propagation of threats and vulnerabilities, and increases shared risk. Co-operation is essential at the domestic and cross-border levels to address these drawbacks (Principle 4). Isolated stakeholders cannot successfully address digital security. For example, organisations' leaders and decision-makers need to co-operate with technical experts to assess digital security risk, and technical experts need to co-operate with leaders to ensure that technical security measures do not undermine their organisation's objectives and activities. Co-operation is also needed within and across organisations, for example to share information such as through Information Sharing and Analysis Centres (ISACs).

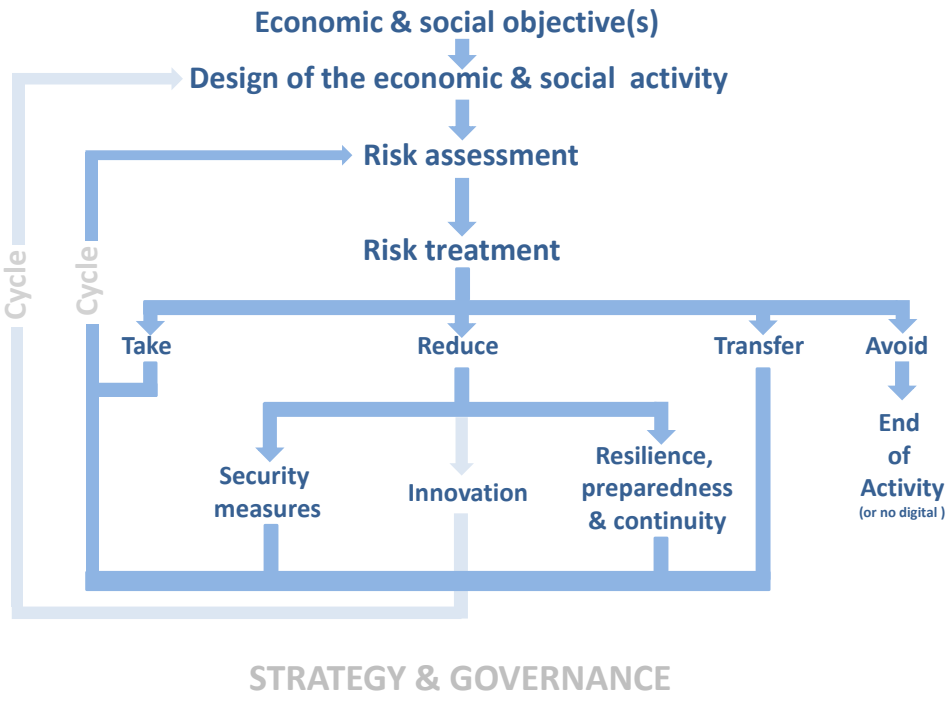
Operational principles

Operational principles focus on the implementation of digital security risk management in organisations. The first step to manage digital security risk in organisations is the adoption of a strategic approach and the establishment of appropriate governance (Principle 5). Integrating digital security risk management in the organisation's overall risk management framework (often called "enterprise risk management") is essential to ensure that digital security decisions are driven by business objectives rather than only technical considerations, and follow established risk management good practice (e.g. systematic approach, continuous improvement cycle, etc.). The corporate board of directors has a clear role in the management of digital security risk, in line with the *G20/OECD Principles for Corporate Governance* chapter on boards which underlines that a key function of the board is to set risk management policies and to ensure "the integrity of the corporation's accounting and financial reporting systems, including […] that appropriate systems of control are in place, in particular, systems for risk management […]" (Principle VI.D.7) (OECD, 2015[10]).

Digital security governance should set clear roles, responsibilities and processes, and ensure that appropriate resources and competencies are available. *Leaders and decision-makers responsible for achieving economic and social objectives should be responsible for digital security risk to these activities* ("risk ownership"). Risks and benefits are inherently related, because by definition risks affect benefits of an activity. As managing risk is a means to increase an activity's likelihood of success, leaders and decision-makers in an organisation who are responsible for an activity's benefits should also be responsible for addressing the digital security risk to that activity and not simply delegate it to technical experts because: *the economic and social consequences of incidents can be much more severe than their technical (i.e. ICT) impact* for the organisation, its partners and third parties. In addition, s*ecurity measures can undermine the activity they aim to protect*. They can create barriers and constraints for this activity, such as increased financial cost, system complexity and time to market, reduced performance, usability, capacity to evolve, innovation, and user convenience.

To increase the likelihood of success, a risk assessment and treatment cycle (Principle 6) addresses such uncertainties. As shown in Figure 6.2, it starts with the definition of the objectives and design of the activities that rely on the digital environment. The risk is then *assessed* to evaluate the probability and possible effects of uncertainties on the objectives of the activity. On the basis of this assessment process, a decision is made on what to do with the risk (risk *treatment*), i.e. whether and how the risk should be modified to increase the likelihood of the success of the activities to support and preserve the objectives.

Figure 6.2. Overview of the digital security risk management cycle



Source: OECD.

The risk treatment process determines which part of the risk should be:

- Taken (i.e. accepted), because the risk is within the bounds that are deemed acceptable by the entity carrying out the activity, also known as its “risk appetite” or “risk tolerance”. Taking the risk means accepting the potential detrimental economic and social consequences of incidents.
- Avoided, knowing that it is not possible to eliminate the digital security risk entirely without at the same time giving up the benefits of using ICTs. In other words, the best way to avoid digital security risk is to not use digital technologies.
- Reduced to the acceptable level according to the entity’s risk appetite, by establishing security measures that reduce the occurrence or impact of incidents. Because some detrimental events can always happen despite security measures in place, there will always be some residual risk that cannot be eliminated and must be accepted. Therefore, it is essential to create resilience and ensure business continuity, to be prepared for incidents and ready to reduce their consequences.
- Transferred to a third-party, for example through insurance, if there is an insurance market.

