

# Resilience in turbulent times

Geopolitical risks and financial institutions

DeNederlandscheBank

EUROSYSTEEM

Authors: Maurice Doll, Frank van Dunné, Lora Steen and Thomas Vos.

The authors thank David Keijzer for his statistical support and the many colleagues at DNB who contributed to this report. Our thanks also go out to the external experts for the useful exchange of views.

# Table of contents

Summary and key messages	4
Introduction	7
Geo-economic fragmentation, the real economy, and financial markets	11
2.1 Exposures, credit and market risks of financial institutions	11
2.2 Increased risk aversion, volatility, and the impact on funding costs	15
2.3 Geopolitical uncertainties underline the importance of proper risk management	16
The changing cyber threat landscape gives rise to risks	18
3.1 The changing threat landscape gives rise to increasing cyber risks	18
3.2 Strengthening operational resilience requires constant effort	22
The changing sanctions landscape: challenges and risks for financial institutions	25
4.1 Changed sanctions landscape gives financial institutions a more prominent role	25
4.2 Implications of the changed sanctions landscape on financial institutions	27
4.3 Adequate compliance with sanctions regime while keeping a close eye on potential side effects	30

# Summary and key messages

**Geopolitical tensions have increased in recent years.** After decades of multilateral cooperation and international free trade, the world is witnessing a shift towards increased protectionism, fragmentation, and block formation. In the current geopolitical environment, conflicts between countries and regions often have a hybrid nature. To maintain or increase their influence on the world stage, influence decision-making in other countries, and to gain access to knowledge and technology available abroad, governments employ a variety of strategies. Trade barriers and industrial policy measures are used to protect strategic sectors. Additionally, Western governments have increasingly imposed financial sanctions. Access to international financial infrastructure and financial services is increasingly used to exert pressure, a practice described as the weaponisation of finance.

**The turbulent geopolitical environment is impacting financial institutions through various channels.** The term 'geopolitical risk' is typically understood as the threat, realization, and escalation of adverse events associated with wars, terrorism and tensions among states and political actors that affect the peaceful course of international relations. The nature of geopolitical risks is such that they are inherently uncertain. Furthermore, in an environment characterised by heightened geopolitical uncertainty, the probability of new and unforeseen shocks only grows. Geopolitical developments impact financial institutions and the macroeconomic environment in which they operate through various channels. Institutions are affected through their exposures to firms prone to disruptions in global supply chains and through operational activities and investments in potentially vulnerable jurisdictions. Furthermore, they may also face deliberate digital or physical disruptions to their own business

processes or to those of critical suppliers or be hit by sanctions. Geopolitical tensions therefore potentially expose financial institutions to a variety of financial and non-financial risks, such as inflation, credit, market, liquidity, and operational risks.

## Geopolitical risks must be embedded in institutions' risk management

**It is imperative that institutions proactively identify and comprehensively manage geopolitical risks, given their potentially significant impact.** In recent years, geopolitical risks have, understandably, become a key concern for financial institution executives. It is crucial for financial institutions to implement effective strategies to mitigate the impact of geopolitical risks. To do so, they need to embed geopolitical risks comprehensively in their risk management. This requires, first and foremost, being alert and anticipating how geopolitical risks may give rise to financial and non-financial risks. To this end, conducting stress tests that capture the impact of geopolitical risks is a valuable exercise. Such stress tests should be based on extreme but plausible scenarios, such as a further escalation of the tensions between China and Taiwan. This provides insight into whether institutions have sufficient buffers in terms of both solvency and liquidity to cope with potential financial risks that may arise from geopolitical developments. In addition to stress tests, targeted scenario analyses provide valuable insight into risks not captured by credit and market risk models. This insight is crucial for identifying the controls needed to mitigate these risks. For example, analysing a situation in which operational activities in a specific jurisdiction are halted, for instance due to sanctions, can assist in identifying operational vulnerabilities and potential risks to business models. It is crucial for institutions to leverage the insights derived from

these forward-looking analyses to refine and enhance their strategy and risk management.

