FIIA REPORT

NOVEMBER 2022 / 71

NAVIGATING GEOECONOMIC RISKS

TOWARDS AN INTERNATIONAL BUSINESS RISK AND RESILIENCE MONITOR

Mikael Wigell, Heiko Borchert, Edward Hunter Christie, Christian Fjäder & Lars-Hendrik Hartwig

FIIA
FINNISH INSTITUTE OF INTERNATIONAL AFFAIRS

Funded by the European Union

FIIA REPORT

NOVEMBER 2022

71

NAVIGATING GEOECONOMIC RISKS

TOWARDS AN INTERNATIONAL BUSINESS RISK AND RESILIENCE MONITOR

Mikael Wigell, Heiko Borchert, Edward Hunter Christie,
Christian Fjäder & Lars-Hendrik Hartwig

FIIA
FINNISH
INSTITUTE
OF INTERNATIONAL
AFFAIRS

European
Commission

FIIA REPORT NOVEMBER 2022 / 71

This report is the outcome of the research project *International Business Risk and Resilience Monitor for Strengthening National Economic Preparedness* funded by the European Union via the Technical Support Instrument and implemented by the Finnish Institute of International Affairs in cooperation with the European Commission's Directorate-General for Reform Support (DG REFORM).

Reports can be ordered from the Finnish Institute of International Affairs.
+**358 9 432 7721 / asiakaspalvelu@fiia.fi**

All FIIA reports and other publications are available on our website at
www.fiia.fi

Language editing: Anna Sinkkonen
Printed by Punamusta Oy, 2022
Graphic design: Mainostoimisto SST Oy
Layout: Lotta-Marie Lemiläinen
ISSN 1458-994X (print)
ISSN 2323-5454 (web)
ISBN 978-951-769-743-9 (print)
ISBN 978-951-769-744-6 (web)

FIIA
FINNISH
INSTITUTE
OF INTERNATIONAL
AFFAIRS

Arkadiankatu 23 b
POB 425 / 00101 Helsinki
Telephone +358 (0)9 432 7000
Fax +358 (0)9 432 7799

www.fiia.fi

CONTENTS

List of abbreviations 7
Foreword 9

Introduction 11

1 Why geoeconomics matters 17

2 Corporate geoeconomic risk management 27

3 Recommendations 63

Final remarks 69

Bibliography 71
Contributors 75
Previously published in the series 77

LIST OF ABBREVIATIONS

CEO	Chief Executive Officer
CFO	Chief Financial Officer
CNI	Critical National Infrastructure
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CRO	Chief Risk Officer
ERM	Enterprise Risk Management
ESG	Environmental, Social and Governance
FDI	Foreign Direct Investment
GRC	Governance, Risk and Compliance
IBRRM	International Business Risk and Resilience Monitor
IPR	International Property Rights
ISO	International Organization for Standardization
MW	Megawatt
OECD	Organisation for Economic Cooperation and Development
PEST	Political, Economic, Social, Technological
PESTEL	Political, Economic, Social, Technological, Environmental, Legal
PG-LESTE	Political, Geoeconomic, Legal, Economic, Social, Technological, Environmental
PRC	People's Republic of China
SCM	Supply Chain Management
SOE	State-owned Corporation
SWIFT	Society for Worldwide Interbank Financial Telecommunication
WTO	World Trade Organization

FOREWORD

Recent years have seen the rise of geoeconomics around the world and the brittleness of global value and supply chains, which has been further increased by the Covid-19 pandemic and Russia's aggression in Ukraine. The risk of disruptions in critical economic flows has heightened, challenging national economic resilience around Europe. For the foreseeable future, the world economy is likely to be a less predictable and more volatile environment than before. Geoeconomic risks are here to stay, and what is needed are new tools to identify, assess and monitor them to enhance preparedness against them.

In September 2021, the Finnish Institute of International Affairs (FIIA) launched the *International Business Risk and Resilience Monitor for Strengthening National Economic Preparedness* project at the request of the Austrian Federal Ministry of Labour and Economy (former Austrian Ministry for Digital and Economic Affairs). The project was funded by the European Union via the Technical Support Instrument ("TSI") and implemented by FIIA in cooperation with the European Commission/European Commission's Directorate General for Reform Support (DG REFORM). Faced with the rise of geoeconomics, Austria seeks to improve its national economic resilience and is in the process of developing a new framework and capstone document for this purpose. To achieve this, Austria requires an improved capability to identify and assess transnational geoeconomic risks. Considering that private sector actors are at the forefront of these risks and responsible for most critical economic activities, they also need to be included in the national risk picture.

Consequently, this project aims to develop new analytical tools to support public and private risk management and enhance strategic-level public–private dialogues concerning geoeconomic risks. It develops an advanced concept for an International Business Risk and Resilience Monitor, a digital tool that combines foresight, risk management and strategy development in dealing with transnational geoeconomic risks. The concept is embedded in a thorough analysis of current geoeconomic trends and an expert assessment of geoeconomic risks from a corporate perspective. This final report summarizes the project's main findings, which are discussed in more detail in several issue-specific publications.

The project team gratefully acknowledges the funding of this project by the European Commission. We extend our gratitude to the Austrian

Federal Ministry of Labour and Economy at whose request this project was initiated. The research team would especially like to thank the members of the steering group for its active and constructive engagement throughout the project. The steering group consisted of representatives of the Austrian Ministry for Digital and Economic Affairs, the National Emergency Supply Agency of Finland as well as the European Commission (DG Reform).

Warm thanks are also due to all the experts who contributed with their views and comments during different stages of the project, particularly in Austria and Finland as well as in other European nations.

Helsinki/Vienna, 15 November 2022

INTRODUCTION

In 1851, German manufacturer Ferdinand Theodor Einem opened a small pastry shop in Moscow. He supplied the Tsar's armed forces with syrup and jam. The business prospered. Throughout the 1870s, Julius Heuss, who took over the reins after Einem's death, strived to make the family-owned company Russia's best pastry producer. The company operated 40 shops from Samarkand to Riga. On the eve of the First World War, the company had been issued a warrant of appointment to the Tsar, a prestigious recognition at the time. Heuss's example is illustrative of the long history of close economic ties between Russia and Germany. In 1901, six out of ten companies in Russia's electricity industry were majority-owned by German investors. Around ten years later, Russia sourced 48 % of its imports from the German Empire, which in turn purchased approximately 44 % of Russia's exports.[1]

Fast forward to today, and more than 1,000 companies have partly or fully withdrawn from the Russian market in the wake of Russia's war of aggression against Ukraine and Western sanctions against Russia. It has been estimated that the value of these companies' investment in Russia "represents the lion's share of all accumulated, active foreign investment in Russia since the fall of the Soviet Union", thereby reversing "three decades' worth of Russian economic integration with the rest of the world".[2]

The contrast between these two examples could not be starker and is a most useful reminder of the Janus-faced nature of cross-national economic ties. Ever since Norman Angell reflected upon the peace-promoting nature of economic interdependence, policy makers and entrepreneurs have developed a much more pronounced interest in the benefits rather than the dark sides of economic cooperation.[3] The risks associated with economic dependence that comes with interdependence has always existed but has been grossly overlooked.

Economic globalization has boosted the exchange of goods, raw materials, services, money and data and enabled substantial movements of people. These exchanges have advanced the idea of a growing "deterritorialization", whereby distance and place no longer matter. But this idea is

1 Creuzberger 2022.

2 Sonnenfeld et al. 2022, 54, 61.

3 Angell 1910.

as alluring as it is flawed. Economic exchange depends on infrastructure, and infrastructure runs through geospatial corridors. These corridors link countries and markets together by connecting sources of origin to destination regions via transit regions. Bound together by corporate supply chains, these corridors are subject to more-or-less stringent regulatory regimes that set the boundaries for economic interaction. These supply chains, in turn, "are not the product of invisible hands . . . but rather the result of concrete policies and competing models of political survival that dominant ruling coalitions adopt in different states".[4]

The mindset that underpins these policies has changed.[5] In the past, globalization benefitted from a benign regulatory approach in which governments clearly separated economic interests from security interests.[6] Since the global financial crisis in 2008 and 2009, however, national security has been increasingly portrayed as economic security.[7] Consequently, governments have become more wary of the negative consequences of global economic exchange in terms of national competitive advantage, the shrinking of the middle class and detrimental effects on human rights, climate change or public health.

Global economic exchange has also come to be seen as more problematic because the practice of geoeconomics has resurfaced.[8] In the broadest sense, **geoeconomics is the pursuit of power politics using economic means. This includes measures such as embargoes, sanctions, export controls, anti-competitive subsidies, investment screening mechanisms and data localization measures**. Geoeconomics is meant to advance and augment the economic interests of one country while disciplining and deterring its strategic competitors. This type of economic statecraft has been motivated by the belief that strategic competitors do not pursue economic cooperation for mutual benefits, but rather aim to advance their own benefits at the expense of others. That is why technological standards, technology transfers and supply chain security are at the heart of today's geoeconomic competition.

This, however, changes the nature of relations between businesses and governments.[9] Gone are the days of laissez-faire governments that give companies a free hand in conducting their affairs. In today's geoeconomic environment, governments intervene more frequently. The level

4 Solingen 2021, 9.

5 Borchert 2019; Choer Moraes and Wigell 2022.

6 Roberts and Lamp 2021.

7 HM Government 2010.

8 On the rise of geoeconomics, see Wigell, Scholvin and Aaltola 2018.

9 Borchert 2019; Sheffi 2020; Weber 2019.

of intervention is also set to cut deeper into business practices as strategic competition between nations is a structural factor that shapes the international system.[10]

This affects businesses at three levels. First, the texture of bilateral and multilateral economic cooperation is fundamentally changing. Entire nations, not only certain market segments, can become no-go areas for companies. This increases the risk of large write-downs on past investments that may become stranded. Second, the nature of industrial competition is changing as political preferences shift towards national champions that benefit from preferential government support measures. Finally, geoeconomics affects corporate decision making and business models because governments may prohibit companies from exporting or importing certain components, restrict research cooperation with certain countries for national security reasons or prohibit investments in certain markets.

Companies, however, are not necessarily passive actors at the receiving end of geoeconomic change. They also have agency. Corporate power may run counter to government interests, and companies may shape economic exchanges to their own commercial advantage.[11] Corporate risk management is an instrument that serves both ends. Still, geoeconomic competition changes the frame of reference for corporate risk management.

Based on an international survey of corporate experts and individual interviews with corporate risk managers, this study argues that awareness of the impact of geoeconomic developments on corporate action is growing, but that more needs to be done to advance corporate geoeconomic proficiency. To that end, this study develops an initial vision for an International Business Risk and Resilience Monitor (IBRRM). We propose that a collaborative tool based on this vision should underpin strategic-level public–private cooperation. Closer cooperation between government ministries and companies is needed to better understand the unfolding geoeconomic landscape and the consequences of policy decisions meant to curb the geoeconomic appetite of strategic competitors.

Einem Pastry, the small shop that grew into a famous establishment in Tsarist Russia, did not withstand the test of history. Nationalized in 1922, the company was rebranded as Red October, although its German origin remained part of the brand name until 1930.[12] The company's fate is a historical vignette of what geopolitical upheavals may bring about. The decoupling that followed echoes with contemporary developments.

10 See, e.g., Alami and Dixon 2020; Choer Moraes and Wigell 2022.

11 Borchert 2021; Choer Moraes and Wigell 2020.

12 Creuzberger 2022.

As governments become more attentive to the modalities of how their nations trade and cooperate with other nations, geoeconomic factors will increasingly affect corporate strategies and business models. Companies, in turn, will have to walk a fine line between anticipating political preferences and upholding their business interests. In this evolving environment, businesses may be torn between the risk of politically misguided investments and excessive risk aversion. In parallel, as the number and complexity of geoeconomic actions increase, ranging from financial sanctions to new export controls and investment prohibitions, it is in the common interest to work on new modes of public–private cooperation and dialogue. We hope that the ideas put forward in this report will contribute towards that goal.

/ 1

1 WHY GEOECONOMICS MATTERS

After a long phase of expanding economic globalization, which unfolded in a largely benign international security environment since 1990, global business activity has started to face new challenges – or new versions of older challenges. At first, this happened slowly and through small crises, and then through a succession of increasingly violent shocks from 2020 onwards. The first major shock was the Covid-19 pandemic, which revealed the brittleness of critical global supply chains and a serious lack of domestic manufacturing capabilities and capacities in many nations. The second major shock is Russia's war of aggression against Ukraine in 2022, to which the European Union (EU), the United States (US) and other Western nations have responded with unprecedented financial sanctions and export control restrictions.

These major shocks come in addition to pre-existing trends whereby states resort, increasingly, to a security-oriented view of international economic exchange, as well as to policies to control or restrict such exchange for reasons of national security. This represents the emergence of an intermediate form of capitalism, which we refer to as strategic capitalism (see Table 1). In strategic capitalism, the state intervenes strongly in markets and industries it deems important from a national security perspective while adopting a liberal stance on other markets and industries. While even economically very liberal systems tend to maintain strong state intervention in the defence and security sectors, in strategic capitalism, the range of markets and industries subjected to security-oriented interventions is broader than in market capitalism but more selective than under state capitalism, in which the motivation for state intervention is ideological and broad-based.[13]

	Market capitalism	Strategic capitalism	State capitalism
Scope of state intervention	Limited	Selective	Broad
Dominant state goal	Economic	Security	Political
State–business relations	Distant	Varied	Close

Table 1: Varieties of capitalism
Source: authors

13 For the conceptualization of strategic capitalism, see Choer Moraes and Wigell 2020.

During the Cold War, members of the European Economic Community may be said to have pursued a mixed model in which security-oriented considerations played a role for some industries, while successive governments of different political persuasions engaged on a more ideological spectrum regarding state-ownership versus privatization of certain industries and critical infrastructures. From the 1980s onwards, the dominant trend in Western economic policy writ large was a move towards free-market reforms, in other words, towards market capitalism. This trend accelerated from 1990. Following the end of the Cold War, a major thrust of Western economic policy was the market opening of new areas of domestic economic activity such as telecommunications, transport and energy, accompanied by successive rounds of trade and investment liberalization with international partners. Business practices evolved in response, in search of economic efficiency and new opportunities, leading to higher levels of both inward and outward foreign direct investment. These developments led to the emergence of longer and more internationalized supply chains, both within the European single market as well as with third countries. In parallel, national security considerations, notably security of supply considerations, were viewed with more optimism and less stringency. The fact that companies and industries were becoming increasingly dependent on extra-European suppliers or clients was viewed largely positively. These trends also strengthened certain business practices such as just-in-time manufacturing, which achieved cost reductions by reducing stockpiling.

Slowly, from the mid-2000s onwards, doubts began to surface about the resilience of the market capitalist model that had emerged. In the European context, concerns were raised about dependence on imports of Russian fossil fuels, notably in light of Russian supply cut-offs to Ukraine and certain other Central and Eastern European countries. In the run-up to the financial crisis of 2008, the price of oil had surged to over 140 dollars per barrel, with the prices of certain metals and agricultural commodities rising in co-movement. Thus, concerns about security of supply, regarding both prices and available quantities, became more topical, especially in the case of fossil fuels. In more recent years, the issue of the availability and global geographic distribution of certain rare minerals (so-called rare earths) also came to the fore.