Continuous, systematic and cyclical risk assessment is essential for leaders and decision-makers to make informed risk treatment decisions that are tailored to constantly changing risk. Threats, vulnerabilities, incidents, technologies, their uses, and their benefits – to name a few variables in the risk equation of an

activity – are extremely dynamic. The risk assessment needs to take into account risk related to suppliers, and partners with whom the organisation is digitally connected. The possible risk treatment decisions (take, reduce, transfer, avoid) require that leaders and decision-makers set their organisation's digital security level of risk appetite (or tolerance) for each activity that relies on the digital environment.

To reduce the risk, security measures can then be selected and operated (Principle 7). Security measures, also called "mechanisms", "controls", or "safeguards", can be of different natures: digital (e.g. security software), physical (e.g. locks, cameras, fences) or mixed (e.g. smart card); related to people (e.g. training), processes (e.g. organisational rule or practice) or technologies (e.g. cryptography), legal (e.g. contract), procedural (e.g. standards), managerial, etc. Security measures may also address vulnerabilities.

In addition to adopting security measures, stakeholders can reduce their exposure to digital security risk by innovating with respect to the activity, as well as the security measures (Principle 8). Innovation to reduce digital security risk can take many forms, which may or may not be related to digital aspects. For example, innovation may relate to the organisation's economic or business model, to processes such as payment methods, or even to redesigning physical, legal, or other non-digital components of a product. As introducing innovation can create uncertainties in an activity, it should trigger a reassessment and treatment cycle, as shown in Figure 6.2. Thus, digital security can add value to an organisation, product or service, and become a driver for innovation, a stimulus for competitive advantage, provided that it is approached as an integral part of the economic and social decision-making processes related to an activity rather than as an isolated and only technical issue.

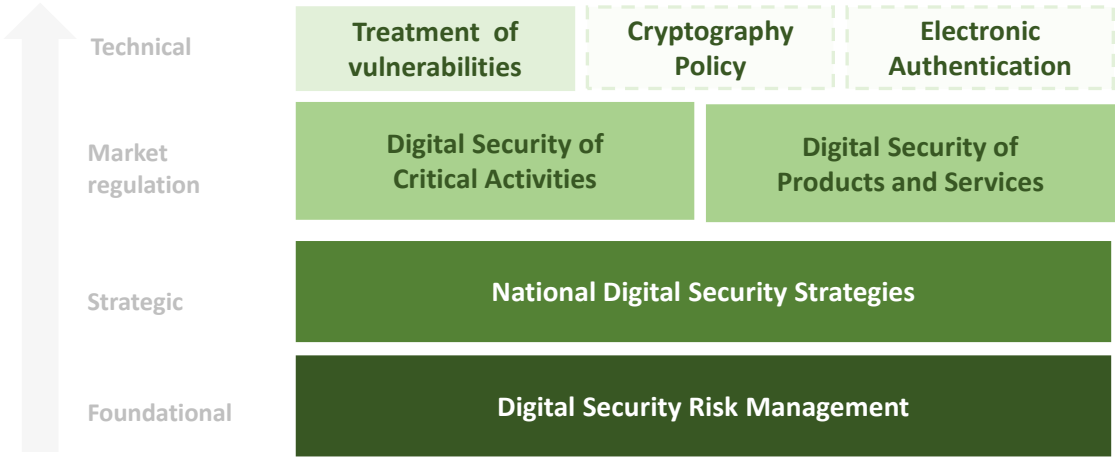
To further reduce risk, resilience, preparedness and continuity measures can be defined in order to be applied when an incident occurs (Principle 9). In addition to security measures and innovation, which aim to prevent the occurrence of harmful incidents, resilience, preparedness, and continuity measures aim to *mitigate economic and social consequences when incidents do occur*. Preparedness and continuity plans are essential to define in advance how to protect, detect, respond, and recover from incidents. Such plans should take into account the extremely rapid pace with which incidents can propagate and escalate in the digital environment.

Digital security public policy

While addressed under different labels, such as information security, data security, IT security, computer security or information assurance, cybersecurity has been a public policy issue for more than 35 years, and even more if one considers the security requirements embedded in privacy and data protection legislations adopted as far back as the 1970s in some countries. However, it is only with the wide adoption of Internet technologies and the broad availability of broadband connectivity that cybersecurity progressively became a standalone policy area with dedicated governance structures, strategies, plans as well as policy initiatives.

Digital security has progressively grown in this context. Today, the OECD maintains a total of seven Council Recommendations which reflect the consensus among OECD countries on how to approach cybersecurity from the economic and social perspective and a commitment to develop policies on that basis. They are introduced in the OECD *Policy Framework on Digital Security: Cybersecurity for Prosperity* (hereafter the Framework) (OECD, 2022[1]), represented in Figure 6.3. This set of Recommendations addresses the most important aspects of digital security policy, without addressing all facets of this complex and constantly evolving area.

Figure 6.3. Overview of the Framework



Source: OECD.

The *Foundational* layer is the basis of digital security policy making upon which all the other layers rely, namely digital security risk management. It includes the fundamental principles to bear in mind to approach cybersecurity from the economic and social perspective, and to establish a *culture of digital security to protect activities, people and the society without inhibiting benefits, opportunities, and human rights*. All the other layers of this Framework are based upon these high-level principles. This layer consists of the Recommendation on Digital Security Risk Management (OECD, 2022[6]).

The *Strategic* layer focuses on how policymakers should use the foundation to develop national digital security strategies ("national strategies") that provide a clear vision to ensure that all stakeholders, from government agencies to public and private sector organisations and individuals, join forces in a coherent and consistent manner. In addition to enabling a holistic and whole-of-government approach for digital security policy, national strategies facilitate the creation of interfaces and synergies with other policy areas, such as digital economy policy, privacy and data protection, sectoral policies (e.g. finance, energy, education, skills) and international co-operation. The strategic layer is reflected in the OECD Recommendation on National Digital Security Strategies (OECD, 2022[11]).

National strategies should articulate a clear vision of the country's objectives with respect to digital security. They should aim to create a culture of digital security and protect individuals as well as public and private organisations from digital security threats while taking into account the need to safeguard national and international security and to preserve human rights and fundamental values. In addition to digital security, a national strategy may address several other dimensions of cybersecurity, such as those introduced in Figure 6.1., which are beyond the mandate of the OECD.