**Supervisors will continue to challenge institutions on how they embed geopolitical risks in their risk management.** Financial institutions are generally expected to understand, manage and report on the material risks they are exposed to, including geopolitical risks. These specific risks will be an important area of focus in our supervision in the years ahead. DNB will hold institutions to account on how they identify and manage risks arising from an increasingly challenging and turbulent geopolitical environment.<sup>1</sup>

### Particular attention must be paid to cyber resilience and sanctions compliance

**Given the increasingly sophisticated and complex set of threats, it is essential to maintain a focus on enhancing cyber resilience. Supervisors will ensure that the new European rules aimed at increasing cyber resilience are properly adhered to.** Financial institutions face cyber risks, including through their (critical) suppliers. These risks can affect individual institutions and have broader implications for the financial system through contagion and potential loss of trust. In addition to implementing robust cybersecurity measures and conducting regular tests, it is essential for institutions to have the resilience needed to safely and efficiently resume services after a cyber incident. This is not only relevant to the institutions themselves, but also to the IT service providers on which they have become increasingly dependent. The European Digital Operational Resilience Act (DORA) introduces more rigorous standards for the management of IT and cyber risks

throughout the outsourcing chain and for institutions' continuity measures. Together with the Dutch Authority for the Financial Markets (AFM), DNB will monitor that institutions comply with DORA.

**The rise in the number of sanctions imposed by governments increases the legal and reputational risks faced by institutions. It is crucial that they fully comply with the sanctions.** Western governments rely more and more on sanctions, particularly financial sanctions. Financial institutions have an important responsibility in complying with these sanctions, given their key role in the payments system, the access to financial services provided by them, and in their role as investors. The rise in the number of sanctions imposed by governments increases the legal and reputational risks faced by institutions. DNB supervises the operations of financial institutions to ensure they fully comply with sanctions. Despite recent improvements, a significant number of institutions still need to make serious efforts to bring sanctions compliance to the required level of maturity. It is crucial for institutions to pay close attention to detection of sanctions circumvention, screening for dual-use goods (which have both military and civilian applications) and the identification of a firm's ultimate beneficial owners (UBO).

### To increase resilience, public-private and European collaboration must be intensified.

**Enhancing resilience requires action from financial institutions and the private sector, as well as more public-private collaboration.** Financial institutions, like any other private actor, are responsible themselves for implementing robust risk management strategies and take the required preventive and mitigating actions to ensure the continuity of their

<sup>1</sup> See also DNB (2024) Supervisory Strategy 2025-2028.

services. It is, however, imperative that public and private parties work closely together to enhance the resilience of society. Timely and broad sharing of cyber threats between different sectors and with the government is essential to spot these threats. Public-private partnerships are imperative to increase the resilience of vital infrastructure, such as telecom, electricity supply, and payments. To ensure resilience in the face of potential disruptions in these vital sectors, whether digital or physical, cross-sectoral collaboration and clear central guidance are essential. The government must continue to initiate large-scale (cyber) drills and practising the activation of the national crisis plan. The insights gained must then be fed back to increase resilience.

**Europe should strengthen its cooperation and integration to face the current complex geopolitical environment.** The current complex geopolitical environment, combined with the resulting cross-border risks, calls for closer European

cooperation. For example, a harmonised sanctions policy helps to safeguard more level playing field between institutions and facilitates sanction compliance by institutions operating in multiple Member States. Moreover, while aiming to reduce strategic dependencies policymakers must carefully weigh the negative effects on the economy and the further fragmentation such a reduction can foster. Lastly, it is essential for the European Union's competitiveness to take steps to complete the single market – in particular the European capital markets union and the banking union. A well-functioning single market and better-functioning funding markets offer additional opportunities for diversification for investors. They are also crucial for growth potential: integrated and liquid capital markets increase access to finance for innovative firms. A well-functioning single market, in which households and firms can prosper, is an important source of protection from adverse developments elsewhere. Thereby contributing to stability in general.

# Introduction

**Geopolitical tensions have increased over the past few years.** The world is facing an increasingly competitive landscape, with countries pursuing their own agendas and reducing risky dependencies. Multilateral cooperation has remained stagnant, and the policy of so called 'strategic autonomy' is becoming the norm. The Russian invasion of Ukraine, rising tensions between China and Taiwan, the US-China trade dispute and the spiralling violence in the Middle East are clear indications of these prevailing geopolitical tensions.