Adding to this growing range of goods now deemed sensitive, concerns also arose regarding certain manufactured goods. During the Trump presidency, the United States began to view China's antagonistic practices in technology transfers and intellectual property as significantly problematic

for industrial competitiveness and national security.[14] Over a short period, views converged significantly between the two sides of the Atlantic (and became largely bipartisan within the US), leading the EU and the US to adopt similar new export control restrictions against China, which were also justified by concerns over human rights abuses. In parallel, with the rise of the Fourth Industrial Revolution and technologies such as artificial intelligence, states across the world – including major rival powers such as Russia and China – openly declared major ambitions to adopt new technologies, viewing them as key to achieving greater state power, including military power.[15]

It was against this rapidly evolving backdrop that two major accelerating shocks occurred: the Covid-19 pandemic, which revealed a disturbing lack of manufacturing capabilities in Western economies, and Russia's 2022 invasion of Ukraine, which has led to unprecedented economic sanctions against Russia – effectively bringing the world close to a complete decoupling between Russia and most of the advanced economies of the OECD. The cascading consequences of Russia's aggression against Ukraine continue to evolve, with major threats to global food supplies and energy markets.

Russian energy and the Fortum company

The debacle of the Finnish majority state-owned energy giant Fortum is a cautionary tale of overexposure to a supplier that had a known propensity for weaponizing energy supplies.

Russia's use of energy supplies as a tool of coercion and the potential dangers of even the first Nord Stream pipeline, not to mention the second, had been well documented already prior to 2010, including in publications issued by both Finnish and Swedish institutions.[16]

In light of the annexation of Crimea and the Donbas War of 2014–2015, certain European corporations' and governments' choice to *increase* their exposure to Russian energy can only be described as a systemic failure to take geoeconomic risks into consideration.

German corporations and the German federal government pursued this trajectory mainly through the Nord Stream 2 project.[17]

14 Office of the United States Trade Representative 2018.

15 Christie et al. 2021.

16 See, e.g., Liuhto (ed.) 2009; Hedenskog and Larsson 2007; Vihma and Wigell 2016.

17 For a geoeconomic analysis of the Nord Stream 2 project, see Vihma and Wigell 2016.

Fortum, which had pre-existing activities in Russia, chose to increase its exposure to the Russian market by purchasing the German energy company Uniper, which had a large Russian portfolio, starting with a purchase of 47.35 % of shares concluded in June 2018,[18] and with subsequent purchases of shares culminating in a 75.01 % stake by August 2020.[19] Through Uniper alone, Fortum had acquired new exposure to the Russian energy market in two forms:

- Power generation facilities inside Russia, totalling 11.245 MW of installed capacity as of December 2021 (for comparison, this equals to around two thirds of Finland's total capacity)[20]
- A stake in the Nord Stream 2 project through loans to Nord Stream 2 AG.

By September 2022, the share price of Uniper had collapsed by 90 % as compared to January 2022, and the German government decided to nationalize Uniper, with Fortum receiving EUR 500 million for its share. At the time, it was estimated that Fortum had made a net loss of EUR 6 billion from its Uniper investment.[21]

In addition to matters of security of supply, the current war involves strong financial sanctions by the US and the EU against Russia. The use of financial sanctions – limiting access to Western capital markets, foreign exchange markets and financial services – has been extensive in recent decades, leveraging the strongly dominant position of Western nations.[22] However, this has also led to attempts by non-Western nations to develop alternative arrangements to circumvent the impacts of such measures. A commonly cited example is the SWIFT financial messaging system and the setting up of Chinese[23] and Russian[24] alternative systems.

As major powers in the international system increasingly compete against one another by using antagonistic economic policies, the prospect of outright decoupling – involving a substantial severance of relations of dependence between them in key areas of economic exchange – is

18 Uniper 2018.

19 Reuters 2020.

20 Uniper 2021.

21 Vanttinen 2022.

22 Nephew 2017.

23 Cross-Border Interbank Payment System (CIPS). For more, see https://www.cips.com.cn/cipsen/7052/7057/index.html.

24 Sistema Peredachi Finansovykh Soobscheniy (SPFS). For more, see https://www.cbr.ru/eng/Psystem/fin_msg_transfer_system/.

becoming more likely. In this regard, we identify three key drivers of change that help to explain the emergence of geoeconomics as a fundamental force in international relations: the weaponization of economic relations, the securitization of economic relations and, as an emerging result, the balkanization of the global economy.[25]

The **weaponization of economic relations** refers to the increasing trend of harnessing and disrupting economic relations to gain strategic and national security advantages. This is now evident in the proliferation of economic and financial sanctions and other forms of economic coercion. The fact that certain states increasingly use economic means as tools of power politics in turn incentivizes all states in the international system to designate a wider range of industries and markets as relevant from a national security perspective, which constitutes the **securitization of economic relations**.

The growing propensity to see global interdependence through the lens of geoeconomic dependence breeds antagonistic dynamics in global economic relations, which can lead to a process of decoupling in bilateral value and supply chains. As these processes proliferate, but with different intensities between different sets of nations, the pattern that risks emerging is a **balkanization of the global economy** – a world of competing standards and regulations that bring about a fragmentation of international value and supply chains.

While the main emerging decoupling dynamic, prior to the Russia–Ukraine war of 2022, has occurred between China and the United States, it has global implications and the potential to become globally pervasive as global technology value and supply chains are not neatly organized around the US and China. Two examples of this are the emerging competition for the dominance of technical standards and the competition for access to strategic resources and components such as semiconductors. The pursuit, by states, of self-sufficiency and strategic autonomy are rational reactions in such an environment, but it is also likely to have further negative impacts on the norms and processes of global trade.

The shift to a new variety of capitalism – i.e., from market capitalism to strategic capitalism – is a deep transformation with a complex set of long-lasting effects. It entails a change of paradigm about how economic activities are carried out and what framework conditions and goals states should set for them. The change is hard to overstate: for decades, the basic assumption – in economics, management classes and policy discussions throughout the Western world – was that the fundamental role of government should be to get out of the way and let business seek out

25 Fjäder, Helwig and Wigell 2021.

opportunities everywhere they may be found. Exceptions to this general rule were overwhelmingly geared towards domestic concerns such as consumer protection, environmental issues or fundamental rights. The notion that states should be interventionist in international business for reasons of national security and national power had faded with the end of the Cold War. The fact that some authoritarian states were evidently not "getting out of the way" but were instead pursuing clear power objectives through antagonistic actions – ranging from aggressive forms of espionage and intellectual property theft to trade coercion and energy supply cut-offs – did not immediately lead to a response. There was a sense among many Western governments that it would be in the own interest of authoritarian states to realize that the market capitalist model is more efficient and more conducive to shared prosperity, and that Western nations' unilateral adherence to the rules would be akin to leading by example. However, authoritarian governments had other ideas in mind. And while it takes "two to tango" to achieve a collaborative solution, it only takes one to start a conflict or act in an exploitative or predatory manner. Fast forward to 2022, and the realization that change is needed is everywhere. Effectively, the entire connection between economics and national security is being rethought. Short-term measures to coerce and to withstand coercion, as well as long-term measures to seek to stay ahead in crucial areas of technology, are common topics of discussion in both the public and private sectors – while the policy responses to address these challenges are multiplying. The emerging landscape is complex. The hitherto narrow and specialist area of export controls is a growing field that more and more companies need to be aware of as the lists of restricted dual-use products keep expanding. The screening of foreign direct investment for national security purposes is an even clearer example. In the European context, such screening barely existed a few years ago, and to the extent that it did, governments were often tempted to overlook the concerns expressed by the security professionals from their own ranks. The brutal process of moving away from Russian energy supplies amid the largest European war since 1945 is a painful reckoning of past practices and assumptions.

For companies, the shift from market capitalism to strategic capitalism is no less monumental. It implies the need to understand the myriad ways in which actions by governments – their home governments as well as foreign governments – may put their revenues, investments and value chains at risk. Every channel of economic exchange may potentially be affected: imports as well as exports, whether of goods or services; portfolio investments; strategic investments; technology transfers and interactions

with stakeholders of all types. Identifying and assessing these risks efficiently can either make or break companies that rely on global markets. To better prepare companies to withstand these disruptions, corporate risk management needs to adapt to and integrate the new universe of risks that pertains to geoeconomics. In the following sections, we take a closer look at how corporations have traditionally considered the risks they face, and how geoeconomic risks should now be added to existing frameworks and practices.

/ 2

2 CORPORATE GEOECONOMIC RISK MANAGEMENT

To a large degree, contemporary corporate risk management does not systematically cover geoeconomic risks. Integrating geoeconomic risks can and should build on existing enterprise risk management. This section explores the core elements of enterprise risk management and suggests potential avenues for their implementation in the context of geoeconomic risks.

2.1 ENTERPRISE RISK MANAGEMENT

Traditionally, corporate risk management has focused on insurance and financial risks, but over the past two decades, it has become broader in focus and increasingly standardised as expectations from investors, regulators, consumers, customers and other stakeholders have become greater. This is in part a response to the increasing complexity and interdependence of doing business internationally, coupled with increasing systemic risks related to global trends such as climate change, biodiversity loss, demographics and geopolitics. At the same time, these changes in corporate risk management are also a response to the evolving standard of responsible corporate citizenship. Spectacular corporate governance failures, such as the Enron and Parmalat scandals, and environmental catastrophes, such as the Deepwater Horizon, Bhopal and Fukushima disasters, have also had significant impacts.[26]

The expansion of corporate responsibility to new areas has led to the creation of standards under the broad umbrella of environmental, social and governance (ESG) issues, which investors have utilised to screen potential investments. In parallel, the scope of risk management has also expanded correspondingly to cover these areas of corporate responsibility and brand reputation, as well as more operational areas such as supply chain security, business continuity, safety, security and cybersecurity.

The Covid-19 pandemic and global headlines about rising geopolitical risks have also highlighted the growing need for companies to tighten their management of both strategic and operational risks. The two interrelated frameworks of corporate governance (the emergence of rules,

26 Monahan 2008.

standards and practices that guide the ethical conduct of business) and risk management (identifying and managing potential hazards to business) have been increasingly bundled together under the common umbrella of *governance, risk and compliance* (GRC). [27]

Within the concept of GRC, risk governance has also experienced a significant evolution towards standardisation. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) published its *Enterprise Risk Management – Integrated Framework* initially in 2004 (updated in 2017), which promoted a more holistic understanding of risk in companies, arguing for linking risk with business strategy and performance and working across internal silos (Figure 1). This approach came to be known as Enterprise Risk Management (ERM).

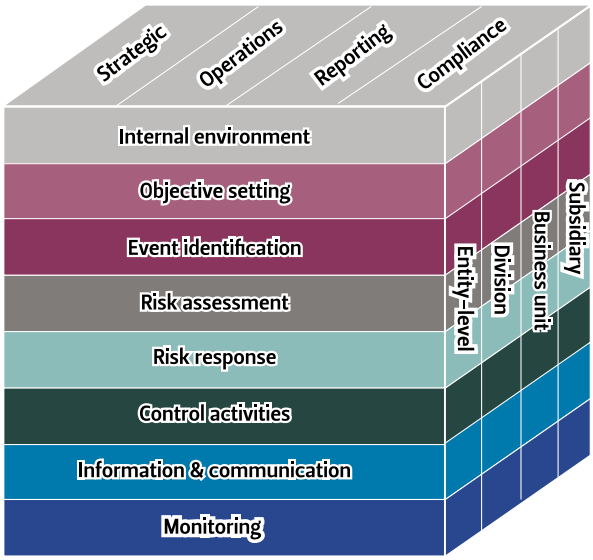


Figure 1: COSO enterprise risk management cube
Source: Williams 2019

Whereas risk management had traditionally been the remit of chief financial officers (CFOs), true to its original focus on financial risks, the mainstreaming of ERM led to the creation of chief risk officers (CROs) in an increasing number of companies to reflect risk management as an enterprise-wide capability. The ERM framework consequently addresses all potential risks across the entire company and all its activities, including processes, products and services, in an end-to-end manner, taking into account factors both internal and external to the company. As a holistic

27 See, e.g., Racz et al. 2010.

discipline, ERM considers an increasing number of risk categories, including but not limited to hazard risk, financial risk, operational risk and strategic risk. The successful implementation of ERM not only enables the organisation to better control all relevant risks, but also to exploit upside risks, i.e., opportunities.

The updated 2017 COSO ERM framework further emphasises the importance of integrating risks into the strategy-setting process and the processes that drive performance to meet the increasing demands of an evolving business environment (Figure 2).[28]

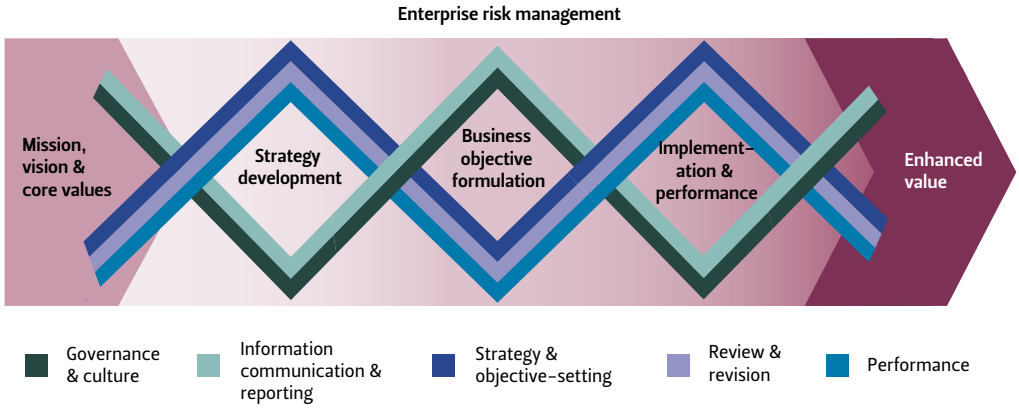


Figure 2: COSO enterprise risk management framework 2017
Source: Williams 2019

In addition to COSO, international standards, principally the ISO 31000:2018 Risk management standard, provide guidance for companies to implementing risk management. The aim of the ISO 31000 standard is to provide comprehensive guidance for organisations to "create and protect value in organizations by managing risks, making decisions, setting and achieving objectives and improving performance".[29] To this effect, the standard outlines the guiding principles for the design, implementation, evaluation, improvement and integration of a risk management framework (Figure 3) in organisations, as well as recommendations for its application.

28 Committee of Sponsoring Organizations of the Treadway Commission (COSO) 2022.

29 International Organization for Standardization (ISO) 2018.

The guiding principles of ISO 31000 are as follows:

- Managing risk is iterative and assists organizations in setting strategy, achieving objectives and making informed decisions.
- Managing risk is part of governance and leadership and is fundamental to how the organization is managed at all levels. It contributes to the improvement of management systems.
- Managing risk is part of all activities associated with the organization and includes interaction with stakeholders.
- Managing risk considers the external and internal context of the organization, including human behaviour and cultural factors.

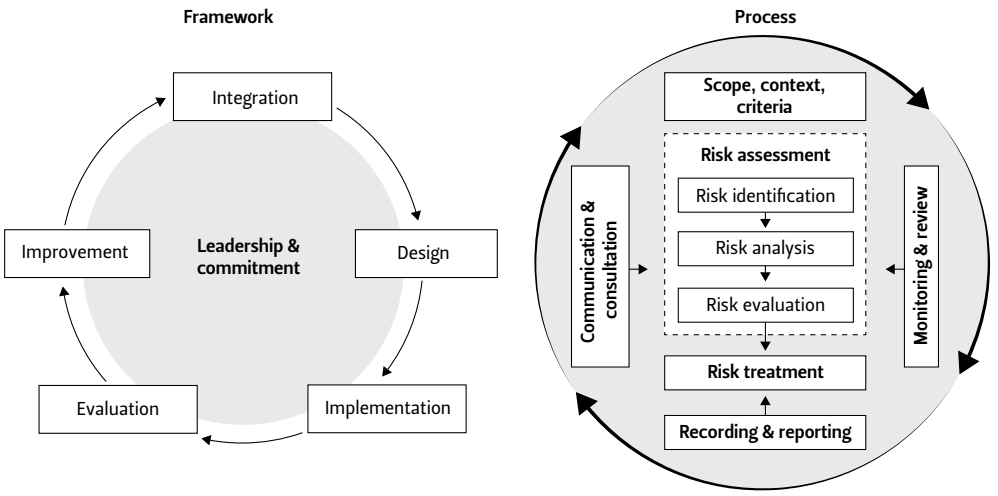


Figure 3: ISO 31000 risk management
Source: International Organization for Standardization (ISO) 2018

The recommendations for risk assessments cover the processes of risk identification, risk analysis, risk evaluation and risk treatment:

Risk identification

- Risk identification aims to find, recognise and describe all risks that may have an impact on the organisation's capabilities to achieve its objectives. This requires gathering all the relevant information regarding the potential hazards, their origins and root causes, and the organisation's vulnerability to them.