The national strategy needs to assign clear responsibilities to one or more existing or new government bodies for the development and implementation of digital security policies called for by the strategy. The OECD recommends that national strategies address at least nine areas, starting with awareness raising, the establishment of incident response capacity (generally through one or more Computer Security Incident Response Teams (CSIRT) or Computer Emergency Response Teams (CERT)), as well as the promotion of risk management standards. Other areas include the development and retention of a skilled workforce, the establishment of vulnerability co-ordination mechanisms to support co-ordinated vulnerability disclosure, the development of a cybersecurity industry, as well as initiatives to encourage research and innovation (OECD, 2020[12]), and the protection of individuals and SMEs (OECD, 2021[13]). Last, but not least, international co-operation should be an important component of national strategies, for sharing

experience and good practices, providing and benefiting from mutual assistance, improving incident response at operational level and developing comparable risk metrics.

The *Market regulation* layer addresses areas where policy intervention is needed because market forces are insufficient to create an optimal level of digital security. While many markets may require policy intervention to enhance digital security across society, so far OECD Recommendations have primarily focused on the following two areas:

- The digital security of critical activities such as financial, health or energy services, the disruption or destruction of which would affect the functioning of the economy and society, human lives, as well as national security. This policy area is further detailed in the next section and supported by the OECD Recommendation on the Digital Security of Critical Activities (OECD, 2019[2]).
- The digital security of the products that contain (computer) code and associated services (e.g. cloud) on which stakeholders' depend to carry out their economic and social activities. OECD work has shown that market forces alone are often insufficient to ensure that such products and services are adequately secure, and that market incentives on their own are unlikely to fix gaps in the digital security of these products and services. The OECD Recommendation on the Digital Security of Products and Services provides guidance in this area (OECD, 2022[14]).

Because market forces alone do not allow for some stakeholders to optimally address digital security, public policies are needed to encourage them to strengthen digital security. In an ideal world, market forces would ensure that products that include code (software, IoT devices, etc.) and related services are sufficiently secure, and that their security measures are proportionate to the risk faced by their users, hence increasing the marginal cost of cyberattacks for malicious actors and discouraging their efforts. However, OECD analysis shows a market failure often prevents stakeholders from optimally valuing the digital security of products and services, and that market incentives on their own are unlikely to fix gaps in digital security risk management (OECD, 2021[15]; OECD, 2021[16]; OECD, 2021[17]). To realign market incentives, digital security policy measures can aim to ensure that suppliers take responsibility for the digital security of their products and services throughout their products and services' lifecycle. This could be broken down into action lines, whereby suppliers adopt *security by design and security by default*, treat and co-ordinate vulnerabilities, adopt responsible end-of-support policies, and co-operate across the supply chain's code owners. Policies can also reduce information asymmetries to *increase transparency and foster information sharing* about the digital security of products and services for example through third-party evaluation such as audits, inspection tests and certification.

The *Technical layer* focuses on more technical aspects that require policy guidance. It includes the need to encourage stakeholders to co-ordinate the disclosure of security vulnerabilities in products, better manage vulnerabilities in information systems, and protect vulnerability researchers, an area covered by the OECD Recommendation on the Treatment of Digital Security Vulnerabilities (OECD, 2022[18]). It also includes Cryptography policy, addressed in the OECD Recommendation concerning Guidelines for Cryptography Policy ("Cryptography Policy Guidelines") (OECD, 1997[19]) and electronic authentication, addressed in the OECD Recommendation on Electronic Authentication (OECD, 2007[20]).

Vulnerabilities are a major source of digital security risk because code is never perfect, and almost always has vulnerabilities, and the same is true for information systems. Vulnerabilities are a by-product of the increasing complexity of code and systems, combined with weak digital security practices among suppliers and users. While it is not possible to completely eradicate vulnerabilities from all code and systems, improving their treatment is a major opportunity to reduce digital security risk and increase trust in the digital transformation era. Addressing these vulnerabilities before attackers take advantage of them is an effective means to reduce the probability of incidents. To reduce security risk, stakeholders should treat vulnerabilities, each according to their role. Developers should look and test for vulnerabilities in their code, develop mitigations to fix them (e.g. "patches", "security updates"), and distribute them to other actors across the value chain towards end-users. Organisations should monitor their information systems to

ensure that these mitigations are appropriately applied and avoid product misconfigurations. Vulnerability treatment refers to the overarching process encompassing the discovery of a vulnerability, how the vulnerability is handled by suppliers ("code owners"), managed by system owners, and publicly disclosed. Over the last few years, the technical community has made progress in developing good practice for treating vulnerabilities, including through co-ordinated vulnerability disclosure (CVD).

However, significant economic and social challenges prevent stakeholders from adopting good practice. For example, software developers and system owners are often insufficiently aware that it is their joint responsibility to address vulnerabilities. They may lack resources and skills, and misaligned market incentives may disincentivise them to act. Software developers and system owners can ignore vulnerability researchers and may even threaten them with legal proceedings. Vulnerability researchers discover and report vulnerabilities to the software developers and system owners who can mitigate them, thereby reducing cost and users' "window of exposure" to digital security risk. When ignored or threatened, vulnerability researchers may be tempted to disclose the vulnerability information publicly without co-ordinating with other stakeholders, which may create risk for all users and the economy. There is also a risk that bad actors may turn to the black market to monetise vulnerability information, thereby feeding the criminal ecosystem.

The OECD Recommendation on the Treatment of Digital Security Vulnerabilities covers five areas for policy action: *Clarifying responsibilities* for each category of stakeholders; *encouraging responsible vulnerability researchers* and c*reating safe harbours to* protect them against threats of legal proceedings from vulnerability owners; f*ostering trust*, by ensuring that stakeholders have access to at least one trusted co-ordinator to assist in resolving issues between them; m*ainstreaming good practice*; *Intensifying domestic and international co-operation*, for example to reduce the grey market for vulnerabilities, share good practice across borders and ensure the cross-border interoperability of legal frameworks to protect vulnerability researchers (OECD, 2022[18]). An additional OECD document provides Good Practice Guidance on the Co-ordination of Digital Security Vulnerabilities Guidance to give policymakers an overarching understanding of the co-ordination of digital security vulnerabilities in practice, while avoiding technical jargon and detailed considerations (OECD, 2022[21]).