**The global economy is increasingly fragmented, reflected by a growing number of trade restrictions.** IMF research shows that more than 2,500 industrial policy measures, of which 70% are trade-distorting<sup>2</sup>, were adopted worldwide in 2023 alone. Growing economic nationalism, as evidenced by recent elections in Europe, along with Brexit and 'America First' policies in the United States, is reinforcing this trend. In addition, it is more difficult to reach agreements within multilateral fora, such as the World Trade Organisation (WTO). Global trade agreements have given way to regional and bilateral trade agreements. This policy shift from integration to disintegration, mostly driven by strategic

considerations, is commonly referred to as 'geo-economic fragmentation'<sup>3</sup>. Geo-economic fragmentation affects global trade. Growth in global trade is slowing down, underlying this is a visible shift towards regionalisation of trade flows.<sup>4</sup>

**Governments are attempting by various means to perpetuate or increase their influence on the world stage, resulting in fragmentation and the formation of blocks between countries and regions.** The unipolar world order, with the United States at its centre that emerged after the collapse of the Soviet Union, is being challenged by countries and regions that are pushing for fundamental changes to that order.<sup>5</sup> Besides increased tensions between Russia and the West, as a result of Russia's invasion of Ukraine, the United States-China relationship stands out in particular. In recent decades, geopolitical and economic competition has intensified. Moreover, conflicts between nations increasingly exhibit hybrid characteristics, as described in Box 1. Finally, the transatlantic relationship is changing as well. While the United States remains the EU's most important ally, its relationship with Europe has become more businesslike.<sup>6</sup>

<sup>2</sup> Evenett, S. et al. (2024) [The return of Industrial Policy in data.](#)

<sup>3</sup> IMF (2023) [Goeconomic Fragmentation and the Future of Multilateralism.](#)

<sup>4</sup> ECB (2023) [The EU's Open Strategic Autonomy from a central banking perspective.](#)

<sup>5</sup> See, for example, WRR (2024) [The Netherlands in a fragmenting world order \(Dutch\).](#)

<sup>6</sup> The Economist (2024) [Trump and other populists will haunt NATO's 75th birthday party.](#)

Box 1

**Conflicts between countries are increasingly taking on a hybrid character**

**Conflicts between countries have become increasingly hybrid in recent decades.** Governments are increasingly deploying diverse tactics, blurring the lines of legitimacy, such as diplomatic and financial sanctions, import and export restrictions, cyber-attacks and espionage. Governments use such means to maintain or enhance their role on the global stage, to gain access to knowledge and technology available abroad, or to influence decision-making in other countries. This phenomenon is known as hybrid warfare.<sup>7</sup> Its increase is both illustrative of the heightened geopolitical tensions and one of their drivers, together with technological developments. It increases the ability to influence political and economic activities in other countries on a larger scale and with greater speed and enables new *modi operandi*.<sup>8</sup> Armed conflict and overt military intervention are seen as a last resort, partly because of the risk of escalation, high costs and limited popular support.

**Russia and China are the biggest threats from a Western perspective.** Russia sees itself in an existential conflict with the West and made hybrid warfare an official strategy long before the annexation of Crimea in 2014.<sup>9</sup> According to the General Intelligence and Security Service of the Netherlands (AIVD), the Netherlands is a major espionage target for Russia. In addition, Russia is exploiting anti-Western sentiments in the Netherlands and is seeking confrontation with the West in the cyber domain.<sup>10</sup> Russia has also shown that it is willing to use energy dependence as a means of exerting pressure. China is a major trading partner of the West in many areas, but at the same time is on a drive for greater global political and economic influence. One way China is doing this is by strategically investing in infrastructure in Asia, Africa, Europe and South America through the Belt and Road Initiative and by making itself independent of foreign technology.<sup>11</sup> Chinese cyber-attacks and espionage in the West are mainly driven by the desire to access Western technology to gain strength in economic and military terms. Finally, medium-sized and smaller countries can also pose a threat to the West. For example, North Korea is trying to loot money through cyber-attacks to fund its treasury, and Iran is trying to access Western knowledge through knowledge institutions.

**The governments of Western countries are also becoming more involved in geopolitical competition.** To do so, they use tools such as restricting exports and imposing financial and diplomatic sanctions (see also Chapter 4). Examples include US import tariffs on steel and aluminium, screening of US outbound investment into China and export restrictions introduced by the United States and EU Member States on chip technology. The US is making strategic use of digital and financial dependencies, such as the central position of the dollar in international trade and payments.<sup>12</sup>

7 See, among others, National Security Analyst Network (2024 (Dutch)), EC and Hybrid CoE (2021), NATO (2024) and NCTV (2019).