Risk analysis

- The purpose of risk analysis is to establish a sufficient level of understanding of the nature of risk, its characteristics and, when possible, the level (magnitude) of risk for the organisation. A good risk analysis involves an educated consideration of all the relevant uncertainties and root causes of a potential risk event, as well as

its consequences (impact), likelihood and possible variations. To establish an understanding of the implications of risk for the organisation, existing controls and their effectiveness against it should be evaluated. Risk analyses can be conducted in varying degrees of detail, depending on the intended purpose of the analysis, as well as the availability and reliability of related information. Risk analyses may be qualitative, quantitative or a combination of both. It is important to also consider the potential evolution of risk over time.

Risk evaluation

- Risk evaluation is an activity intended to enable decision making regarding risk. As such, it involves determining the relevance of the risk in the context of the organisation's objectives and deciding the course of action with respect to the organisation's established risk tolerance and existing controls. The organisation may decide to accept the risk, rely on existing controls, withdraw from the activity or determine its risk treatment options.

Risk treatment

- Should the organisation decide to continue the activity but determine that it wants to control the probability or consequences (impact) of the risk, it needs to establish and select the appropriate risk treatment options. These should always balance the consequences of the risk with the costs, efforts and disadvantages of the risk treatment. The generic risk treatment options are:
  - **Avoid**. The organisation may choose not to start or to discontinue the activity to avoid the risk.
  - **Accept**. The organisation may decide to accept the risk if it considers the benefits of engaging in the activity higher than the value or consequences of the risk. This must be an informed decision.
  - **Mitigate**. The organisation may choose to apply controls to lower the possibility of occurrence of the risk or its consequences to reduce the level of residual risk.
  - **Transfer**. The organisation may attempt to transfer or share the risk or part of it with a customer or partner, or by purchasing an insurance against it. This is another viable option for reducing the residual risk to an acceptable level.

The analytical framework presented above has underpinned our approach to the IBRRM project, the structure of this report and the project deliverable reports that were submitted to the European Commission, as illustrated in Figure 4. The following sections will explore these steps in the context of corporate geoeconomic risk management.

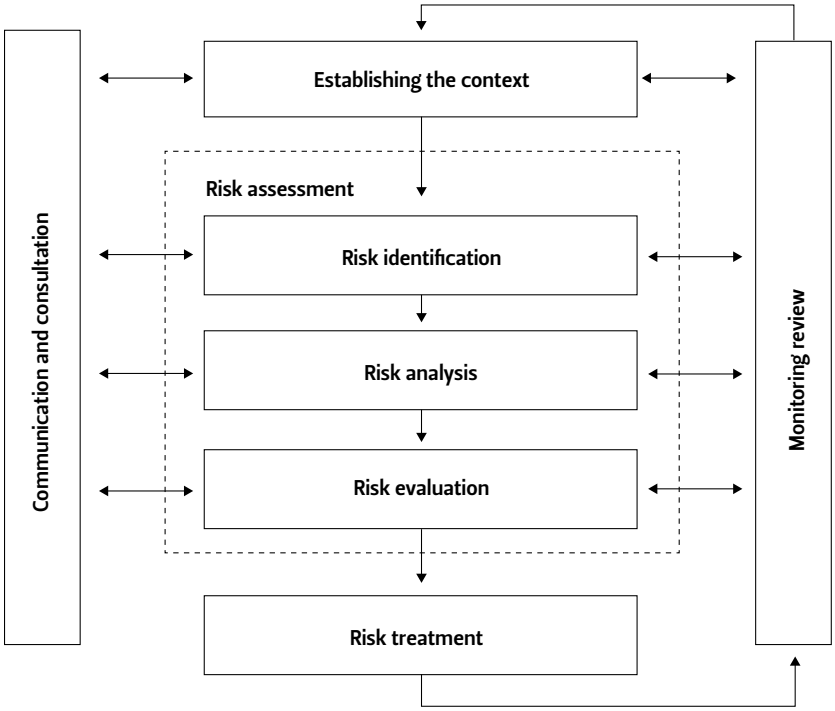


Figure 4: IBRRM and the risk management process according to ISO 31000:2018
Source: authors

2.2 GEOECONOMIC RISK IDENTIFICATION

As argued above, risk identification sets the stage for understanding risk landscapes. However, before illustrating risk identification from the corporate perspective, we also wish to highlight **the position of geoeconomic risks from a state perspective**. We propose one possible approach in Table 2. In it, we distinguish between threats which result from hostile intent and risks which do not. As is common in security policy analyses carried out by states, we also differentiate between state and non-state actors as sources of risks or threats. We then consider three key areas of harm, namely population and society, environment, and economy and technology, while noting that different breakdowns can also be used.[30]

30 National risk assessments use a variety of breakdowns regarding areas of harm. For example, the Swiss government's national risk assessment focuses on four areas of harm, which are people, environment, economy and society. See Federal Office for Civil Protection FOCP (2020).

In the approach presented in Table 2, geoeconomic measures occupy a clearly delineated place: they constitute threats, not risks; they emanate from state actors, not non-state actors; and the area of harm they affect is the economy of a rival state, including its technological capabilities.

		Risks		Threats	
		State actors	**Non-state actors**	**State actors**	**Non-state actors**
Area of harm	**Population and society**	Foreign state failure leading to uncontrolled population movements	Natural disasters; major accidents	Armed attacks; hybrid threats, e.g. disinformation, sabotage	Domestic and transnational crime and terrorism
	Environment	Lax environmental regulations on the part of another state	Domestic and transnational environmental degradation, e.g., due to natural disasters, industrial accidents	Intentional attacks to damage the natural environment	Cross-border dumping of hazardous industrial waste
	Economy and technology	Foreign state failure leading to economic shocks	Market-driven international supply or demand shocks, e.g. supply shortages in energy or raw materials	**Geoeconomic measures** Financial sanctions; import bans; export bans; state-driven currency manipulation; state-sponsored industrial espionage	Corporate-sponsored industrial espionage; market-driven reputational attacks, speculative attacks

Table 2: Risk typology – state perspective
Source: authors

It is necessary to understand the motives for deploying policy measures. For example, a state aid measure may be driven by domestic political factors, ranging from social or regional policy considerations to outright clientelism. Alternatively, such a measure may be part of a deliberate industrial strategy that embeds antagonistic or even hostile foreign policy objectives. The state aid measure should be deemed geoeconomic in the latter case, but not in the former. The identity of the ultimate actor or sponsor of the measure is also relevant. As illustrated in Table 2, state-sponsored industrial espionage[31] should be viewed as geoeconomic, whereas purely corporate-sponsored industrial espionage should not.

31 We use the term "industrial espionage" to refer to all espionage against corporate targets and the terms "state-sponsored" versus "corporate-sponsored" to specify which type of actor sponsors it. We choose to refrain from using the term "economic espionage".

An example of state-sponsored industrial espionage is the case of Mr Hao Zhang, a Chinese national who was found guilty of industrial espionage in the United States in 2020.[32] The court established that Mr Zhang had "plotted with Tianjin University to take trade secrets from two U.S. companies, including his own employer, to China for the benefit of the Chinese Government". The trade secrets stolen by Mr Zhang were related to advanced filter technologies designed to enhance the performance of wireless devices. Zhang and a co-conspirator worked for two US companies and conspired with Tianjin University, which acted as an instrument of Chinese state interests. Following a plan developed with the university, Zhang stole the trade secrets, left the US, set up a rival company registered in the Cayman Islands and filed for and obtained patents in his own name using the stolen trade secret information.

Moving on to the **position of geoeconomic risks from a corporate perspective**, one common practice is to break down risks emanating from a company's external environment by main categories. One of the most established approaches is the PEST analysis, in which PEST stands for political, economic, social and technological factors.[33] PEST analyses have been extended in recent years, leading notably to the PESTEL framework (adds environmental and legal factors) and STEEPLE framework (adds ethical factors). We will focus on the PESTEL (also known as PESTLE) framework, which is the most commonly used.

Looking at the PESTEL analysis, it is not entirely clear where geoeconomic measures should be placed in the framework. They derive from government decisions and are usually industry-specific and in some cases firm-specific. Some of these measures may have the same legal bases that are used for ordinary product or market regulation measures, while others may rely on legal instruments related to external trade or investment. On the other hand, what is viewed as "economic" in a PESTEL analysis largely refers to market forces, or to market forces that come under the influence of states' macroeconomic policies (e.g., monetary and fiscal policies), which are usually too broad-based to be geoeconomic in nature. In sum, there is a case for viewing geoeconomic measures as a new category between the political and legal categories included in PESTEL analyses. Rearranging these categories, we propose an extension of the PESTEL framework which we refer to as PG-LESTE, as shown in Table 3.[34]

32 U.S. Department of Justice 2020.

33 Sammut-Bonnici and Galea 2014.

34 The original PESTEL category descriptions in Table 3 are based on Washington State University management course guide material, available at https://libguides.libraries.wsu.edu/c.php?g=996573&p=7214435.

PG-LESTE	Type of risk
Political	Government policies, leadership and change; foreign trade policies; internal political issues and trends; tax policy; regulation and deregulation trends
Geoeconomic	Government measures aimed at specific industries for strategic or national security reasons with the goal of protecting them at national level and/or harming those industries in a rival nation. Typical measures include financial sanctions; import bans; export bans; outward investment bans; inward investment screening; anti-competitive uses of product or market regulations, standards or administrative requirements; and state-sponsored industrial espionage and intellectual property theft.
Legal	Health and safety; equal opportunities; advertising standards; consumer rights and laws; product labelling and product safety
Economic	Economic growth; inflation and interest rates; job growth and unemployment; labour costs; impact of globalisation; disposable income of consumers and businesses; likely changes in the economic environment
Social	Demographics (age, gender, race, family size); consumer attitudes, opinions and buying patterns; population growth rate and employment patterns; sociocultural changes; ethnic and religious trends; living standards
Technological	New ways of producing goods and services; new ways of distributing goods and services; new ways of communicating with target markets
Environmental	Scarcity of raw materials; pollution targets; doing business as an ethical and sustainable company; carbon footprint targets

Table 3: Risk typology – corporate perspective
Source: authors

European sanctions against Russia:
Luxury goods exports versus diamond imports

What could European businesses reasonably expect with respect to the Russian market in January 2022? At a consultation event attended by a member of the research team in early 2022, well-informed former government officials from both sides of the Atlantic focused their presentations on the sanctions that had been pre-announced, such as new export controls on dual-use products, sanctions against Russian banks, the possibility of disconnecting Russia from the SWIFT financial messaging system and individual sanctions involving asset freezes and travel bans.

These were expected to be applied to senior Russian decision makers, including President Vladimir Putin. It was anticipated that energy supplies would enter into the picture, including the risk of a full Russian supply cut. What the experts on this particular occasion did not anticipate were the impacts on non-strategic, consumer-oriented sectors – except for indirect effects that would arise from depressed demand as a result of the macroeconomic

effects of the financial sanctions. On 15 March 2022, the European Union decided to prohibit the export of luxury goods to Russia. The prohibition covers, inter alia, wines, cigars, clothing, footwear, jewellery, tableware and watches of a value exceeding EUR 300 per item, as well as electronic items for domestic use of a value exceeding EUR 750 and vehicles of a value exceeding EUR 50,000.[35] However, at the end of September 2022, the discussions on the EU's eighth sanctions package revealed that there was still a lack of consensus among member states on prohibiting imports of Russian diamonds into the European Union.[36] As these examples illustrate, geoeconomic measures can affect a very broad range of sectors, including consumer-oriented sectors. While certain sectors may succeed in obtaining carve-outs, evidently there is a strong case for businesses from all sectors to consider a wide range of possible futures and to prepare accordingly.

Risk management is not free. Companies rank risks, whether implicitly or explicitly, and are better prepared to handle some rather than others. The types of risks companies are most aware of depend on a combination of their own experience and external sources of information, from both industry and government, nationally and internationally. Given the limited resources and the need to prioritize, companies may not always be willing and able to plan for risks that seem fuzzy or remote. Public authorities can raise awareness of certain types of risks, or even mandate risk mitigation measures (as with cybersecurity, for example). However, from a corporate perspective, governments are also sources of revenue risks, at home and abroad. In the international picture, further complexity arises if one considers the interactions between states, including conflicts between them. In addition to the direct risks of property damage and loss of life resulting from use of force, states also compete in the realm of geoeconomics. In any case, the range of risks to revenues that European companies are beginning to face from 2022 onwards is broader, more complex and more fluid than at any time in recent decades. This is particularly true for geoeconomic risks.

35 Council Regulation (EU) 2022/428.

36 Brussels Times 2022.

Chinese trade sanctions against Lithuania: A failed attempt at dividing Europe

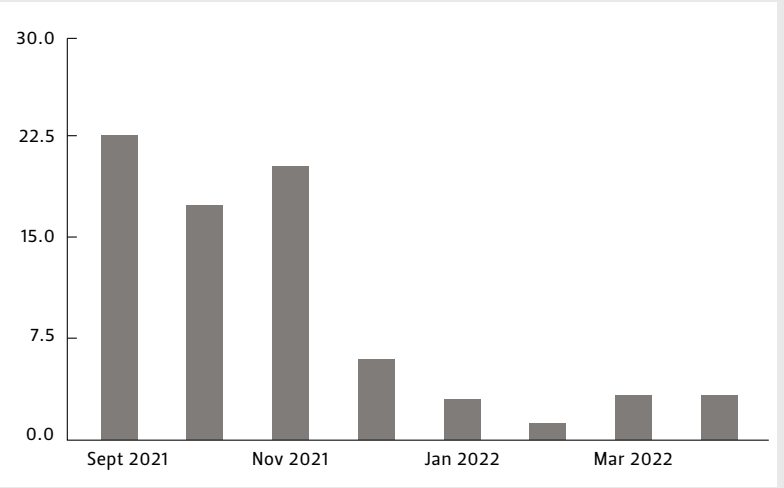


Figure 5: Lithuanian goods exports to China, EUR millions
Source: Eurostat database – international trade in goods

Starting from December 2021, China introduced unannounced on imports of goods. China's actions were motivated by diplomatic symbolism as Beijing objected to the *Taiwanese Representative Office in Lithuania* using the word "Taiwanese" instead of "Taipei", which Beijing usually tolerates for similar offices in other EU member states. [37] As a result of the embargo, Lithuania's monthly exports to China fell from around EUR 20 million to less than EUR 5 million (see Figure 5). The European Commission established that China's measures included "a refusal to clear Lithuanian goods through customs, rejection of import applications from Lithuania, and pressuring EU companies operating out of other EU member states to remove Lithuanian inputs from their supply chains when exporting to China".[38] Following these findings, the European Union referred the case to the World Trade Organization (WTO). China's actions against Lithuania were particularly troubling in that Beijing not only embargoed imports from Lithuania, but also sought to impose secondary restrictions by pressuring non-Lithuanian EU companies to remove Lithuanian inputs from their exports to China. While many companies feared being "shut out of China

37 Pitchers 2022.

38 European Commission 2022b.

completely" if they complained,[39] the European Commission's principled approach appears to have been successful in containing the dispute and defeating China's attempted "secondary sanctions" as broader EU exports to China remained largely unaffected.