The digital security of critical activities

The digital transformation of critical activities such as the delivery of water, energy, healthcare, communications, and banking services increasingly exposes them to cybersecurity threats, which can affect the health, safety, and security of citizens, the functioning of essential services, or economic and social prosperity more broadly. This section builds upon the OECD Recommendation on the Digital Security of Critical Activities (OECD, 2019[2]), as well as the Going Digital Toolkit note on the same subject (Bernat, 2021[3]). It introduces key concepts, such as critical activities, critical information infrastructure (CII), cybersecurity and digital security risk management, and helps policymakers identify what needs to be protected and what types of measures operators of critical activities should take. It further discusses the institutional framework to develop and supervise policies to enhance the digital security of critical activities, including trust-based partnerships.

What is a critical activity?

A critical activity is an economic and social activity, the interruption or disruption of which would have serious consequences on the health, safety, and security of citizens; or the effective functioning of services essential to the economy and society, and of the government; or economic and social prosperity more broadly (OECD, 2019[2]). The latter type of critical activities includes those that are essential for prosperity without being necessarily critical to the functioning of the economy and society, nor affecting the health, safety and security of citizens. For example, car manufacturing or mining, in a country where such activities

would represent a significant share of the GDP. Countries use different terminology to refer to critical activities, such as “critical functions” (CISA, 2024[22]) or “essential services” (European Union, 2022[23]). The notion of critical activity (sometimes called critical functions or essential services) is different from that of critical infrastructure because it focuses on the risk to the delivery of the service rather than to the assets on which the delivery of the service relies.

The notion of critical infrastructure emerged in the late 1990s, as some OECD countries started to adopt critical infrastructure protection policies. These policies typically considered critical infrastructure sectors such as energy, finance, communications or public health.

Progressively, the need to develop policies to protect information systems and networks that support such critical infrastructure sectors became increasingly clear. Around 2008, it seemed natural to call these ICT assets “critical information infrastructure” (CII), as if they formed an additional critical infrastructure sector. However, although quite popular among experts, the concept of CII has rarely been used to develop domestic policy frameworks. This may be due to the difficulty to delineate CII in practice. For example, the Internet can be considered as being part of the CII because most operators of other critical infrastructures rely on it, such as banks, hospitals and energy distributors. However, these operators also rely on their internal critical information systems and networks, which therefore are also part of the CII. Some parts of these information systems and networks may be internal to the operators of critical infrastructure, i.e. “on-premises”, but others may be “in the cloud”, i.e. on the Internet, and owned and managed by third parties, potentially in other jurisdictions. This combination of shared and isolated, as well as internal and external technical components makes CII difficult to represent and more complex than the more traditional “critical infrastructure” sectors upon which the CII concept was inspired.

In 2019, the OECD agreed to simplify the framework established in its 2008 Recommendation on the protection of critical information infrastructure (OECD, 2008[24]) by focusing on the need to enhance the digital security of critical activities, i.e. encourage operators of critical activities to better manage digital security risk.

From the perspective of the OECD, the overarching challenge for enhancing the digital security of critical activities is to develop policies that encourage, and in some countries require, operators of critical activities to strengthen digital security, without creating unnecessary burdens that would inhibit or reduce their ability to realise the full potential of digital transformation. Such policies need to be consistent with the OECD digital security risk management principles, including with regards to human rights and fundamental values.

Policies to enhance the digital security of critical activities aim primarily at encouraging public and private operators of these activities, such as banks, hospitals, water and energy distributors, communication network providers, airports, rail companies, etc., to better manage digital security risk. Targeting too many operators that are not truly vital to the delivery of the critical activities at stake would impose unnecessary burdens on large parts of the economy. Targeting too few would not sufficiently protect the economy. Therefore, governments need a process to identify which operators should be targeted by their policies.

To determine which operators the policy should target, governments can build upon an existing critical infrastructure protection or national risk management framework to protect their critical infrastructure. In the lack of such a framework, they have to develop a methodology from scratch. The first step is the development of a national risk assessment covering all economic and social activities. On the basis of this assessment, and working with relevant public and private actors, the government identifies critical activities and the operators of these critical activities. Different countries have different methodologies to do so, taking into account different thresholds or criteria of criticality (e.g. possible number of users or citizens impacted by an incident). For example, the European Union Network and Information Security 2 (NIS 2) Directive considers important and essential entities, with criteria such as their sector, size and turnover (European Union, 2022[23]).

Overarching principles in regulating operators of critical activities to strengthen digital security

While operators are responsible for the digital security of their activities, governments – in their role to protect the public interest – are expected to intervene, including to determine the level of risk that the society can tolerate with respect to critical activities, and to ensure the continuity of these activities.

The nature of governments' intervention takes many forms and uses many tools including standards' promotion, legal obligations, regulation, co-regulation, encouragement of self-regulation, crisis management assistance and technical support, among others. There has been a recent trend towards the adoption of mandatory regulation, largely driven by the implementation of the 2016 NIS Directive in the European Union, according to which EU members had to create compliance requirements for operators of essential services, and reinforced by the 2022 NIS 2 Directive which extends the goals and scope of the previous Directive to strengthen protection (European Union, 2022[23]). In contrast, some countries such as Japan and the United States favour a voluntary approach, whereby they provide support and guidance to operators without establishing mandatory requirements.

Overall, governments share common objectives with respect to the types of measures that operators should take, such as adopting enhanced digital security risk management and sharing risk-related and/or best practice information, and/or reporting incidents.