8 Sweijts, T. (2022) *Between war and peace, 'Hybrid Threats' and NATO's strategic concept*.

9 De Wijk, R. et al. (2021) *Russian hybrid warfare (Dutch)*.

10 AIVD (2024) *Annual Report 2023*.

11 See, among others, AIVD, MIVD and NCTV (2022, Dutch) and The Economist (2020).

12 See, for example, Farrell H. and Newman A. (2024) *Underground Empire - How America weaponised the world economy*, Penguin Random House.



**The Dutch economy is sensitive to geo-economic fragmentation.** In 2021, the Netherlands was the world's sixth-largest exporter and the eighth-largest importer of goods. Additionally, the Netherlands is both a major investor abroad as well as a recipient of foreign direct investment (FDI).<sup>13</sup> Its high degree of openness makes the Netherlands vulnerable to disruptions in global supply chains and to trade and capital restrictions. Such disruptions and restrictions will require firms to adjust. That may lead to upward price pressures and have implications for economic growth and financial stability.<sup>14</sup>

**The (digital) threat to the Netherlands is as strong as ever and is constantly changing.** Similar to other Western countries, foreign interference increasingly poses a threat to social and economic security in the Netherlands, according to publications by the General Intelligence and Security Service of the Netherlands (AIVD), the Military Intelligence and Security Service (MIVD) and the Dutch National Coordinator for Counterterrorism and Security (NCTV).<sup>15</sup> The implications for the Netherlands are amplified by its open nature as an important hub for goods, services and data.<sup>16</sup> Besides Russia, the biggest threat in this respect comes from China. Especially knowledge-intensive sectors are potential targets for cyber-attacks, espionage, sabotage and strategic takeovers. Examples of these sectors include the semiconductor -,

aerospace -, and maritime industries. Likewise, vital sectors, such as energy and telecom, are potential targets. This may also apply to the financial sector, due to the important societal role played by financial institutions and the information and (monetary) assets they manage.

**Geopolitical developments can affect Dutch financial institutions through various channels.**

Increasing geo-economic fragmentation and geopolitical risks<sup>17</sup> affect financial institutions through various financial and non-financial risks, as shown in Figure 1. The speed at which different channels impact financial institutions varies. For example, cyber-attacks on institutions or critical third parties have the potential to cause significant damage in the short term, while it may take some time for institutions to suffer credit losses due to imposed trading restrictions. Moreover, different channels can reinforce each other. Tighter funding conditions caused by increased uncertainty could further increase credit losses for banks, especially among firms already facing disruptions in their supply chains. This may also give rise to liquidity risks if these firms are forced to draw more heavily on existing credit lines. In addition, cyber-attacks that give rise to operational risks for a particular financial institution can have the potential to have broader ramifications when they result in a loss of confidence among depositors in the institution's ability to safeguard their funds.

<sup>13</sup> DNB (2024) *Revision of balance of payments: International relations in sharper focus (Dutch)*.

<sup>14</sup> DNB (2023) *Geo-economic fragmentation: economic and financial stability implications*.

<sup>15</sup> See, among others, NCTV (2022), AIVD (2024) and MIVD (2024).