• Armed conflicts	• National security risks from foreign direct investment in the home country	• Unfair competition in foreign countries due to hidden foreign government assistance
• Regional instability	• Risks due to restrictions on foreign direct investment in the home country	• Capital market restrictions
• Cyberattacks against companies	• Rising or new export risk insurance costs	• Import bans, embargoes and other import restrictions
• Physical attacks against companies	• Export subsidies in foreign countries	• Export bans or new export controls
• Critical national infrastructure failure	• Government audits and safety/security reviews in foreign countries	• Sanctions introduced by governments for political or geopolitical reasons against foreign persons, companies or industries
• Extreme weather events and natural disasters	• Local content requirements in foreign countries	• Techno-nationalism through anti-competitive use of technical standards
• Public health risks	• Arbitrary withdrawals of licences or authorisations in foreign countries	• Techno-nationalism through boycotts of foreign technology
• Intellectual property rights violations	• Unfair competition in foreign countries due to foreign state aid	• State-owned companies as competitors
• Industrial espionage		
• Reputational attacks and negative information campaigns		
• Macroeconomic risks		
• Market risks		
• Regulatory risks		
• Carbon border adjustment mechanism risks		

Table 4: IBRRM geoeconomic risk catalogue
Source: authors

What are the risks – geoeconomic and otherwise – that companies are most aware of, and what risks are they best prepared for? How do companies evaluate and assess different kinds of risks at this time? And how do companies take steps to raise resilience and acquire the ability to handle crises and shocks?

It is with these questions in mind that we developed this project's geoeconomic risk catalogue. The catalogue draws on relevant interdisciplinary literature and policy commentary. We also screened 45 annual reports from Finnish and Austrian listed companies for references to geoeconomic and other types of risks. In addition, we analyzed several national documents such as national security strategy documents and economic policy documents. This analysis resulted in our geoeconomic risk catalogue, which consists of a total of 30 risk categories, which deliberately encompass both geoeconomic and non-geoeconomic risks, as summarized in Table 4.

39 Miller et al. 2021.

Survey of corporate respondents

The risk catalogue served as the basis for the project's survey of corporate respondents. In the survey, respondents were presented with the risk catalogue and asked to rate each of the 30 risk categories according to three perspectives:

- **Relevance**, namely the significance of the risk category in relation to business objectives and business organization in general.
- **Impact**, namely the negative consequences to business objectives and operations, should the risk category materialize.
- **Preparedness**, namely how ready the respondent's company was to tackle the impacts that could be expected to occur, should the risk category materialize.

Respondents were asked to rate each risk category according to each of these three perspectives on a scale from 1 (lowest) to 4 (highest). Importantly, by multiplying the ratings for relevance with those for impact, a quantitative measure of risk could be estimated for each of the 30 risk categories.

2.3 GEOECONOMIC RISK MAP

These results were then processed to generate a geoeconomic risk map, which is a two-dimensional map of the average degree of preparedness and the average measure of risk for each risk category (see Figure 6).[40] The key findings can be summarized as follows:

- First, we highlight the **top three risk categories** in terms of risk level. These were cyberattacks, failure of national critical infrastructure and macroeconomic risks. These risks were important in terms of both relevance and impact. We also found that companies rated themselves as well prepared for these three risk categories. The first two categories have also been at the core of national security debates since the September 2001 terrorist attacks on the United States. These findings are thus in line with national security discussions and preparedness activities.
- Second, the top left quadrant of the risk map comprises a **hybrid set** of risk categories for which the estimated risk level was lower but for which self-assessed preparedness was relatively high. This diverse set of risk categories includes traditional macro-level risk categories such as public health risks and the risk of industrial espionage. This group also includes regulatory and market risks, as well

40 The risk map and its description constitute the "risk analysis" and "risk evaluation" stages according to ISO 31000:2008 (Figure 3).

as violations of corporate intellectual property rights (which may or may not be a geoeconomic risk, depending on the actors involved). Sanctions, local content requirements and export risk insurance costs can be regarded as geoeconomic risk categories. The same holds true for disagreements between countries on carbon border adjustment regimes, although we express a note of caution over how well corporate respondents could assess this last category of risk, given the ongoing evolution of policies on this topic.

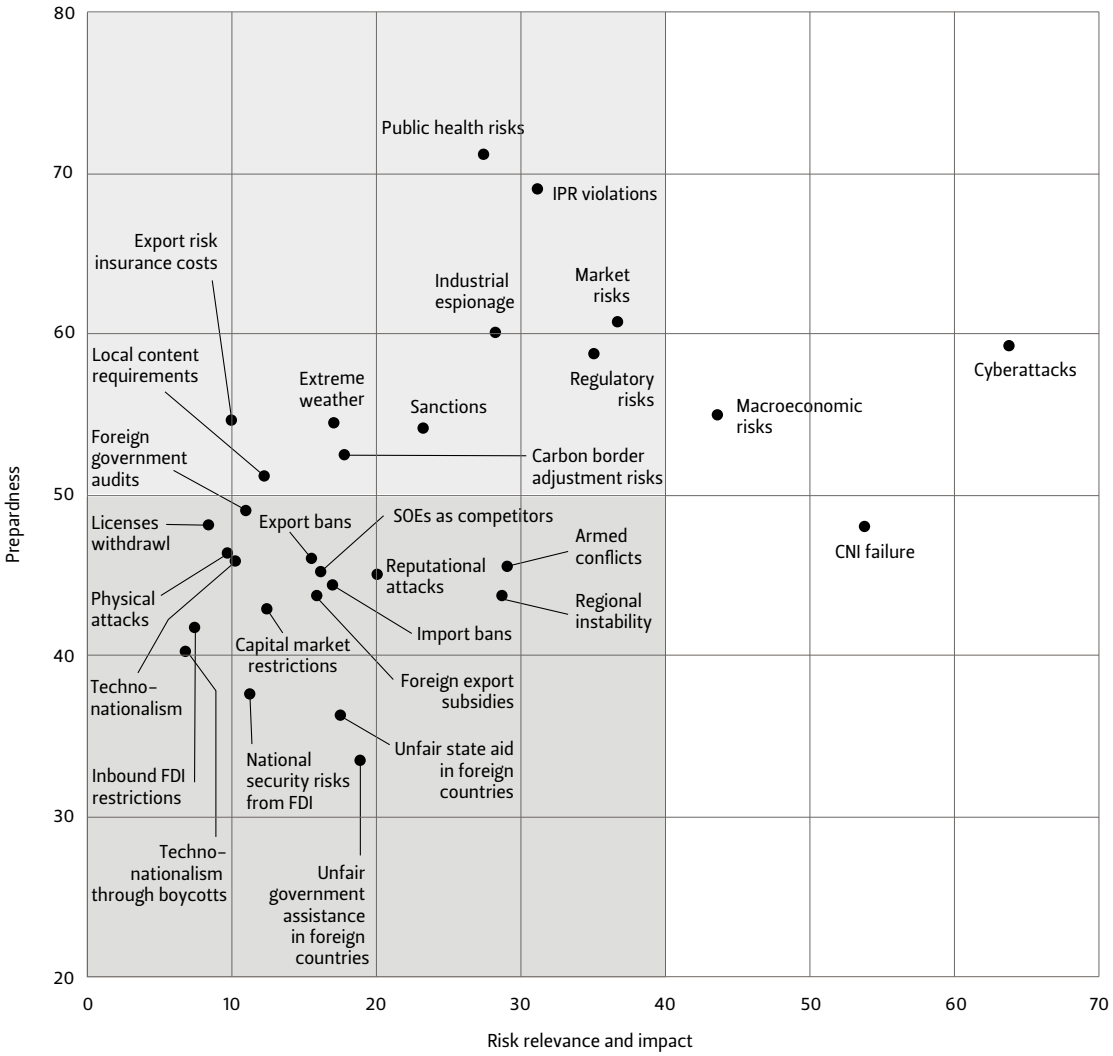


Figure 6: IBRRM geoeconomic risk map
Bottom left quadrant depicts risk categories with low risk value and low preparedness. Upper left quadrant depicts risk categories with low risk value but high preparedness. Quadrants on the right refer to risk categories with high risk values.
Source: authors

- Finally, the third group in the bottom left quadrant of the map is made up of risk categories that companies considered **less relevant** and for which they were also **less well prepared**. This is the most striking finding of the survey because this group includes geoeconomic risk categories that have dominated economic news headlines over the past three to five years, such as import and export bans, the rise of state-owned enterprises as competitors and national security concerns related to foreign direct investment (FDI). This suggests that companies may lack awareness of and preparedness for risk categories that have become – and will likely continue to become – more salient given the evolution of relations between states and the concomitant rise of geoeconomics.
- The seven risk categories for which preparedness was found to be the lowest were:
  - Unfair competition in foreign countries due to hidden foreign government assistance
  - Unfair competition in foreign countries due to foreign state aid
  - National security risks from FDI in the respondent's home country
  - Techno-nationalism through boycotts of foreign technology
  - Risks due to FDI restrictions in the respondent's home country
  - Capital market restrictions
  - Import bans, embargoes and other import restrictions.

Sector-specific findings

The survey results were also broken down by sector of activity, allowing for sector-specific insights regarding the highest- and lowest-ranked risk categories according to the three perspectives (relevance, impact, preparedness). These insights are summarized below.

- **Construction**
  Cyberattacks and macroeconomic risks were the top two risk categories in terms of both relevance and impact, followed by sanctions (in terms of relevance) and critical national infrastructure failure (in terms of impact). In terms of preparedness, unfair competition in foreign countries due to hidden foreign government assistance and due to foreign state aid were the two risk categories for which companies reported being the least prepared. These results are

consistent with the cyclical nature of the construction sector, as well as with its inherent exposure to public sector decisions in relevant markets of operation.

- **Transportation**
  Cyberattacks and armed conflict were the top two risk categories in terms of both relevance and impact. This result is consistent with the fact that transportation depends on digital services and access to countries of origin, transit and destination. The risk categories with the lowest levels of preparedness were capital market restrictions, national security risks from FDI in the home country and local content requirements in foreign countries. This may be seen as partly surprising: the highly internationalized nature of the transportation equipment sector could have driven this sector to develop higher preparedness for the geoeconomic risks in question.

- **Basic materials**
  Critical national infrastructure failure and macroeconomic risks were the top two risk categories in terms of both relevance and impact. Seeing as the sector is materials- and energy-intensive, critical infrastructure, notably energy supply, is inherently crucial. The sector also has long investment cycles and a sensitivity to economic cycles. As with construction, the top two risk categories in terms of low preparedness were unfair competition on foreign markets due to hidden foreign government assistance and due to state aid.

- **Commerce**
  Commerce followed most other sectors in terms of the key geoeconomic risks by relevance and impact, but in addition to transportation, it was the only sector for which local content requirements in foreign countries was a low-preparedness category. National security risks from FDI in the home country came second in terms of low preparedness. This may be due to the fact that so far, this sector has not been a major focus of discussions on security risks from FDI, such that there may be lack of experience in the sector on this particular topic.

- **Financial services**
  Market risks were the top category in both relevance and impact. It was the only sector for which this was the case, but the result is consistent with the sector's business model. Cyberattacks ranked second by relevance and third by impact: the sector has been a major target of malign cyber activities since the 1990s. Regulatory risks were ranked third in terms of relevance, which may be explained by the link between changes in regulations and revenue risks. Categories with low preparedness included regional instability and techno-nationalism through boycotts of foreign technology.

- **Information and communication technology (ICT)**
  Cyberattacks and critical national infrastructure failure were the top two risk categories in terms of both relevance and impact. Intellectual property rights violations were a highly ranked category in terms of relevance, and industrial espionage was ranked highly in terms of impact. This very well reflects the technology-intensive nature of the sector. As risk categories with low preparedness, respondents identified national security risks from FDI in their home country, unfair competition due to hidden foreign government assistance and techno-nationalism through boycotts of foreign technology. The identification of the last as a category with low preparedness may seem somewhat surprising as it has been a salient issue for many years.

Screening of foreign direct investment in the EU

While some individual EU member states have had security screening procedures in place for foreign direct investment (FDI) for many years, it was not until 2019 that the first EU-wide framework was adopted through Regulation (EU) 2019/452. In September 2022, the European Commission published its second annual report on the implementation of the regulation.[41] While the regulation does not require member states to establish a national screening mechanism, the European Commission encourages all member states to do so, and there is an element of peer pressure on national governments to move forward. In June 2022, only Bulgaria and Cyprus had "no publicly reported initiative underway" to set up a screening mechanism.

41 European Commission (2022a).

The regulation offers a significant degree of flexibility to member states, but it explicitly authorizes (and, in practice, encourages) national governments to consider screening and potentially restricting investments that pertain to critical infrastructure (whether physical or virtual), critical technologies and dual-use items (including artificial intelligence, robotics, semiconductors, cybersecurity, aerospace, defence, energy storage, nanotechnologies and biotechnologies), the supply of critical inputs (including energy, raw materials, food), access to sensitive information, or the freedom and pluralism of the media. Member states are also encouraged to consider whether the foreign investor is controlled by the government, including state bodies or armed forces, of the country of origin of the investment.[42]

In the case of Italy, for example, screening legislation has been in place since 2012. However, by March 2022, only six investment deals had ever been blocked. While five of the six cases involved Chinese investors, there is evidence that investment screening has been insufficient. In March 2022, Italy had to annul the sale of Alpi Aviation, [43] a military drone technology company, which had been acquired by Chinese investors in 2018 without the knowledge of the Italian Defence Ministry.[44]

2.4 HOW CORPORATIONS DEAL WITH GEOECONOMIC RISKS

In addition to the geoeconomic risk map (Figure 6) and the sector-specific findings based on the survey, the IBRRM project also sought to generate more detailed insights[45] based on case studies of selected companies.[46] Table 5 summarizes the main findings of the semi-structured interviews that were conducted with the representatives of seven companies. We summarize the key findings as follows:

- **Evolution of the risk picture**
  Our respondents believed that the corporate risk landscape had become more challenging. Companies feel that certain foreign markets have become no-go areas due to sanctions, which increase the

42 Regulation (EU) 2019/452 of the European Parliament and of the Council, Article 4.

43 Fonte et al. 2022.

44 Waldron 2021.

45 A total of seven personal interviews were conducted, with each interview taking 90 to 120 minutes.

46 This section combines elements of "risk evaluation" with "risk treatment" as envisaged in ISO 31000:2018 (Figure 3).

risk of losing assets and investments and create reputational risks. There is a growing interest in better understanding the effects of sanctions regimes and the conditions that might prompt governments to adjust them. In addition, climate policies are seen as a new source of geoeconomic risks, because these policies could be instrumentalized by foreign governments and competitors.

- **Geoeconomic risk appetite**
  We define risk appetite as the "explicit, updated, widely known" and strategy-related level of risk a company is willing to take.[47] Our estimation of the companies' geoeconomic risk appetite is mixed. Although businesses readily acknowledged the existence of general risk awareness, the true level of their geoeconomic risk appetite remained fuzzy. This could result from methodological challenges as geoeconomic measures can affect business models directly (e.g., export bans) or indirectly (e.g., reorganization of supply chains due to foreign dependence risks). Without a proper understanding of these consequences, it is difficult to generate a holistic risk picture and determine which risks are deemed by businesses to be acceptable or unacceptable.

- **Risk management systems**
  Establishing risk management systems has become standard corporate practice, and in most cases, these risk management systems are driven by the reporting requirements of the chief financial officer. However, there are two challenges. First, it is hard to properly gauge the role of geoeconomic risks in relation to other corporate risks and how businesses deal with potential trade-offs. Second, the financial perspective on risk management is essential, but it might no longer be sufficient as companies might be willing to accept financial losses in return for other advantages such as political support. Existing ERM frameworks might therefore need to be critically reviewed because companies need more than financial benchmarks to distinguish between acceptable and unacceptable geoeconomic risks.