As it is not possible to protect everything at the same level, the designated operators of critical activities need to identify the functions without which they could not effectively carry out their critical activities, as well as the critical parts of the digital ecosystem supporting these critical functions. Digital ecosystems include hardware, software, networks and data, operational technologies that detect or cause changes in physical processes (such as industrial control systems), as well as the internal and external entities, persons, and processes that design, maintain and operate them, and the relationships between them. Lastly, operators need to systematically and cyclically manage digital security risk related to these critical functions. They conduct a digital security risk assessment, and make a business decision to treat digital security risk.

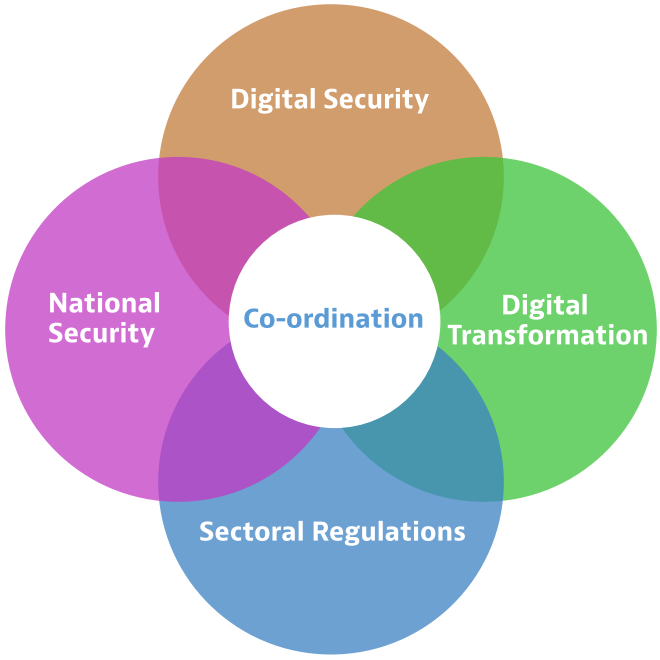
A key challenge for government intervention is to formulate recommendations or requirements to implement state-of-the-art digital security risk management at the appropriate level of detail. Digital technologies are dynamic, and so are threats, vulnerabilities, as well as techniques and processes to protect digital ecosystems. If policy measures are too detailed, public policies aiming to incentivise operators to take more robust security measures may be quickly outdated and become an inhibiting factor for operators, without providing the expected level of security. If they are too generic, operators may face regulatory uncertainty if they experience difficulties in interpreting policies for implementation and compliance purposes.

In the United States, for example, the government promotes the Cybersecurity Framework developed by the National Institute of Standards and Technologies (NIST) in co-operation with the industry (NIST, 2024[25]). The Cybersecurity Framework is voluntary guidance based on existing standards, guidelines, and practices. This Framework is widely recognised as a useful tool, including beyond the United States and beyond operators of critical activities. In Japan, the National Center of Incident readiness and Strategy for Cybersecurity (NISC) provides guidance through the Cybersecurity Policy for Critical Infrastructure Protection which includes Guideline for Establishing Safety Principles for Ensuring Information Security of Critical Infrastructure. In March 2021, the Korea Internet & Security Agency (KISA) issued "Technical Vulnerability Analysis and Assessment Guidelines for Critical Information Infrastructure" in order to strengthen the cybersecurity capacity of critical infrastructure operators.

The OECD Recommendation on digital security of critical activities represents the consensus among OECD members regarding the high-level set of risk management measures that operators should be recommended to adopt (OECD, 2019[2]).

Policies to enhance the digital security of critical activities are at the crossroad of several areas (Figure 6.4). They aim to support digital transformation by ensuring trust in activities that are essential to the functioning and prosperity of our economies and societies. Therefore, they are part of a national *digital transformation policy* agenda, as well as national *digital security* agenda. As explained above, policies to enhance the digital security of critical activities can build upon the national risk assessment resulting from the country's critical infrastructure protection framework, which is often part of a *national security and public safety* agenda. In addition, they also span across different sectors such as finance, energy, communications, transports and health care, with specific technical, market, economic, regulatory, cultural and other characteristics. Therefore, these policies can also be viewed as part of several *sectoral* agendas (e.g. smart cities, smart grid, smart health, etc.) and have to take into account sectoral regulations and market conditions. The United States 2024 Executive Order 14117 on "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern" and the related data security rule, which restrict the transfer of bulk sensitive personal data to countries of concern, protects US national security while addressing the intersecting demands of privacy and cybersecurity and avoiding broad data localisation mandates (US Department of Justice, 2025[26]).

Figure 6.4. Co-ordination to enhance the digital security of critical activities



Source: OECD.

It is generally a significant challenge for governments to take into account these different perspectives in a balanced manner. Three elements are required: 1) adopting at the highest level of government, and as part of a national digital security strategy, clear objectives to strengthen digital security and resilience of critical activities, 2) adopting a domestic governance mechanism that allocates responsibility to one or more government bodies to enhance the digital security of critical activities within and across sectors, and 3) ensuring a whole-of-government domestic co-ordination to establish intra-governmental co-operation, ensure consistency of the measures adopted across sectors, allocate resources across responsible government bodies and create a critical mass of expertise and skills, and facilitate cross-border co-operation.

Governance framework for digital security of critical activities in OECD counties

There is no one-size-fits-all approach to a whole-of-government co-ordination in OECD countries. Governance frameworks vary significantly, according in part to a country's constitution, style of government, and administrative structure. In all cases, governance frameworks need to ensure consistency with human rights and fundamental values.

The governance relates generally to three key functions: 1*)* the definition of the overarching policy framework or strategy, 2*)* the implementation of the framework in each sector and 3*)* the operational capacity. The three functions can be centralised in a single body as in France (the National Agency for the Security of Information Systems, ANSSI), or distributed in different ways.