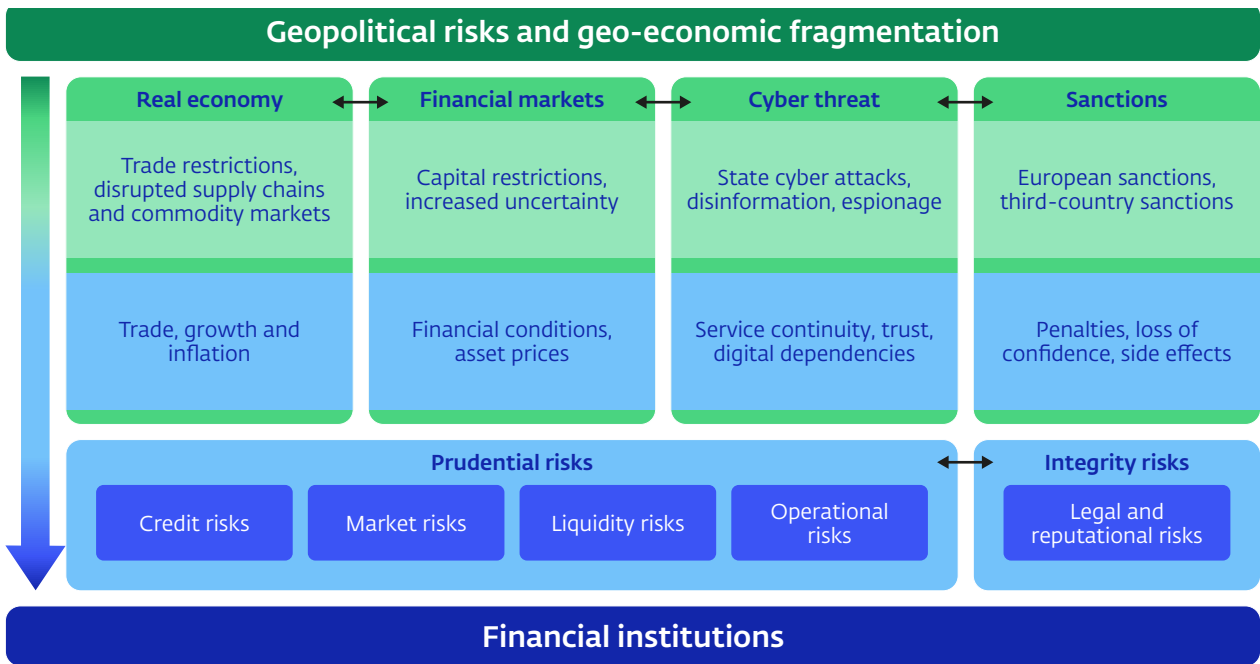
<sup>16</sup> ANV (2019), *Integrated Risk Analysis National Security, National Security Analyst Network*

<sup>17</sup> This study adopted Caldara and Iacoviello's (2022) widely used definition of geopolitical risks: "the threat, realization, and escalation of adverse events associated with wars, terrorism, and any tensions among states and political actors that affect the peaceful course of international relations."

The following chapters provide a detailed examination of the ways in which geopolitical developments impact financial institutions, as well as an analysis of the associated risks. Chapter 2 discusses how geopolitical developments can affect institutions through the real economy, financial markets, and institutions' exposures. Chapter 3 discusses the risks posed by the changing cyber

threat landscape, including the role of state actors, chain dependencies and the need for effective response and recovery plans. Chapter 4 then discusses financial sanctions, the role of financial institutions in implementing these sanctions, and the side effects of sanctions that can give rise to risks for institutions.

Figure 1 Geopolitical developments and risks for financial institutions



Source: DNB, partly inspired by IMF (2023)

# Geo-economic fragmentation, the real economy, and financial markets

Dutch financial institutions are particularly susceptible to geo-economic fragmentation through their exposures to firms prone to disruptions in global value chains. Additionally, geopolitical developments may generate uncertainty and volatility in financial markets, which in turn may push up funding costs for institutions, in addition to exacerbating market risks. It is of the utmost importance that institutions identify and comprehensively manage geopolitical risks in a timely manner.

## 2.1 Exposures, credit and market risks of financial institutions

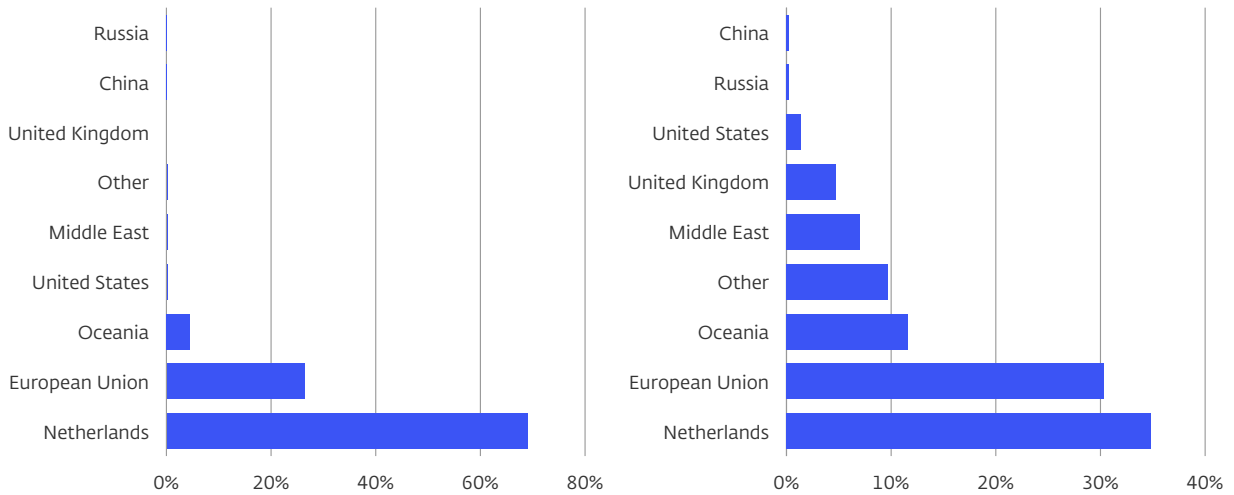
**Financial institutions are exposed to geopolitical risks through activities in countries that are distant from the Netherlands from a geopolitical perspective.** To illustrate, financial institutions such as banks, insurance firms and pension funds were compelled to implement write-downs on their Russian assets in the wake of the Russian invasion of Ukraine (see also Chapter 4). That said, previous research conducted by DNB shows that *direct* exposures of financial institutions to countries at a geopolitical distance from the Netherlands, which in that analysis included Russia, Iran and China, are limited and have continued to decline in recent years.<sup>18</sup> Of the total corporate loan portfolio of Dutch banks,