47 Rice and Zegart 2018, 129.

- **Risk mitigation**
  Geographic diversification of suppliers, markets, components and technology providers was considered the state of the art to aim for across the seven case studies. However, in the current international context, certain key considerations apply:
  - The desirable degree of diversification has yet to be reached, it will take time to achieve it, and the current war in Europe and global security of supply issues both drive the need for it while also making its short-term attainment more difficult.
  - The options to diversify are more limited in certain industries (e.g., oil and gas) than in others.
  - Governments need to be careful not to overstimulate companies with incentives to diversify because this could prove to be economically inefficient in a broader or longer-term perspective. In addition, it is not entirely clear what state support measures to promote economic security may be deemed legitimate in the context of World Trade Organization (WTO) commitments.

- **Investor relations**
  Although not all our case study respondents touched upon this issue, those who did affirmed that investors and supervisory board members want companies to outline how they deal with geoeconomic issues. To complement the seven case studies, we also analyzed the annual reports of 45 listed companies from Finland and Austria to gain a better understanding of the existing level of geoeconomic risk reporting to financial stakeholders. Our general finding was that many risk reports are so generic that it is hard to understand how individual geoeconomic risks affect corporate activities. Consequently, companies should develop a more granular and dedicated vocabulary for external stakeholders to better understand how geoeconomic risks might affect business prospects. In so doing, C-level decision makers might want to consider spending more time explaining their company's specific position in earnings calls with financial analysts, general corporate statements about geoeconomic topics and communication with the broader public.

- **Public–private and private–private partnerships**
  Stepping up public–private interaction in response to political decisions that affect business prospects seems logical, but our findings are mixed. While some companies consult with public authorities

at home and abroad, others do not. One case study respondent considered engagement with public authorities to be a potential reputational risk. This finding is a reminder that public and private sector actors can – for various reasons – be reluctant to engage with each other. To overcome such reluctance, the characteristics of each industry will need to be considered when designing a framework that enables public–private interaction on geoeconomics.

New forms of private–private interaction on geoeconomic risks are also clearly relevant to deal with supply chain risks, for example. On this issue, our findings are mixed, with some companies reporting dialogue with other corporations (e.g., to enhance their understanding of specific risks), while others categorically ruled out cooperation with others for reasons of competition. These results suggest that trust will be a key issue to create an environment in which C-level decision makers from different corporations could feel (relatively) at ease to exchange views and engage in mutual identification of lessons for the future.

	Company 1 (Electronics)	Company 2 (Mobility)	Company 3 (Telecommunications)
Most important (geoeconomic) risks	· China · Sanctions · War against Taiwan · Cybercrime · Foreign exchange rate risk · Inflation	· War · Inflation · Security of supply (and shortage of critical components) · Covid-19	· Sanctions against countries that are critical as markets to be served and providers of technology and products · Sanctions against technology suppliers · Supply chain interruptions and sourcing
Risk evolution	· Ups and downs · Risk landscape has become tougher	· Different risks materialise at the same time · Lower inflation in China makes it increasingly difficult to pass on price hikes in Europe · More aggressive competitors, also from China · CO_2 transparency requirements are an increasing concern · Significant and unresolved issue: post-Ukraine war sanctions – how long will these sanctions last?	· Risk landscape has become much more challenging
Specific regional risks	· Not discussed	· Not discussed	· Regional diversification to avoid critical dependencies
Corporate activities most affected	· Production · Supply chain management (SCM) · Procurement	· All-encompassing	· Supply chain interruptions affect sourcing
Geoeconomic risks vs. other risks	· Geoeconomic risks constitute a strategic risk; focus is on operational risk · Company 1 tries to balance strategic and operational risk	· Not addressed	· Not addressed
Risk appetite	· Company has a dedicated process to define its risk appetite, but geoeconomic risk appetite has not been defined · Process details not provided	· Company develops investment goods. Given the long product life cycles, the company needs to master risks	· Four-part score to assess risks: averse, cautious, open and hungry · Company has defined "zero tolerance" risks such as information security · Currently, company 3 takes a more systematic approach to assess and handle geopolitical risks; in the past, these risks have been addressed on an "as needed" basis

Table 5: Main case study findings
Source: authors

Company 4 (Energy)	Company 5 (Digital industry)	Company 6 (Telecommunications)	Company 7 (Energy)
• Sanctions • Supply chain and inventory management risks • Seasonal risks	• Local content requirements and partner selection • Increasingly tough competitors • Local sovereignty requirements • Supply chain risks and stability/integrity of supply chains • Natural hazards • Shortage of IT experts • Price risks	• Geopolitics • Regulatory risks • Anti-corruption • Sanctions • Trade regulation • Taxes • National security • Competition law • Export controls • Cybersecurity	• Geopolitics • Sanctions • Supply chain risks • Macroeconomics • Global economic slowdown • Human rights • Sustainability
• Sanctions: stable evolvement • Supply chain risks have become more challenging • Transparency requirements have drastically increased, pushed by legislators as well as investors	• Situation is much worse than in the past • Suppliers of critical components went out of business due to price fluctuation (e.g., energy, components)	• Geopolitical risks and protectionism on the rise • Geopolitics is becoming a criterion for customers choosing vendors • Russo-Ukrainian war forced an exit	• Ongoing sanctions risk concerning Iran and Venezuela • China-related risk is changing from human rights and sustainability to geoeconomics
• Some countries have become no-go areas	• China is of limited relevance • Local availability of infrastructure shapes strategy in different regions • Local content demands vary, but the company has trusted partners in one production country to mitigate the respective risk	• China	• Not addressed
• SCM • Sales • Operational compliance, bookkeeping and PR	• Not addressed	• Production • Research and development • SCM	• SCM
• Geopolitical risks are paramount	• Not addressed	• Enterprise risk management includes geopolitical risks	• Not addressed
• No formal definition • Compliance policy used to shape corporate risk policy • There is a written set of rules, but no general policy. Ambition to introduce the respective policy within the next two years • Code of conduct is public	• Co-CEO and head of international business decide on market entries abroad and thus shape the risk appetite of company 5	• Not formally defined	• Not formally defined

	Company 1 (Electronics)	Company 2 (Mobility)	Company 3 (Telecommunications)
Risk assessment process	• Half-year assessments of medium and long-term risks • Quarterly assessments of short-term risks (one synchronised with the budget planning process, three synchronised with forecasts) • Key account managers and sales directors on the spot are responsible for assessing market risks • Enterprise risk management adopts a broader (more holistic) view and oversees the production of a common risk map	• Synchronised with financial mid-term planning • Headquarters has not set specific reporting requirements	• Risk assessment is synchronised with the overall budgeting and planning processes • Quarterly reports to the board of directors and supervisory board; right now, the schedule is bi-monthly • More detailed discussions with the supervisory board to explain what is going on and how company 3 might be affected; discussions also offer an opportunity to elaborate on hypotheses and scenarios • Cyber risks are also discussed with the supervisory board
Processes, methods and instruments to assess geoeconomic risks	• Not addressed	• Each commodity group gets an overall risk score based on criteria such as (1) risk of depending on a monopolist, (2) quality risk, (3) planning risk, (4) price behaviour, (5) market risk and (6) financial situation of a supplier/partner	• Company uses expert groups to assess certain risks such as cyber risks and macro risks • Central assessment of macro risks and supplier risks provides guidance for other corporate functions
Risk management tools	• Not addressed	• Corporate supervisor looks at critical monopolists and critical risk factors that could be detrimental for the company • Developed real-time dashboard to illustrate daily operations with a focus on single suppliers and single commodity groups	• Not addressed
Use of external sources	• Yes, but not specified	• Partly yes, as consultants are being contracted	• Case by case, for example, credit ratings, compliance databases or ESG
Board responsibility	• CFO	• Overall risk scores and financial risks reported to the CFO • All other risk scores reported to the heads of business units	• CFO as the focal point • Board of directors gets regular briefings as each member has a different perspective on the risks affecting the company
Specific budget for geoeconomic risk assessment	• No	• Not addressed	• No

Table 5: Main case study findings
Source: authors

	Company 4 (Energy)	Company 5 (Digital industry)	Company 6 (Telecommunications)	Company 7 (Energy)
	• Compliance is in charge • Company has adopted a reactive risk management approach • Semi-weekly and weekly reporting cycle • Annual risk reporting	• Market entry decisions – as well as the respective risk analyses – are based on personal experience • High cultural affinity with target countries and long-time experience in doing business in the target regions	• Enterprise risk management framework covers the overall governance of risks in the company • Risk council reviews of both strategic and operational risks • Global leadership team reviews • Board reviews • Sarbanes-Oxley reporting (compliance) • Risk management covered in the annual report	• Enterprise risk management framework with a formal cycle of review and reporting
	• Company 4 uses an internal rating score card • Experience of the company's experts is key in assessing risks • Overall, the risk management unit has been significantly professionalised, internal resources have been beefed up, and company 4 also contracts external services	• See above	• Within the ERM framework • No specific category for geoeconomic risks	• Within the ERM framework
	• Would be useful in relation to qualitative assessments, classification of risks and foresight, in particular • However, will be extremely difficult to set up. Major hurdle: reluctance of companies to share information	• Not addressed	• Multiple, but not specified	• Not addressed
	• Not discussed, but see above (contracting services)	• No, no need for further information sources right now	• Geopolitical risk reporting • Bespoke reports	• Yes (risk information)
	• CFO	• Co-CEO (with regard to market entry decisions)	• CFO (technically the CEO is ultimately responsible)	• CFO • Strategic risk technically owned by the CEO • Many functions participate
	• No	• Not addressed	• No	• Not addressed

	Company 1 (Electronics)	Company 2 (Mobility)	Company 3 (Telecommunications)
Mitigation measures	· In 2021, company 1 decided to establish a new plant in a different country to advance diversification	· Insurance for certain risks under discussion	· Focus on efficiency has changed: company 3 is ready to shoulder costs if this enables continuity of operations · Stockpiling of components · Electricity purchasing agreements to deal with fluctuating energy prices · Georedundancy to create cross-regional digital infrastructure clusters · Nearshoring of critical tasks (e.g., software development) · Business continuity management
Investor relations	· Investors ask about risks related to specific countries · Close interaction with subsidiaries; information is also shared with investors	· Other companies are interested in whether company 2 continues to operate in Russia	· Financial analysts are quicker in assessing how (geoeconomic) risks could affect the company · Most often, the focus is on the financial consequences of risks: what is the value contribution of market xy to the overall result?
Added value of information provided by public authorities	· Situational assessment provided by embassies would be most useful (could be coordinated at the European level)	· Not addressed	· Not addressed

Table 5: Main case study findings
Source: authors

Company 4 (Energy)	Company 5 (Digital industry)	Company 6 (Telecommunications)	Company 7 (Energy)
· Take a risk · Change the existing approach · Decide not to take a risk	· Stockpiling of critical components is a key mitigation instrument · Business continuity management important given natural hazards abroad · Sovereign definition of product requirements that need to be met and certified help to mitigate risks, too. Sometimes, however, sovereign requirements may collide with the company's multi-sourcing strategy · Company conducts supplier audits to issue supplier certificates · Cooperation with trusted and certified partners that can provide different components, which mitigates the risk of critical dependencies · General policy not to accept certain critical components from China	· Market and supply chain diversification · Business continuity plans · Crisis management	· Market and supply chain diversification · Business continuity management
· Geoeconomic risks are very important · Risk information is part of the company's annual report (but the company hardly ever talks about risk mitigation solutions in the public) · Overall, investors and rating agencies want more information about geoeconomic risks and risks in general	· Not addressed	· Not addressed	· Not addressed
· Very sceptical about information provided by authorities as authorities do not run businesses; this holds particularly true for any kind of public advice on how to mitigate specific risks	· See below	· Some useful information in relation to the Russo-Ukrainian war and sanctions	· Valuable due to the company's formal role in national security of supply

	Company 1 (Electronics)	Company 2 (Mobility)	Company 3 (Telecommunications)
Public–private cooperation	· Close cooperation with local authorities; the focus is on daily business rather than the assessment of geoeconomic trends and risks	· Unknown to the interview partner	· Authorities: cooperation on sanctions in view of obtaining export licences · Chamber of commerce: consolidated assessment of sanctions · Internal focus only: supply chain issues, operationally critical infrastructure components, energy
Private–private cooperation	· Not addressed	· War: exchange of views with other companies · CO_2: cooperation to find common solutions	· Competition prevents direct interaction · Supplier relationship management used to interact with suppliers
Miscellaneous		· Risk foresight "tool" would be very helpful · Could provide a kind of common baseline in view of what might become relevant for companies; could provide a basis to compare internal assessments with information provided based on the "tool" · 10-year focus would be helpful	

Table 5: Main case study findings
Source: authors

Company 4 (Energy)	Company 5 (Digital industry)	Company 6 (Telecommunications)	Company 7 (Energy)
· Currently a non-issue · Selective interaction on issues like capital market regulation and export control	· Well-functioning cooperation with a business association, which is most helpful in (1) assessing local risks and (2) identifying local partners · Company has never considered talking to the Ministry about (geoeconomic) risks · Close cooperation with the Ministry is considered to be a reputation risk	· Consults with authorities, acts independently	· Close cooperation due to formal responsibilities in national security of supply
· Yes, exchange with companies operating in the same industry · Business associations are helpful to organise and leverage lobbying power	· Not addressed	· Not addressed	· Not addressed
		· Russo-Ukrainian war raised geoeconomics to the corporate agenda	· "Radical transparency" between governments and business would help in addressing geoeconomics · Sharing of information is the key, also between companies

2.5 INTERNATIONAL BUSINESS RISK AND RESILIENCE MONITOR: VISION

Drawing on all the elements described in the previous sections, we now present our proposed vision for an international business risk and resilience monitor (IBRRM). As we have argued, there is a need for better awareness of and preparedness for geoeconomic risks on the part of both private sector and public sector actors. As we have also argued, the nature of the geoeconomic challenge naturally calls for a new dialogue and mutual understanding between businesses and governments. In a very practical sense, we have shown how data collected from corporate entities can help to map the territory, identify risk categories and rank or rate them in terms of relevance, impact and preparedness. Practical visualization tools such as the risk map presented above are evidently useful. To go further, we envisage a broader set of methods, processes and tools which could be used collaboratively to accumulate knowledge and data, facilitate scenario analyses and help build a better common understanding of present and future challenges for a relevant set of stakeholders. Therefore, the IBRRM, when fully developed, should be a collaborative tool embedded in a public–private framework to advance common activities that benefit shared economic security needs. To that end, our vision is that the IBRRM should:

- Advance mutual understanding of the current economic security situation, as well as alternative future development paths, based on various scenarios of relevance for economic security
- Provide information about current (and prospective) risks, likely impacts and perceived preparedness/readiness in dealing with these risks
- Advance public and private understanding about the interplay of relevant risk categories and key trends likely to shape their future evolution
- List major national and international mitigation measures that are either under consideration or already enacted in response to geoeconomic risks – including a better understanding of the impacts of certain geoeconomic actions (e.g., the impacts on the national economy of sanctions enacted by a third country)
- Provide a comprehensive data space or data repository that facilitates access to relevant information by all relevant decision makers.