For example, the strategy development can be led by a department or ministry (e.g. Germany, the United Kingdom, Japan), and the operational capacity can be located in a separate agency (e.g. NCSC in the United Kingdom, the Federal Office for Information Security (BSI) in Germany, NISC in Japan). The implementation of the framework and supervision can be centralised or decentralised through sectoral regulators. In Denmark, the overarching policy framework was developed by the Ministry of Finance as part of the national digital security strategy, but each ministry responsible for a critical sector (energy, healthcare, transports, etc.) is required to develop a specific sub-strategy in its area of competence (Danish Ministry of Finance, 2018[27]). In Türkiye, cybersecurity strategies are developed by the Cyber Security Board, under the Ministry of Transport and Infrastructure. The relevant authorities regulating critical infrastructure sectors, if any, or the relevant ministries, are responsible for implementing the macro-level measures in the Board's cybersecurity action plans. In many countries, the body in charge of operational digital security assistance can liaise with law enforcement and intelligence bodies.

Each approach has pros and cons. For example, a centralised approach facilitates regulatory consistency but makes detailed sector-specific regulation more difficult, requiring the central body to consult relevant sectoral regulators and create links with private operators of critical activities. A decentralised approach facilitates the development and implementation of sector-specific regulation while requiring more efforts to ensure consistency across sectors and provide the government with a holistic understanding of the situation. A key advantage of the decentralised approach is that sectoral regulators already have relationships with operators in their sectors and understand their constraints. However, operators may be reluctant to disclose digital security-related information to sectoral regulators which might be used for other regulatory purposes (European Commission, 2019[28]).

An important aspect is the need to ensure that the responsible body (or bodies) has (or have) sufficient capacity to accomplish its (their) tasks, including funding and resources as well as digital security expertise, which is scarce in most countries and difficult to retain in the public sector. It may seem easier to aggregate a critical mass of digital security expertise through a central body, as the bulk of technical digital security challenges is common to all sectors.

Governments can address this issue by separating the policy from the operational expertise. For example, in the United Kingdom, the NCSC supports sectoral regulators by offering technical advice and Computer Security Incident Response Team (CSIRT) services. A central body can also issue guidance and guidelines to help sectoral agencies carry out their mission, as in Japan and the United Kingdom (DCMS, 2018[29]; Government of Japan, 2024[30]). In reality, most countries follow a relatively hybrid model. Countries with a centralised approach compensate centralisation through intra-governmental consultations and co-operation, and countries with a decentralised model generally maintain a central operational body to support sectoral regulators and ensure holistic situational awareness.

As part of this overarching framework, governments should build capacity to support digital security risk management and resilience of critical activities. This includes developing a new or strengthening an existing incident response capability through a computer security incident response team (CERTs/CSIRTs) or Security Operation Centre (SOCs), or several of them operating for example by sector. While

governments need to have at least one CERT/CSIRT to address incidents in their own systems, other CERTs/CSIRTs are not necessarily public sector bodies. Governments also often take a leadership role to organise sector and cross-sector cybersecurity exercises or drills with operators to test and improve existing measures, including information flows between stakeholders during crises. Such exercises can involve partners across borders at regional (e.g. Cyber Europe organised by ENISA) and international levels (e.g. US-led Cyberstorm organised by CISA) (ENISA, 2024[31]; CISA, 2024[32]).

The security of communication networks

In 2023, the OECD analysed the security of communication infrastructure (OECD, 2023[4]) in light of recent development such as the generalisation of digital transformation and how it affects communication operators. Given the crucial role of communication networks to digital transformation, their digital security and resilience have become a priority for policy makers across the OECD to ensure the functioning of our digitally dependent economies and societies and to strengthen trust in the ongoing digital transformation. However, cyberattacks on these networks are on the rise and increasingly sophisticated. At the same time, communication networks are undergoing significant changes and are being upgraded to new technological standards (e.g. 5G), which, in turn, impact their security.

The report finds four trends that are changing communication networks and the digital security implications these raise (OECD, 2023[4]):

- The increasing criticality of and reliance on communication networks by the economy and society, which is changing the context of digital security of communication networks.
- An increased virtualisation of networks and a greater use of cloud services.
- A shift towards more openness in networks, including for the Radio Access Network (RAN).
- The role of artificial intelligence in communication networks.

Each of these trends is shaping communication networks and, therefore, prompts questions on their implications on digital security.

On the one hand, these trends benefit digital security risk management of communication infrastructure. They can help improve network visibility and management, enable network segmentation and isolation, allocate security resources more effectively, and automate the early detection of malware and malicious activity (OECD, 2023[4]). Increased transparency and reduced dependencies on certain suppliers are additional possible benefits to digital security, driven by the shift towards more openness.

On the other hand, these trends also challenge digital security risk management in communication infrastructure. Overall, the report finds that they result in:

- An expanding attack surface (i.e. the set of points of an information system which are potentially vulnerable to an attack). Since the architecture of communication networks is increasingly complex, and because networks are increasingly software-defined, cloud-based and virtualised, they contain more software vulnerabilities that can be exploited (OECD, 2023[4]).
- A broader and more complex supply chain. Some of the technological advancements outlined in the trends tend to increase the dependency of network operators on some of their suppliers and to redistribute control and responsibility for the management of digital security risk along the entire value chain. These suppliers include providers of communication equipment, as well as providers of cloud and managed services, which are likely to play an increasingly important role in the digital security of communication networks. The communication infrastructure supply chain is often complex, which makes the allocation of responsibility in case of a digital security incident even more difficult.
- An aggravating threat landscape, driven in part by the commoditisation of attacks (e.g., “ransomware-as-a-service”) and the increasing sophistication of state-sponsored and other threat

actors. Against this backdrop, malicious actors' motivation to breach communication networks' availability, integrity or confidentiality is significantly increasing as communication networks become increasingly critical (OECD, 2023[4]).