0.5% was granted to firms in this category of countries. Through their loan portfolio, Dutch banks have exposures mainly to Dutch households and firms in the Netherlands and other EU Member States (see Figure 2). Insurance firms and pension funds also have exposures mainly to the Netherlands, other EU Member States, the United States and the United Kingdom through their investment portfolios. Of their direct investments in corporate bonds and equities, insurance firms and pension funds invested less than 1% in firms based in countries geopolitically distant from the Netherlands. Incidentally, insurance firms are not only exposed to geopolitical risks through their assets, but could also potentially be affected through their liabilities. Box 2.1 discusses this in greater detail.

<sup>18</sup> See DNB (2024). In this analysis, research conducted by Baba et al. (2023) distinguished between like-minded, neutral and opposing countries, based on the way they voted on the UN resolution on the human rights situation in the occupied regions of Ukraine. The 'opposing' group consists of 15 countries. This underlying division of countries into groups cannot be considered absolute, as it relates to a specific UN resolution. The geographical exposures of pension funds and insurance firms exclude holdings in investment funds.

Figure 2 Geographical exposure of Dutch banks' credit portfolios

Loans to households (left, % of total) and loans to firms (right, % of total)



Note: The figure shows shares of different countries and continents in total household and corporate loan portfolios of Dutch banks, respectively. The Oceania group includes Australia and New Zealand; the Middle East includes Türkiye, Saudi Arabia, Israel, Qatar and the United Arab Emirates. Data refer to 2023.

Source: DNB (2024).

**Financial institutions are especially sensitive to geo-economic fragmentation through corporate global value chains**

Geo-economic fragmentation can impact financial institutions' investment and credit portfolios *indirectly*. The firms they have invested in, or provided credit to, may face disruptions in their supply chains, for example due to trade restrictions. Particularly vulnerable to such disruptions are firms that depend on goods and raw materials from countries that are geopolitically distant from the Netherlands, or for which these countries are important export markets. The potential supply risks associated with increasing export restrictions on critical commodities, combined with the geograph-