To accomplish these tasks, the IBRRM could provide users with core and supporting functionalities as illustrated in Figure 7. The core functionalities would cover four aspects:

- **Risk map**
  The risk map would offer a window to describe and assess each risk category individually and to produce an aggregate overview of all the individual risk assessments. As the IBRRM is meant to support economic security, the risk assessment functionality could be expanded by including specific extra elements, such as sector-specific risk assessments for different risk categories and time horizons; estimates of the economic relevance of each risk category, including expected damage if the risk materializes, and the costs of investments undertaken to advance preparedness for the same risk category.
- **Geoeconomic action tracker**
  The geoeconomic action tracker would provide a meta-level consolidation of existing geoeconomic actions taken at national and international levels, as well as countermeasures adopted by states that are systemic rivals. For that purpose, the tracker would tap into specialized databases to create a new one-stop-shop resource for users. In addition to describing each single action and indicating the entities affected by these actions, the tracker could also track and illustrate media sentiment related to specific geoeconomic developments because public sentiment may in some cases be of particular relevance.
- **Impact assessment**
  The impact assessment functionality would look at the economic consequences of geoeconomic policy decisions. The primary focus would be on the impact on companies originating from nations that have adopted a specific action (e.g., EU nations adopting sanctions against Russia) or have been targeted with geoeconomic action by foreign governments (e.g., companies from EU nations targeted by Chinese economic coercion). The overall purpose of the impact assessment would be to help users gain a better understanding of the vulnerabilities of their own corporation, industry or national economy, because these vulnerabilities will in turn drive an individual organization's risk appetite, as well as the ability of governments and businesses to withstand geoeconomic pressure.

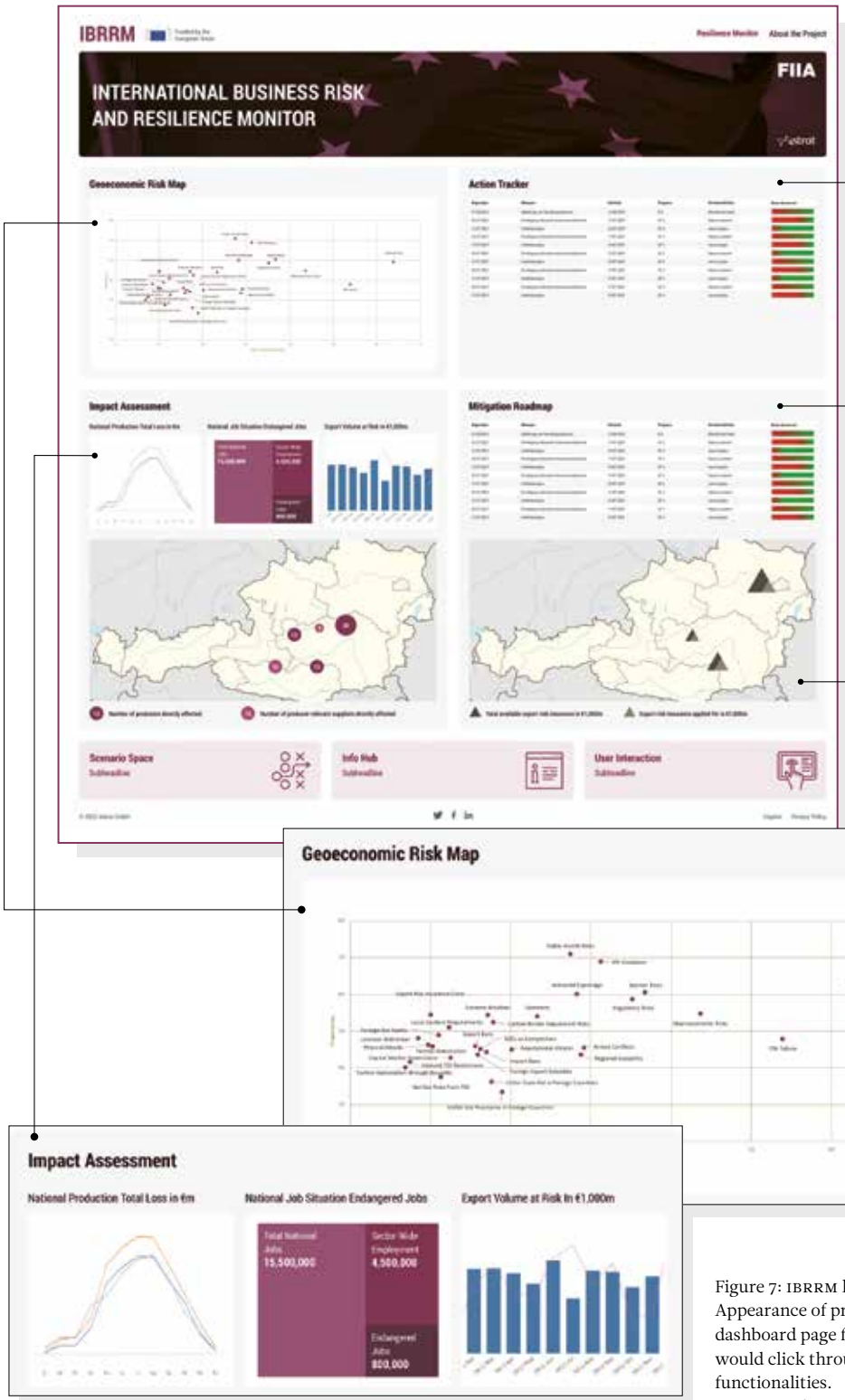
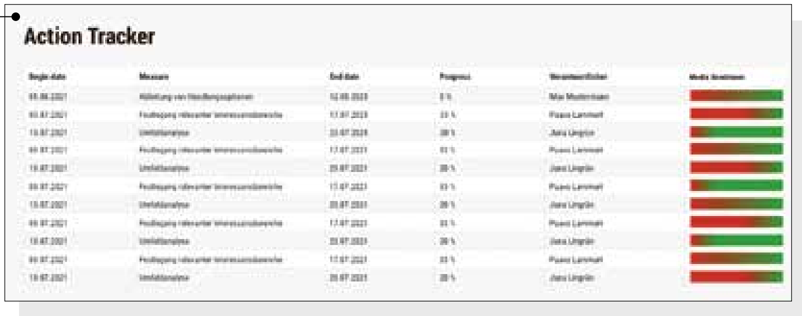
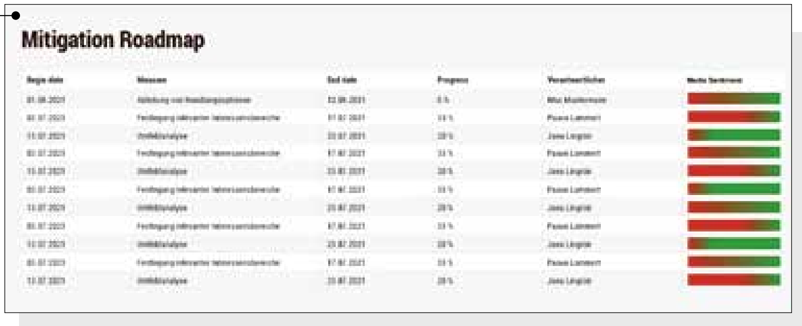
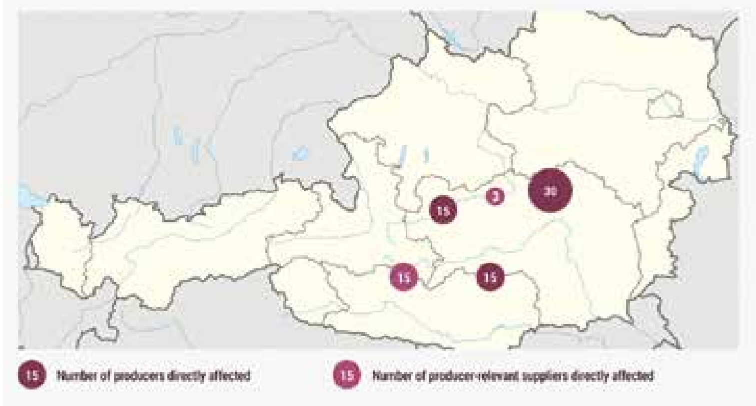
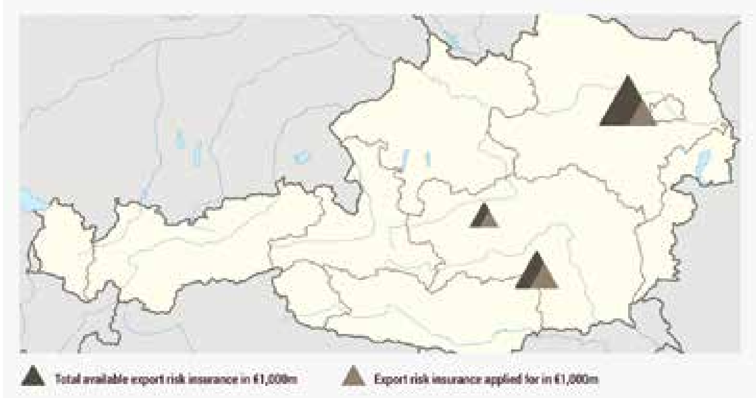


Figure 7: IBRRM key functionalities
Appearance of proposed IBRRM dashboard page from which users would click through to specific functionalities.
Source: authors


Action Tracker


Mitigation Roadmap


15
3
30
15
15
15
15
Number of producers directly affected
15
Number of producer-relevant suppliers directly affected


Total available export risk insurance in €1,000m
Export risk insurance applied for in €1,000m

- **Risk mitigation radar**
  The risk mitigation radar would give an overview of what has been done to dampen the consequences of geoeconomic measures taken by home or foreign governments. The risk mitigation radar could focus on financial resources committed to supporting national companies that are directly affected. Depending on the available data, users could, for example, visualize different aspects such as products, companies or geoeconomic instruments of interest to better understand the set of companies affected by geoeconomic actions.

In addition, the three suggested supporting functionalities would:

- Provide a collaborative scenario development space to complement the risk map, consider alternative future development paths and promote mutual understanding of geoeconomic trends among public and private stakeholders
- Offer users an information repository containing all the sources used to conduct risk assessments and define scenarios, as well as key official documents such as government decisions and entity lists
- Give users options to create various user fora and offer different modes of interaction to facilitate direct communication and online collaboration.

/ 3

3 RECOMMENDATIONS

This report has provided an advanced concept for the International Business Risk and Resilience Monitor (IBRRM) to be used as a collaborative tool in support of public–private cooperation. In this section, we outline our final recommendations. Recommendations 1 to 3 address the setup under which the tool would be used. Recommendations 4 to 6 address broader flanking policies or actions to advance geoeconomic understanding.

RECOMMENDATION 1: ESTABLISH STRATEGIC-LEVEL PUBLIC–PRIVATE DIALOGUE

Governments increasingly intervene in business practice, while companies can support or undermine government objectives. Synchronizing the activities of both parties thus requires a new kind of public–private dialogue at the strategic level. Regular gatherings between ministers and executives of leading national companies from critical infrastructure and strategic technology sectors, for example, should become the norm. Together, they should review the geoeconomic activities of strategic competitors and assess how to join forces in repelling rival action and advancing their own interests. The IBRRM would serve as a most useful tool to inform this debate as it provides insights into corporate risk assessment as well as the consequences of economic statecraft on business.

However, public–private cooperation needs to be embedded in public–public and private–private dialogue about how to prepare for the fallout of assertive geoeconomic competition. On the public–public side, regulatory agencies should strive to develop a mutual understanding of how regulatory action in one sector might affect the regulatory requirements in dependent sectors. Private–private dialogue, on the other hand, refers to the idea that companies involved in the same supply chain could step up joint efforts to stabilize these supply chains against external geoeconomic forces, engage in joint activities to identify critical components or provide mutual backup in the event that production facilities go offline.

Public–private dialogue could start with a focus on one or two topics at a time to establish trust and create an atmosphere in which every participant feels at ease to share information not normally discussed in

public. Such a discussion will need to provide added value for everybody involved. Public sector partners need to understand that dialogue really is a two-way street that must also benefit the private sector rather than only meeting public sector information requirements. Private sector partners, in return, need to balance the requirement of treating corporate information restrictively with the benefit of gaining access to otherwise non-accessible government information (see also recommendation 3). Given the existing reluctance to share information, think tanks might play an important role as mediators and facilitators.

Most importantly, these dialogues should not stop at national borders. This project has brought Finnish and Austrian stakeholders together to map geoeconomic risks for companies. Bilateral cooperation sheds light on diverging risk assessments and provides a first opportunity to better understand how elements of the risk preparedness approach in one country could inform partner activities. These kinds of cross-border activities become more important in the future. The European Commission, for example, requires nations to assess the potential cross-national impact of foreign direct investments on security and public order and has introduced a respective cooperation mechanism.[48] The information needed to conduct this assessment could be included in a future IBRRM solution.

Public-private dialogue with international partners needs to be designed carefully. Western nations might see a need to step up dialogue exclusively among like-minded partners that share similar value sets. This political preference, however, might run counter to existing corporate supply and value chains that are very likely to also include corporate partners from nations with diverging political regimes. Inviting these partners might be extremely relevant from a corporate perspective, whereas political preferences might prevent their inclusion. This underlines the delicate balance that public and private sector partners need to strike.

RECOMMENDATION 2: COMMISSION REGULAR GEOECONOMIC RISK ASSESSMENTS

Public and private stakeholders benefit from a mutual understanding of the relevant risks and their impact. National governments should thus strive to commission regular assessments of the geoeconomic risks most pertinent to national companies.[49] These geoeconomic risk maps would complement existing national security risk maps. These assessments

48 Regulation (EU) 2019/452 of the European Parliament and of the Council, Article 8.

49 See also Wigell et al. 2022, 19–20.

could also entail joint assessments with regional partners to help advance regional approaches in ensuring security of supply, for example.

Nations have set up various preparedness regimes and delineated tasks and responsibilities between public and private sector stakeholders. Given the need for holistic responses to geoeconomic challenges and close interagency interaction, a country's premier office – e.g. the Prime Minister's Office in Finland or the Chancellery in Austria – would be most suited to commission such assessments. The implementation could be delegated to a team consisting of the most relevant government agencies and business associations as well as leading research institutes. The last would provide scientific input and ensure the setup of an institutional memory, while the first two would facilitate access to key stakeholders and provide essential input.

These new geoeconomic risk assessments should become a standard item on the public–private meeting agenda. This would provide much-needed visibility and draw attention to the most pressing needs to be addressed.

Moreover, regular geoeconomic risk assessments would also provide ample opportunities to look into future developments by, for example, engaging in scenario analyses and joint discussions on the strategy options emanating from these scenarios and their likely consequences. This perspective would also offer public and private foresight entities opportunities to contribute towards a well-informed geoeconomic debate.

The frequency and thematic scope of the proposed geoeconomic risk assessments are to be discussed. Given the fast-paced developments of the recent past, publishing such an assessment annually might not be adequate to capture their dynamics. Instead, these reports could appear on a quarterly basis in line with the regular reporting cycles of stock-listed companies. Whereas quarterly reports could be used to take the pulse of private sector experts, annual reports could offer an opportunity to look at broader trends and reflect on medium- to long-term scenarios and policy options. In addition, annual reports could also be used for thematic breakdown analyses of specific regions, industry sectors, and technology and market segments, for example.

RECOMMENDATION 3: PROVIDE A FRAMEWORK FOR GEOECONOMIC INFORMATION EXCHANGE

Exchanging information about geoeconomic challenges is essential for public–private interaction to work properly. Specific data, however, may be classified by public and private stakeholders. Governments therefore

need to ensure with regulatory action that information can circulate without restrictions among qualified recipients. This is important as existing regulation and legislation is often driven by sector-specific requirements, whereas geoeconomic risk assessments require a cross-sectoral approach. Consequently, regulatory authorities should join forces with business associations to verify existing frameworks in view of possible stumbling blocks as well as gaps that need to be filled. In this regard, the existing information exchange practice established to advance critical infrastructure protection and cybersecurity, for example, could serve as a useful blueprint.

Moreover, leading business associations should take the initiative and look at the required framework for direct business-to-business interaction. These associations could also provide the trusted environment for exchanges among company experts, for example.

RECOMMENDATION 4: ADVANCE EXECUTIVE GEOECONOMIC PROFICIENCY

Awareness raising is essential to prepare public and private executives for today's geoeconomic environment. Executive leadership courses are one building block to improve geoeconomic proficiency.