The paradox facing governments is that while communication networks are increasingly considered critical infrastructure, their digital security ultimately depends upon decisions made by third parties, namely network operators and their suppliers. Nevertheless, governments do have a clear role to play to incentivise the adoption of digital security best practices and to support an enabling environment that empowers stakeholders to reach an optimal level of digital security (OECD, 2023[4]). This can be fostered through the following policy objectives that can help structure public policy interventions to improve the digital security of communication infrastructure (OECD, 2023[4]):

- First, adopting a holistic and strategic approach towards enhancing the digital security of communication infrastructure**,** which i) considers the entire lifecycle of products and services on which operators rely, ii) gathers all relevant stakeholders and iii) is co-ordinated across the whole government and at the international level. Importantly, co-ordination across governmental agencies and a clear definition of responsibility and/or mandates between them are essential.
- Second**,** incentivising network operators to enhance digital security and adopt comprehensive risk management frameworks (i.e., risk assessment and risk treatment) and encouraging them to explore more advanced security approaches, such as the "zero trust" model.
- Third, addressing supply chain digital security risk by incentivising suppliers to improve supply chain transparency (e.g. through enhanced traceability of components and digital security certification) and supporting supply chain diversification.

To complement these policy objectives, governments can apply several policy actions to address the cross-cutting challenges and uphold policy objectives, ranging from light-touch to more interventionist approaches**:** voluntary frameworks and guidance, multistakeholder initiatives and funding research, third-party evaluation and certification, public procurement, and legal requirements (OECD, 2023[4]). These actions can be shaped as needed to carefully address the cross-cutting challenges in terms of scope, scale and speed of cyberattacks. OECD countries have introduced policy initiatives spanning these policy actions, from voluntary frameworks to legal requirements on digital security. However, digital security is an ever-moving target that requires constant re-evaluation, both regarding the best practices available for private stakeholders to implement as well as the structure and objective of public policies to create the enabling environment to incentivise the adoption of best practices by private stakeholders (OECD, 2023[4]).

Conclusions

This chapter discussed how the OECD approaches digital security from the economic and social perspectives. It explained the main differences between digital security and the other dimensions of cybersecurity and presented digital security risk management. After a brief overview of areas of policy action related to digital security, the chapter detailed the OECD approach to strengthening the digital security of critical activities, an area at the intersection of economic and national security policy making, including with a focus on the security of the communication infrastructure.

As this chapter illustrates, OECD has a range of tools to assist governments in advancing digital security. The *Policy Framework on Digital Security: Cybersecurity for Prosperity* presents the OECD approach to digital security as reflected in the seven Recommendations adopted by the OECD Council to guide governments in their efforts to strengthen digital resilience and build robust trust foundations for our digital future. The Framework covers the Recommendations on:

- Digital Security Risk Management (OECD, 2022[6])
- National Digital Security Strategies (OECD, 2022[11])

- The Digital Security of Critical Activities (OECD, 2019[2])
- The Digital Security of Products and Services (OECD, 2022[14])
- The Treatment of Digital Security Vulnerabilities (OECD, 2022[18])
- Cryptography Policy (OECD, 2007[20])
- Electronic Authentication (OECD, 1997[19]).

In addition to Recommendations and guidance documents, the OECD has been analysing other aspects of digital security, such as the security of the domain name system (DNS) (OECD, 2022[33]) and routing security (OECD, 2022[34]). The OECD Global Forum on Digital Security for Prosperity (GFDSP) also provides an international multilateral setting for all stakeholder communities of experts to dialogue, share experiences and influence public policy making on digital security. The GFDSP holds thematic events every year. Outputs from these discussions influence international public policy discussions and can lead to the development of analytical work, principles and international policy recommendations, both at the OECD and in other international fora. The GFDSP discussed issues such as open source and zero trust in 2024, the Internet of Things in 2023, and digital security innovation in 2019 (OECD, 2024[35]).

As the implications of digital security on the economy and society become more pronounced, and as the pace of technology development accelerates, the OECD will maintain a key focus on this critical area of economic security and continue supporting governments and stakeholders, notably through:

- Identifying and analysing policy implications to digital security of frontier issues such as quantum computing and generative AI. Quantum information technologies, in particular, are expected to have a disruptive impact on digital security in that they would make some of today's widely-used encryption methods less secure, but at the same time could boost the development of new, more resistant defences (OECD, 2024[36]).
- Supporting the implementation of the OECD Policy Framework on Digital Security: Cybersecurity for Prosperity (OECD, 2022[1]), including through consideration and analysis of the role of labels and certification schemes as complementary policy measures; of vulnerabilities related to the systemic risks to global supply chains represented by Managed Service Providers (MSPs) (OECD, 2024[36]); and of measures to bridge the skills gap for digital security.
- Building on the OECD's work on measuring cybersecurity posture and performance across countries (OECD, 2024[37]), work to measure cybersecurity uncertainty can complement existing statistics and help anticipate emerging cybersecurity trends, develop more targeted cybersecurity awareness programmes, and promote a more secure and resilient digital ecosystem. Efforts to measure cybersecurity innovation can also support a more robust evidence base for designing and implementing digital security policies.

This work will aim to keep policymakers ahead of new developments in the evolving area of digital security and build stronger defences for the digital future.

References

Bernat, L. (2021), "Enhancing the digital security of critical activities", *Going Digital Toolkit Note, No. 17*, https://goingdigital.oecd.org/data/notes/No17_ToolkitNote_DigitalSecurity.pdf. [3]

CISA (2024), *Cyber Storm : Securing Cyber Space*, https://www.cisa.gov/cyber-storm-securing-cyber-space. [32]

CISA (2024), *National Critical Functions*, https://www.cisa.gov/topics/risk-management/national-critical-functions. [22]

Danish Ministry of Finance (2018), *Danish Cyber and Information Security Strategy*, https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf. [27]

DCMS (2018), *NIS Regulations: Guidance for Competent Authorities*, https://www.gov.uk/government/publications/nis-regulations-guidance-for-competent-authorities. [29]

ENISA (2024), *Cyber Europe*, https://www.enisa.europa.eu/topics/training-and-exercises/cyber-exercises/cyber-europe-programme. [31]

European Commission (2019), *Report from the Commission assessing the consistency of the approaches taken by Member States in the identification of operators of essential services*, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52019DC0546&from=EN. [28]

European Union (2022), *Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union*, http://data.europa.eu/eli/dir/2022/2555/oj. [23]

Government of Japan (2024), *The Cybersecurity Policy for Critical Infrastructure Protection (4th Edition)*, https://www.nisc.go.jp/eng/pdf/cip_policy_2024_eng.pdf. [30]