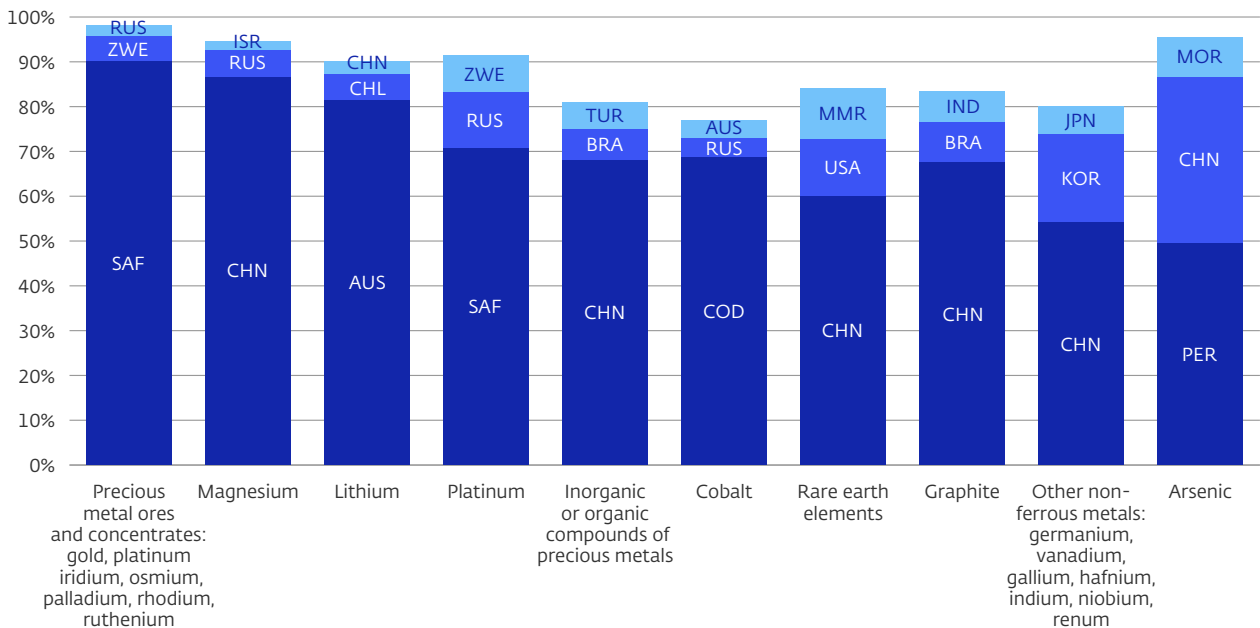
ically concentrated extraction and processing of these commodities, serve to illustrate this (see Figure 3).<sup>19</sup> DNB research shows that banks are particularly sensitive to geo-economic fragmentation through their lending to the manufacturing industry.<sup>20</sup> This is because the manufacturing industry relies comparatively heavily on imports from countries that are geopolitically distant from the Netherlands. Banks are exposed to this because business loans to industry make up a relatively large share of their loan portfolios. The same applies to pension funds and insurance firms through their investments in industrial firms, which exposes them to market risks.

<sup>19</sup> See, for example, OECD (2023) *Raw materials critical for the green transition*.

<sup>20</sup> DNB (2024) *Financial Stability Report, Autumn 2024*.

Figure 3 High geographical concentration of extraction of critical raw materials

Share of global production (%)



Note: The figure shows the top three producing countries for the ten most production-concentrated critical raw materials. AUS = Australia, BRA = Brazil, CHN = China, CHL = Chile, COD = Democratic Republic of Congo, IND = India, ISR = Israel, JPN = Japan, KOR = South Korea, MOR = Morocco, MMR = Myanmar, PER = Peru, TUR = Turkey, RUS = Russian Federation, SAF = South Africa, USA = United States and ZWE = Zimbabwe.

Bron: OECD (2023).

**The impact of geo-economic fragmentation on the Dutch economy exposes financial institutions to credit risk, market risk, and inflation risks.**

Disruptions in global value chains and energy and commodity markets can have negative effects on global trade and economic growth. The same applies to industrial policies aimed at producing strategic goods locally and to initiatives aimed at repatriating production from abroad (reshoring). These developments could have an upward effect on prices in the short to medium term as imports are replaced by more expensive alternatives.<sup>21</sup> Analyses conducted by the Netherlands Bureau for Economic Policy Analysis (CPB) and DNB indicate that an increase in geo-economic fragmentation is exerting downward pressure on economic growth

and real incomes in the Netherlands, contributing to higher inflation and leading to an uptick in unemployment.<sup>22</sup> This impacts the balance sheets of financial institutions. For example, a 2023 stress test, conducted by the European Banking Authority (EBA), on 70 European banks demonstrates that geopolitical developments, including lower growth, higher inflation, and higher interest rates, have a considerable impact on banks' capital positions. Banks' capital ratios deteriorate significantly, however, banks are able to absorb this shock as their starting positions have improved since the financial crisis.<sup>23</sup> At the end of this year, the European Insurance and Occupational Pensions Authority (EIOPA), will present the results of a stress test with a geopolitical scenario for insurance firms.

21 ECB (2023) [The EU's Open Strategic Autonomy from a central banking perspective](#).  
 22 See CPB (2024) and DNB (2023).  
 23 EBA (2023) [2023 EU-wide stress test: results](#).