These courses need to shape a joint understanding of the geoeconomic practices strategic competitors are using to understand the vulnerabilities and need for action.[50] Case studies shedding light on how companies operating in different market segments deal with their respective challenges would be as important as in-depth analyses of public sector decision making related to the use of geoeconomic instruments.

How to best organize these courses very much depends on the overall national setup. Finland's National Defence Courses[51] and Austria's *Strategischer Führungslehrgang*[52] stand in the tradition of engaging public and private sector actors in more general national security introductions. Other EU member states offer similar courses. Existing courses could be expanded to address the interplay between geoeconomics, national security and corporate development. Moreover, existing general management courses offered by management universities could be complemented with foreign and security policy modules as well as specific modules dealing with geoeconomics from a corporate perspective. Whatever the preferred

50 As discussed in recommendation 1, these courses could also include partners from abroad.

51 See https://maanpuolustuskorkeakoulu.fi/en/national-defence-courses.

52 See https://stratfuelg.gv.at/.

approach, it would be important to have harmonized strategic guidelines that outline the learning and knowledge transfer outcomes to be achieved with C-level education on geoeconomics.[53]

The IBRRM could provide a collaborative information basis to underpin these courses and share information among participants in the aftermath. The regular geoeconomic risk analyses would serve as an additional input to these courses as they would highlight how the geoeconomic risk picture evolves over time.

RECOMMENDATION 5: CONSIDER TRANSPARENCY AND COMMUNICATION REQUIREMENTS RELATED TO GEOECONOMICS

Companies report on corporate risks based on different requirements. However, many risk reports are so generic that it is hard to understand how individual geoeconomic risks affect corporate activities. Business associations and member companies should take the lead and assess how corporate communication – and investor relations in particular – can meet the growing information need of investors and the informed public audience concerning the impact of geoeconomic developments on corporate activities.

This aspect becomes more pertinent as many companies already engage in sustainability reporting. Today, sustainability reporting focuses on environmental, social and governance criteria. However, sustainability is also endangered by geoeconomic risks that affect the availability of technologies, cut off the provision of key raw materials or subsidize the development of products in a way that is detrimental to good climate protection practice. This is why sustainability reporting should be broadened to include geoeconomic risks as well.

RECOMMENDATION 6: CONSIDER THE ROLE OF INCENTIVE-BASED REGULATION IN PREPARING FOR GEOECONOMIC RISKS

Incentive-based regulation uses carrots and sticks to prompt changes in individual behaviour. It has been one instrument used to advance environmental regulation based on market principles. The same idea could be

53 These courses could also be tailored to address the needs and availabilities of different target groups; for example, by limiting C-level courses to two days only, while the course for the next management level could be more extensive to enable looking at critical issues in more depth.

applied to advance corporate preparedness in dealing with geoeconomic risks.

Public incentives are one way to provide incentives. Governments could, for example, consider tax breaks for investments in alternative sources of technology to promote supply chain resilience.[54] Stepping up export risk insurance for operations in countries considered more palatable than others is another idea. Moreover, governments can put money on the table to incentivize supply chain reorganization, as in Japan[55] and South Korea,[56] or to stimulate the reshoring of critical manufacturing capacities, a measure recently taken in the United States.[57]

Private incentives provide another perspective. On the one hand, companies can step up geoeconomic preparedness by asking suppliers to shed light on how they deal with geoeconomic risks and include benchmarking in service level agreements, for example. In addition, companies can also consider mutual help for supply chain partners by exchanging critical personnel in times of shortages, sharing raw materials or providing liquidity when partners run out of funds.

On the other hand, financial analysts and insurance companies can play key roles as well. Both assess to what extent companies withstand risks and how they prepare to weather storms should these risks materialize. Investments in business continuity management and the diversification of key suppliers, key materials and essential supply lines advance corporate preparedness and can reduce critical dependence. These investments cost money to bolster the corporate coping capacity. Financial analysts could positively acknowledge these investments and portray them as much-needed activities to cushion the geoeconomic risks a company faces. In addition, insurance companies could provide discounts on companies that undertake certain preparedness measures. They could also consider a risk premium when companies reduce risks by moving corporate activities from one location to another to lower the level of geoeconomic dependence, for example. Sophisticated hedging policies using state-of-the-art technologies are another way to advance corporate risk mitigation, and companies that use these technologies could benefit from bonus ratings by insurance companies and financial analysts.

54 On a related matter, Japan is currently considering the idea of "offering tax incentives to defense contractors that bolster cybersecurity measures". See Miki 2022.

55 Todo 2022.

56 Kim 2020.

57 For example, the CHIPS and Science Act was signed into law by President Joseph R. Biden on 9 August 2022. See The White House 2022.

FINAL REMARKS

Geoeconomics matters. It matters to businesses, and it matters to states. In this report, we have highlighted the key research findings of the IBRRM project, in the course of which we surveyed companies, carried out detailed corporate case studies and developed a vision for a new tool to understand and respond to geoeconomic risks.

Traditional risk analysis frameworks may not offer a clear place for the very particular intersection of political and economic risks that geoeconomics represents. As we have broadly defined it, geoeconomics is the pursuit of power politics using economic means. This includes measures such as embargoes, sanctions, export controls, anti-competitive business support measures by rival states – whether through financial means or otherwise – as well as policy responses such as screening of foreign investments. The first contribution of this report was to suggest how to position geoeconomic risks in comparison to other risks or threats from a state and a corporate perspective. Building on these considerations, we developed a geoeconomic risk catalogue – covering all types of risks, including several crucial categories of geoeconomic risks – and used this catalogue to generate a geoeconomic risk map, which helps to assess businesses' existing degrees of awareness of and preparedness for various categories of risk.

One of our central findings, illustrated through the risk map, is that both awareness of and preparedness for geoeconomic risks are likely insufficient in many European firms. Businesses, national governments and the EU institutions have a common interest in becoming better at understanding, assessing, anticipating and mitigating multiple types of geoeconomic risks.

The nature of this challenge calls for new forms of public–private, private–private and public–public cooperations and partnerships. Through detailed case studies, we were able to deepen our insights and explore the nature of the geoeconomic challenges faced by certain European companies – as well as their potential needs and readiness for new forms of cooperation.

In the final sections of this report, we also presented a vision for a collaborative tool that would enable stakeholders – both businesses and governments – to work together to better document, understand, anticipate and mitigate geoeconomic risks.

As part of our final recommendations, we have stressed the need to create a new strategic-level public-private dialogue to better address collaboratively the challenges ahead. We also believe there is a growing need for public authorities to commission regular geoeconomic risk assessments, as well as for the creation of executive-level education – for both private and public sector decision makers – concerning geoeconomic risks and how to master them.

In an era of disruption and renewed great power competition, the very nature of how to do business and how to govern the relations between businesses and governments is changing rapidly. With this work, we hope to have contributed to a way forward.

BIBLIOGRAPHY

Alami, Ilias and Adam D. Dixon (2020) "The strange geographies of the 'new' state capitalism". *Political Geography* 82, https://doi.org/10.1016/j.polgeo.2020.102237.

Angell, Norman (1911) *The Great Illusion*. New York/London: G. P. Putnam's Sons, https://archive.org/details/greatillusion00angeiala.

Borchert, Heiko (2021) "New Geoeconomics: A Primer". In *Storms Ahead. The Future Geoeconomic World Order*, edited by Johann Strobl and Heiko Borchert. Vienna: Raiffeisen Bank International, 16–35, https://bit.ly/3OULw21.

Borchert, Heiko (2019) Flow Control Rewrites Globalization. Implications for Businesses and Investors. *HEDGE21 Strategic Assessment* (Dubai: HEDGE21/ALCAZAR Capital), https://www.borchert.ch/wp-content/uploads/2021/08/1901_Borchert_Flow_Control.pdf.

Brussels Times (2022) "EU will not ban Russian diamonds in new sanction package". 30 September 2022, https://www.brusselstimes.com/298419/eu-will-not-ban-russian-diamonds-in-new-sanction-package.

Choer Moraes, Henrique and Mikael Wigell (2022) "Balancing Dependence: The Quest for Autonomy and the Rise of Corporate Geoeconomics". In *The Political Economy of Geoeconomics: Europe in a Changing World*, edited by Milan Babic, Adam D. Dixon and Imogen T. Liu. Cham: Palgrave Macmillan, 29–55.

Choer Moraes, Henrique and Mikael Wigell (2020) "The Emergence of Strategic Capitalism. Geoeconomics, Corporate Statecraft, and the Repurposing of the Global Economy". *FIIA Working Paper* 117, September 2020, The Finnish Institute of International Affairs, https://www.fiia.fi/en/publication/the-emergence-of-strategic-capitalism.

Christie, Edward Hunter, Caroline Buts and Cindy Du Bois (2021) "America, China, and the struggle for AI supremacy". Presentation delivered at the 24th Annual International Conference on Economics and Security, Volos, Greece, 8–9 July 2021.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2022) "Enterprise Risk Management – Integrating with Strategy and Performance (2017)". 27 April 2022, https://www.coso.org/SitePages/Enterprise-Risk-Management-Integrating-with-Strategy-and-Performance-2017.aspx?web=1.

Council Regulation (EU) 2022/428 of 15 March 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine. OJ L 87I, 15.3.2022, p. 13–43, https://eur-lex.europa.eu/eli/reg/2022/428.

Creuzberger, Stefan (2022) *Das Deutsch-russische Jahrhundert. Geschichte einer besonderen Beziehung*. Hamburg: Rowohlt.

European Commission (2022a) Report from the Commission to the European Parliament and the Council: Second Annual Report on the screening of foreign direct investments into the Union. COM (2022) 433 final, 1 September 2022.

European Commission (2022b) "EU refers China to the WTO following its trade restrictions on Lithuania". Press release, 27 January 2022, https://ec.europa.eu/commission/presscorner/detail/en/IP_22_627.

Eurostat (2022) EU trade since 1999 by SITC (DS-018995) [Data file]. Downloaded on 19 September 2022. https://ec.europa.eu/eurostat/data/database.

Farrell, Henry and Abraham L. Newman (2019) "Weaponized Interdependence. How Global Economic Networks Shape State Coercion". *International Security* 44 (1): 42–79.

Federal Office for Civil Protection FOCP (2020) National risk analysis report. Disasters and Emergencies in Switzerland 2020. December 2020, https://www.babs.admin.ch/en/aufgabenbabs/gefaehrdrisiken/natgefaehrdanalyse.html.

Fjäder, Christian, Niklas Helwig and Mikael Wigell (2021) "Recognizing 'Geoeconomic Risk'. Rethinking Corporate Risk Management for the Era of Great-Power Competition". *FIIA Briefing Paper* 314, June 2021, The Finnish Institute of International Affairs, https://www.fiia.fi/en/publication/recognizing-geoeconomic-risk.

Fonte, Giuseppe, Angelo Amante and Gavin Jones (2022) "Exclusive – Italy annuls sale of military drones firm to Chinese investors, sources say". *Reuters*, 10 March 2022, https://www.reuters.com/world/exclusive-italy-annuls-sale-military-drones-firm-chinese-groups-sources-say-2022-03-10/.

Hedenskog, Jakob and Robert L. Larsson (2007) *Russian Leverage on the CIS and the Baltic States*. Stockholm: Swedish Defence Research Agency (FOI).

HM Government (2010) A Strong Britain in an Age of Uncertainty. The National Security Strategy. *Cm* 7953, October 2010, https://www.gov.uk/government/publications/the-national-security-strategy-a-strong-britain-in-an-age-of-uncertainty.

International Organization for Standardization (ISO) (2018) ISO 31000:2018(en) Risk management – Guidelines, https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en.

Kim, Sam (2020) "South Korean Firms Reluctant to Bring Production Back from China". *Bloomberg*, 5 October 2020, https://www.bloomberg.com/news/articles/2020-10-05/south-korean-firms-reluctant-to-bring-production-back-from-china.

Liuhto, Kari (ed.) (2009) *The EU-Russia gas connection: Pipes, politics and problems*. Electronic Publications of Pan-European Institute 8/2009. Turku: University of Turku.

Miki, Rieko (2022) "Japan plans cybersecurity tax break for defense contractors". *Nikkei Asia*, 19 August 2022, https://asia.nikkei.com/Business/Aerospace-Defense/Japan-plans-cybersecurity-tax-break-for-defense-contractors.

Miller, Joe, Guy Chazan and Andy Bounds (2021) "German business hits out at China after Lithuania trade row snares exports". *Financial Times*, 17 December 2021, https://www.ft.com/content/15119be1-3d57-4769-8f82-ff8cb36a668b.

Monahan, Gregory (2008) *Enterprise Risk Management. A Methodology for Achieving Strategic Objectives*. Hoboken: John Wiley & Sons.

Nephew, Richard (2017) *The Art of Sanctions. A View from the Field*. New York: Columbia University Press.

Office of the United States Trade Representative (2018) *Findings of the investigation into China's acts, policies, and practices related to technology transfer, intellectual property, and innovation under section 301 of the trade act of 1974*. Washington DC: Office of the United States Trade Representative.

Pitchers, Christopher (2022) "Brussels backs Lithuania in row with China over Taiwan". *Euronews*, 14 January 2022, https://www.euronews.com/my-europe/2022/01/14/brussels-backs-lithuania-in-row-with-china-over-taiwan.

Racz, Nicolas, Edgar Weippl and Andreas Seufert (2010) "A Frame of Reference for Research of Integrated Governance, Risk and Compliance". In *Communications and Multimedia Security: 11th IFIP TC6/TC11 International Conference, CMS 2010, Linz, Austria, May 31–June 2, 2010, Proceedings*, edited by Bart Decker and Ingrid Schaumüller-Bichl. Berlin/Heidelberg: Springer.

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. OJ L 79I , 21.3.2019, p. 1–14, https://eur-lex.europa.eu/eli/reg/2019/452/oj.

Reuters (2020) "Fortum raises stake in Uniper to more than 75%". 18 August 2020, https://www.reuters.com/article/uniper-ma-fortum-oyj-idUSL8N2FK2OR.

Rice, Condoleezza and Amy Zegart (2018) *Political Risk. How Businesses and Organizations Can Anticipate Global Insecurity*. New York/Boston: Twelve.

Roberts, Anthea and Nicolas Lamp (2021) *Six Faces of Globalization. Who Wins, Who Loses, and Why It Matters*. Cambridge/London: Harvard University Press.

Sammut-Bonnici, Tanya and David Galea (2014) "PEST analysis". In *Wiley Encyclopedia of Management*, edited by Cary L. Cooper. Hoboken: John Wiley & Sons.

Sheffi, Yossi (2020) *The New (Ab)Normal. Reshaping Business and Supply Chain Strategy Beyond Covid-19*. Cambridge: MIT CTL Media.

Solingen, Etel (2021) "Introduction: Geopolitical Shocks and GSCs". In *Geopolitics, Supply Chains, and International Relations in East Asia*, edited by Etel Solingen. Cambridge: Cambridge University Press, 1–21.

Sonnenfeld, Jeffrey, Steven Tian, Franek Sokolowski, Michal Wyrebkowski and Mateusz Kasprowicz (2022) "Business Retreats and Sanctions Are Crippling the Russian Economy". *SSRN*, 20 July 2022, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4167193.

The Economist (2021) World Trade. Special Reports. 9 October 2021, https://www.economist.com/special-report/2021-10-09.

The White House (2022) "FACT SHEET: CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China". *Briefing Room/Statements and Releases*, 9 August 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/.

Todo, Yasuyuki (2022) "Japan's post-Covid-19 approach to supply chains". *East Asia Forum*, 3 July 2022, https://www.eastasiaforum.org/2022/07/03/japans-post-covid-19-approach-to-supply-chains/.

Uniper (2021) *Uniper List of Assets December 2021*. Düsseldorf: Uniper.