ISO/IEC (2022), *ISO 31073:2022(en) - Risk management — Vocabulary*, https://www.iso.org/obp/ui/#iso:std:iso:31073:ed-1:v1:en. [7]

NIST (2024), *NIST Cybersecurity Framework 2.0*, https://www.nist.gov/cyberframework. [25]

OECD (2024), *Digital Economy Outlook: Volume 2*, https://doi.org/10.1787/3adf705b-en. [36]

OECD (2024), *Global Forum on Digital Security for Prosperity*, https://www.oecd.org/en/networks/global-forum-on-digital-security-for-prosperity.html. [35]

OECD (2024), "New perspectives on measuring cybersecurity", *OECD Digital Economy Papers*, No. 366, OECD Publishing, Paris, https://doi.org/10.1787/b1e31997-en. [37]

OECD (2023), "Enhancing the security of communication infrastructure", *OECD Digital Economy Papers*, No. 358, OECD Publishing, Paris, https://doi.org/10.1787/bb608fe5-en. [4]

OECD (2022), *Good Practice Guidance on the Co-ordination of vulnerabilities*, OECD, Paris, https://one.oecd.org/document/DSTI/CDEP/SDE(2021)9/FINAL. [21]

OECD (2022), *OECD Policy Framework on Digital Security: Cybersecurity for Prosperity*, OECD Publishing, Paris, https://doi.org/10.1787/a69df866-en. [1]

OECD (2022), *Recommendation of the Council on Digital Security Risk Management*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0479. [6]

OECD (2022), *Recommendation of the Council on National Digital Security Strategies*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0480. [11]

OECD (2022), *Recommendation of the Council on the Digital Security of Products and Services*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0481. [14]

OECD (2022), *Recommendation of the Council on the Treatment of Digital Security Vulnerabilities*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0482. [18]

OECD (2022), "Routing security: BGP incidents, mitigation techniques and policy actions", *OECD Digital Economy Papers*, No. 330, OECD Publishing, Paris, https://doi.org/10.1787/40be69c8-en. [34]

OECD (2022), "Security of the Domain Name System (DNS): An introduction for policy makers", *OECD Digital Economy Papers*, No. 331, OECD Publishing, Paris, https://doi.org/10.1787/285d7875-en. [33]

OECD (2021), "Digital security in SMEs", in *The Digital Transformation of SMEs*, OECD Publishing, Paris, https://doi.org/10.1787/cb2796c7-en. [13]

OECD (2021), "Enhancing the digital security of products: A policy discussion", *OECD Digital Economy Papers*, No. 306, OECD Publishing, Paris, https://doi.org/10.1787/cd9f9ebc-en. [16]

OECD (2021), *Smart policies for smart products: A policy maker's guide to enhancing the digital security of products*, https://www.oecd.org/digital/smart-policies-for-smart-products.pdf. [17]

OECD (2021), "Understanding the digital security of products: An in-depth analysis", *OECD Digital Economy Papers*, No. 305, OECD Publishing, Paris, https://doi.org/10.1787/abea0b69-en. [15]

OECD (2020), "Encouraging digital security innovation : Global Forum on Digital Security for Prosperity", *OECD Digital Economy Papers*, No. 298, OECD Publishing, Paris, https://doi.org/10.1787/e65d02af-en. [12]

OECD (2020), "Going Digital integrated policy framework", *OECD Digital Economy Papers*, No. 292, OECD Publishing, Paris, https://doi.org/10.1787/dc930adc-en. [5]

OECD (2019), *OECD Recommendation on Digital Security of Critical Activities*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0456. [2]

OECD (2018), *OECD Due Diligence Guidance for Responsible Business Conduct*, https://mneguidelines.oecd.org/OECD-Due-Diligence-Guidance-for-Responsible-Business-Conduct.pdf. [9]

OECD (2015), *G20/OECD Principles of Corporate Governance*, OECD Publishing, Paris, https://doi.org/10.1787/9789264236882-en. [10]

OECD (2011), *OECD Guidelines for Multinational Enterprises, 2011 Edition*, OECD Publishing, Paris, https://doi.org/10.1787/9789264115415-en. [8]

OECD (2008), *Recommendation of the Council on the Protection of Critical Information Infrastructures*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0361. [24]

OECD (2007), *Recommendation of the Council on Electronic Authentication*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0353. [20]

OECD (1997), *Recommendation of the Council Concerning Guidelines for Cryptography Policy*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0289. [19]

US Department of Justice (2025), *Data security*, https://www.justice.gov/nsd/data-security. [26]

Notes

[1] OECD Directorate for Science, Technology and Innovation.

[2] OECD Going Digital Toolkit, Individuals who have experienced security incidents – last 3 months, [accessed 29 July 2024], https://goingdigital.oecd.org/datakitchen/#/explorer/1/toolkit/indicator/explore/en.

[3] https://www.imf.org/en/Publications/GFSR/Issues/2024/04/16/global-financial-stability-report-april-2024?cid=bl-com-SM2024-GFSREA2024001, p77-78.

New Approaches to Economic Challenges

Economic Security in a Changing World

Discussions of different aspects of economic security, such as supply chain resilience, energy security and cybersecurity, have intensified in recent years. They tend to take place in distinct fora, yet they are closely intertwined. To shed light on these interlinkages and foster synergies between different expert communities, the OECD organised a workshop on Economic Aspects of National Security in February 2024, as part of the New Approaches to Economic Challenges (NAEC) work programme. This report aims to extend the discussion and provide further insights into the main topics addressed during the workshop. It builds on the expertise across the OECD Secretariat and the International Energy Agency. It discusses specific aspects of economic security in the context of heightened geopolitical tensions, high interconnectedness spurred by globalisation, and green and digital transitions. By focusing on these emerging issues, the report seeks to provide insights that facilitate informed policymaking and strategic responses to ensure economic stability and resilience in an ever-changing world.

PRINT ISBN 978-92-64-87007-9
PDF ISBN 978-92-64-62069-8