Uniper (2018) "Uniper statement: Fortum completes acquisition of approximately 47.35 percent of Uniper". Press release, 28 June 2018, https://www.uniper.energy/news/uniper-statement-fortum-completes-acquisition-of-approximately-4735-per-cent-of-uniper.

United States. White House Office (2017) *National Security Strategy of the United States of America*. December 2017, https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf.

U.S. Department of Justice (2020) "Chinese Citizen Convicted of Economic Espionage, Theft of Trade Secrets, and Conspiracy". Press release 20-598, 26 June 2020, https://www.justice.gov/opa/pr/chinese-citizen-convicted-economic-espionage-theft-trade-secrets-and-conspiracy.

Vanttinen, Pekka (2022) "Finland: Uniper's nationalisation a 'regrettable' necessity, relief". *Euractiv*, 22 September 2022, https://www.euractiv.com/section/politics/short_news/finland-unipers-nationalisation-a-regrettable-necessity-relief/.

Vihma, Antto and Mikael Wigell (2016) "Unclear and Present Danger: Russia's Geoeconomics and the Nord Stream II Pipeline". *Global Affairs* 2 (4): 377–388.

Waldron, Greg (2021) "Rome says Chinese firm illicitly acquired local UAV maker". *Flight-Global*, 3 September 2021, https://www.flightglobal.com/military-uavs/rome-says-chinese-firm-illicitly-acquired-local-uav-maker/145325.article.

Washington State University (n.d.) Course Guides, MGMT 491, PESTEL Analysis, https://libguides.libraries.wsu.edu/c.php?g=996573&p=7214435. Accessed 1 October 2022.

Weber, Steven (2019) *Bloc by Bloc. How to Build a Global Enterprise for the New Regional Order*. Cambridge/London: Harvard University Press.

Wigell, Mikael, Matthias Deschryvere, Christian Fjäder, Niklas Helwig, Ville Kaitila, Heli Koski, Josi Seilonen and Arho Suominen (2022) Europe Facing Geoeconomics: Assessing Finland's and the EU's Risks and Options in the Technological Rivalry. *Publications of the Government´s analysis, assessment and research activities* 2022:12, February 2022, Prime Minister's Office, https://julkaisut.valtioneuvosto.fi/handle/10024/163804.

Wigell, Mikael, Sören Scholvin and Mika Aaltola, eds. (2018) *Geo-economics and Power Politics in the 21st Century: The Revival of Economic Statecraft*. London/New York: Routledge.

Williams, Carol (2019) "COSO ERM Framework – Background and Overview". *ERM Insights by Carol*, 11 March 2019, https://www.erminsightsbycarol.com/coso-erm-framework/

CONTRIBUTORS

Dr Mikael Wigell (IBRRM Project Leader) is Research Director at FIIA. He is also Adjunct Professor of International Political Economy at Tampere University and Member of the World Economic Forum Expert Network. He earned his PhD at the London School of Economics, and he has been Visiting Fellow at the Changing Character of War Centre, Oxford University. He has previously been Member of the Development Policy Committee of the Finnish Government and Chairman of the Finnish International Studies Association (2017–2019). His work on geoeconomics and economic statecraft has been published in top-ranked international academic journals such as *International Affairs*, *World Development*, *The Washington Quarterly*, *Comparative Strategy*, *Democratization*, *Asia Europe Journal* and *Global Affairs*. He has also written policy reports and briefings for the European Commission, the European Parliament, the Finnish Government and the Japan Development Bank. He is the editor (with Mika Aaltola and Sören Scholvin) of *Geo-Economics and Power Politics in the 21st Century: The Revival of Economic Statecraft* (Routledge 2018; 2020).

Dr Heiko Borchert owns and manages Borchert Consulting & Research AG, a strategic affairs consulting boutique. He is also Co-Director of the Defense AI Observatory at Helmut Schmidt University/ University of the Federal Armed Forces, Senior Research Fellow at the German Institute for Defense and Strategic Studies, Associate Fellow at the Center for Advanced Security, Strategic and Integration Studies (CASSIS), subject matter expert at the Hague Center for Strategic Studies (HCSS) and member of the advisory boards of *Zeitschrift für Außen- und Sicherheitspolitik and The Defence Horizon Journal.* He has studied international relations, business administration, economics and law at the University of St. Gallen, where he also received his PhD. His latest book as editor (with Johann Strobl) is *Storms Ahead: The Future Geoeconomic World Order* (Vienna Raiffeisen Bank, 2021).

Dr Christian Fjäder is currently heading the Geostrategic Intelligence Group, a private boutique consulting agency. He was Senior Research Fellow at FIIA during the project and prior to that, Director for Policy Planning and Analysis at the National Emergency Supply Agency (NESA) in Finland, with responsibilities in strategy development, international relations, and analysis and research coordination. He also has extensive corporate experience in security, risk and resilience leadership in regional and global leadership roles. For instance, he has headed Nokia's regional corporate security function in the Asia–Pacific region and the company's corporate resilience functions as the global Head of Risk and Resilience. He has a PhD in International Relations from the University of Sydney, an MBA from Bond University, and an MA in International Relations and a BA in International Studies from Flinders University, Australia.

Edward Hunter Christie is Senior Research Fellow at FIIA. He worked as a research economist at the Vienna Institute for International Economic Studies from 2002 to 2010, with a notable focus on international trade and energy security. From 2010 to 2014, he worked in public affairs at EU level, as Senior Policy Adviser and subsequently as Chief Economist for a European industry association in the transport sector. After that, from 2014 to 2020, he served as a NATO official in roles pertaining to defence economics, strategic foresight and technology policy. While at NATO, his work focus included analyses pertaining to economic sanctions, coercion and decoupling, as well as the links between economic and fiscal conditions and military capabilities. He holds an MSc in Economics from the London School of Economics.

Lars-Hendrik Hartwig is a consultant at the Austrian consultancy Repuco (part of the msg Group). A political science graduate, he completed his master's degree at the University of Heidelberg in 2017. He has worked at the Institute of Political Science (IPW) and the Alfred Weber Institute for Economic Sciences (AWI), focusing on EU topics and security policy issues, among others. Since 2019, he has been based in Vienna and is engaged in projects on the strategic direction of digital policy, strategy development in the public and private sectors, and foresight analyses with a focus on risk and security trends.

PREVIOUSLY PUBLISHED IN THE SERIES

Mikael Wigell, Mariette Hägglund, Christian Fjäder, Emma Hakala, Johanna Ketola & Harri Mikkola
Nordic Resilience. Strengthening cooperation on security of supply and crisis preparedness, FIIA Report 70 (2022)

Katja Creutz & Sia Spiliopou Åkermark
The Faroe Islands, Greenland and the Åland Islands in Nordic cooperation, FIIA Report 69 (2021)

Katja Creutz, Sofie Berglund, Telli Betül Karacan, Alberto Giacometti, Kristi Haugevik, Ninna Nyberg Sørensen, Mari Wøien Meijer, Axa Lares
Nordic cooperation amid pandemic travel restriction, FIIA Report 68 (2021)

Niklas Helwig (ed.)
Strategic autonomy and the transformation of the EU: New agendas for security, diplomacy, trade and technology, FIIA Report 67 (2021)

Bart Gaens, Ville Sinkkonen
Great-power competition and the rising US-China rivalry: Towards a new normal?, FIIA Report 66 (2020)

Teemu Tammikko, Tuomas Iso-Markku
The EU's external action on counter-terrorism: Development, structures and actions, FIIA Report 65 (2020)

Antto Vihma, Gunilla Reischl, Astrid Nonbo Andersen, Sofie Berglund
Climate change and populism: Comparing the populist parties' climate policies in Denmark, Finland and Sweden, FIIA Report 64 (2020)

Niklas Helwig, Juha Jokela, Clara Portela (eds.)
Sharpening EU sanctions policy: Challenges and responses in a geopolitical era, FIIA Report 63 (2020)

Ryhor Nizhnikau, Arkady Moshes (eds.)
Ukraine and its regions: Societal trends and policy implications, FIIA Report 62 (2020)

Emma Hakala, Harri Mikkola, Juha Käpylä, Matti Pesu & Mika Aaltola
Suomen huoltovarmuus ja Baltian alue: Tiivistyvät yhteydet muuttuvassa turvallisuusympäristössä, FIIA Report 61 (2019)

Leo Michel & Matti Pesu
Strategic deterrence redux: Nuclear weapons and European security, FIIA Report 60 (2019)

Katja Creutz, Tuomas Iso-Markku, Kristi Raik and Teija Tiilikainen
The changing global order and its implications for the EU, FIIA Report 59 (2019)

Arkady Moshes, András Rácz (eds.)
What has remained of the USSR: Exploring the erosion of the post-Sovie space, FIIA Report 58 (2019)

Marcin Kaczmarski, Mark N. Katz and Teija Tiilikainen
The Sino-Russian and US-Russian relationships: Current developments and future trends, FIIA Report 57 (2018)

Kristi Raik, Mika Aaltola, Jyrki Kallio and Katri Pynnöniemi
The security strategies of the US, China, Russia and the EU: Living in different worlds, FIIA Report 56 (2018)

Harri Mikkola, Mika Aaltola, Mikael Wigell, Tapio Juntunen ja Antto Vihma
Hybridivaikuttaminen ja demokratian resilienssi: ulkoisen häirinnän mahdollisuudet ja torjuntakyky liberaaleissa demokratioissa, FIIA Report 55 (2018)

Mika Aaltola, Charly Salonius-Pasternak, Juha Käpylä and Ville Sinkkonen (eds.)
Between change and continuity: Making sense of America's evolving global engagement, FIIA Report 54 (2018)

Marco Siddi (ed.)
EU member states and Russia: national and European debates in an evolving international environment, FIIA Report 53 (2018)

Elina Sinkkonen (ed.)
The North Korean Conundrum: International responses and future challenges, FIIA Report 52 (2017)

Mika Aaltola and Bart Gaens (eds.)
Managing Unpredictability
Transatlantic relations in the Trump era, FIIA Report 51 (2017)

Tuomas Iso-Markku, Juha Jokela, Kristi Raik,Teija Tiilikainen, and Eeva Innola (eds.)
The EU's Choice
Perspectives on deepening and differentiation, FIIA Report 50 (2017)

Mika Aaltola, Christian Fjäder, Eeva Innola, Juha Käpylä, Harri Mikkola
Huoltovarmuus muutoksessa: Kansallisen varautumisen haasteet kansainvälisessä toimintaympäristössä, FIIA Report 49 (2016)

Juha Pyykönen
Nordic Partners of NATO: How similar are Finland and Sweden within NATO cooperation? FIIA Report 48 (2016)

Kristi Raik & Sinikukka Saari (eds.)
Key Actors in the EU's Eastern Neighbourhood: Competing perspectives on geostrategic tensions, FIIA Report 47 (2016)

Toivo Martikainen, Katri Pynnöniemi, Sinikukka Saari & Ulkopoliittisen instituutin työryhmä
Venäjän muuttuva rooli Suomen lähialueilla: Valtioneuvoston selvitys- ja tutkimustoiminnan raportti

Mika Aaltola & Anna Kronlund (eds.)
After Rebalance: Visions for the future of US foreign policy and global role beyond 2016, FIIA Report 46 (2016)

Katri Pynnöniemi & András Rácz (eds.)
Fog of Falsehood: Russian Strategy of Deception and the Conflict in Ukraine, FIIA Report 45 (2016)

Niklas Helwig (ed.)
Europe's New Political Engine: Germany's role in the EU's foreign and security policy, FIIA Report 44 (2016)

András Rácz
Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist, FIIA Report 43 (2015)

Katri Pynnöniemi, James Mashiri
Venäjän sotilasdoktriinit vertailussa: Nykyinen versio viritettiin kriisiajan taajuudelle, FIIA Report 42 (2015)

Andrei Yeliseyeu
Keeping the door ajar: Local border traffic regimes on the EU's eastern borders, FIIA Report 41 (2014)

Mika Aaltola, Juha Käpylä,Harri Mikkola, Timo Behr
Towards the Geopolitics of Flows: Implications for Finland, FIIA Report 40 (2014)

Juha Jokela, Markku Kotilainen, Teija Tiilikainen, Vesa Vihriälä
EU:n suunta: Kuinka tiivis liitto? FIIA Report 39 (2014)

Juha Jokela (ed.)
Multi-speed Europe? Differentiated integration in the external relations of the European Union, FIIA Report 38 (2013)

Sean Roberts
Russia as an international actor: The view from Europe and the US, FIIA Report 37 (2013)

Rosa Balfour, Kristi Raik
Equipping the European Union for the 21st century: National diplomacies, the European External Action Service and the making of EU foreign policy, FIIA Report 36 (2013)

Katri Pynnöniemi (ed.)
Russian critical infrastructures: Vulnerabilities and policies, FIIA Report 35 (2012)

Tanja Tamminen (ed.)
Strengthening the EU's peace mediation capacities: Leveraging for peace through new ideas and thinking, FIIA Report 34 (2012)

Harri Mikkola, Jukka Anteroinen, Ville Lauttamäki (eds.)
Uhka vai mahdollisuus? Suomi ja Euroopan puolustus- ja turvallisuusmarkkinoiden muutos, FIIA Report 33 (2012)

Touko Piiparinen & Ville Brummer (eds.)
Global networks of mediation: Prospects and avenues for Finland as a peacemaker, FIIA Report 32 (2012)

Mia Pihlajamäki & Nina Tynkkynen (eds.)
Governing the blue-green Baltic Sea: Societal challenges of marine eutrophication prevention, FIIA Report 31 (2011)

Arkady Moshes & Matti Nojonen (eds.)
Russia-China relations: Current state, alternative futures, and implications for the West, FIIA Report 30 (2011)

Teija Tiilikainen & Kaisa Korhonen (eds.)
Norden – Making a Difference? Possibilities for enhanced Nordic cooperation in international affairs, FIIA Report 29 (2011)

Timo Behr (ed.)
Hard Choices: The EU's options in a changing Middle East, FIIA Report 28 (2011)

Jyrki Kallio
Tradition in Chinese politics: The Party-state's reinvention of the past and the critical response from public intellectuals, FIIA Report 27 (2011)

Steven Parham
Controlling borderlands? New perspectives on state peripheries in southern Central Asia and northern Afghanistan, FIIA Report 26 (2010)

Mari Luomi
Managing Blue Gold: New Perspectives on Water Security in the Levantine Middle East, FIIA Report 25 (2010)

Tapani Paavonen
A New World Economic Order: Overhauling the Global Economic Governance as a Result of the Financial Crisis, 2008–2009, FIIA Report 24 (2010)

Toby Archer, Timo Behr, Tuulia Nieminen (eds)
Why the EU fails – Learning from past experiences to succeed better next time, FIIA Report 23 (2010)

NAVIGATING GEOECONOMIC RISKS

TOWARDS AN INTERNATIONAL BUSINESS RISK AND RESILIENCE MONITOR

Geoeconomics – the pursuit by states of power politics using economic means – is the new reality in which European and global businesses operate. From financial sanctions and trade embargoes to rival state-sponsored technology theft and anti-competitive practices, European companies face an urgent need to understand, assess, anticipate and mitigate a whole new range of risks that are fundamentally different from ordinary market or regulatory risks. As state actors play a central role in both enacting geoeconomic measures and responding to them, the need for new forms of public–private partnership and collaboration is likewise rising. To that end, this report develops a vision for a new collaborative tool – an international business risk and resilience monitor – which both corporations and public authorities could contribute to and use together to advance awareness of and preparedness for rapidly emerging risks to economic security. /

FIIA
FINNISH
INSTITUTE
OF INTERNATIONAL
AFFAIRS

ISBN (print) 978-951-769-743-9
ISBN (web) 978-951-769-744-6
ISSN (print) 1458-994X
ISSN (web) 2323-5454