## Box 2.1

**Geopolitical risks and insurance claims**

**Insurance firms are exposed to geopolitical risks not only through their investments, but also potentially through their insurance liabilities.** Insurance firms are exposed to underwriting risks stemming from the insurance coverage they provide. Geopolitical events can result in unanticipated growth in claims, particularly for non-life insurance firms operating in specific segments, such as aviation and marine insurance. These are often niche insurers. It is common practice for large business risks to be placed with foreign insurance firms or insured on the exchange through co-insurance, whereby the risk is borne by multiple insurance firms. Similarly, indirect effects of geopolitical risks can affect the claims burden of non-life insurance firms. For example, inflation can lead to higher claims and payments. It is crucial for insurance firms to maintain vigilance and, when appropriate, adapt their policies to minimise the adverse effects on their financial position.<sup>24</sup>

**Outside the Netherlands, insurance firms are reducing or cancelling coverage in order to manage risks, particularly in regions that are prone to geopolitical instability.** Aviation insurance firms have limited the coverage they offer to airlines based in Israel and Lebanon.<sup>25</sup> Insurance for commercial shipping in the Red Sea and the Strait of Hormuz is also under pressure, due to attacks by Houthi forces.<sup>26</sup> Where insurance coverage is restricted, firms should bear the consequences of damage themselves. It is crucial for insurance firms to ensure that the wording in their policies accurately reflects their desired risk exposures, particularly with regard to coverage and exclusions. This is essential for underwriting risk management. They should also pay particular attention to so-called 'silent coverage', which arises when policies do not explicitly exclude certain risks, leaving insurance firms facing claims not anticipated when setting premiums.<sup>27</sup> Dutch non-life insurance firms are not permitted to provide coverage for claims resulting from or related to armed conflict, civil war, insurrection, internal disturbances, riots, or mutiny occurring within the Netherlands.<sup>28</sup> The financial risks associated with covering these risks are significant enough to potentially cause financial difficulties for insurance firms if these risks materialise.

**When reinsurance firms limit insurance coverage, the risks to the original insurance firm may go up.** Insurance firms can mitigate underwriting risks by reinsuring them, in whole or in part. If a reinsurance firm withdraws or adversely changes the terms of coverage, insurance firms may face an increase in the underwriting risks to which they are exposed. Where reinsurance firms choose to continue providing cover, geopolitical risks may be reflected in higher premiums or uninsured risks.<sup>29</sup> Insurance firms are therefore well-advised to keep a close eye on these developments.

<sup>24</sup> See also DNB (2023), [Good practice document for inflation risk of insurance firms \(Dutch\)](#).

<sup>25</sup> Reuters (2023) [Exclusive: Aviation war insurers cancel some cover for Israel, Lebanon](#).

<sup>26</sup> See, for example, Reuters (2024) [War insurers shrug off Rubymar sinking in Red Sea, rates stable](#).

<sup>27</sup> This is the case, for example, with cyber risks. See also DNB (2022) [Insurers in a changing world](#).

<sup>28</sup> This is known as the war risk prohibition ([Section 3:38 of the Wft, Dutch](#)). The prohibition only covers insurance firms supervised by DNB. In addition, an exception has been made for marine, transport, aviation and travel insurance, provided DNB has not raised any objections.

<sup>29</sup> Insurance Insider (2023) [Geopolitical risk: A growing threat to insurer profitability](#).

## 2.2 Increased risk aversion, volatility, and the impact on funding costs

**Geopolitical developments can lead to financial market volatility and price shocks, creating market risks and affecting financial institutions' share prices.** Geopolitical risks and their materialisation can cause rapid shifts in market sentiments and price shocks. Also, a more subdued economic outlook and upward price pressures driven by geopolitical developments may affect market participants' expectations of corporate profitability. Geopolitical shocks are thus associated with lower equity valuations, higher risk premia, and increased volatility. Valuations of the transport and aviation sectors and parts of manufacturing, including the steel industry, have appeared particularly sensitive to geopolitical shocks. However, share prices of banks and insurance firms react more strongly to geopolitical shocks than the average for all sectors in the economy.<sup>30</sup> Incidentally, market reaction tends to fade, and recovery occurs some time after a shock, but with greater and prolonged tensions and heightened uncertainty, geopolitical events can affect financial markets for longer.

**Increased uncertainty and impediments to cross-border capital flows act as a brake on diversification.** Capital restrictions limit the ability of financial institutions to diversify, which can have adverse effects on the shock resilience of the financial system. Increased uncertainty and risk aversion also affect the volume and direction

of cross-border capital flows. For example, IMF research shows that increasing tensions between countries have a negative impact on the volume of cross-border capital flows between them.<sup>31</sup> Such de-risking by financial institutions may further encourage fragmentation.

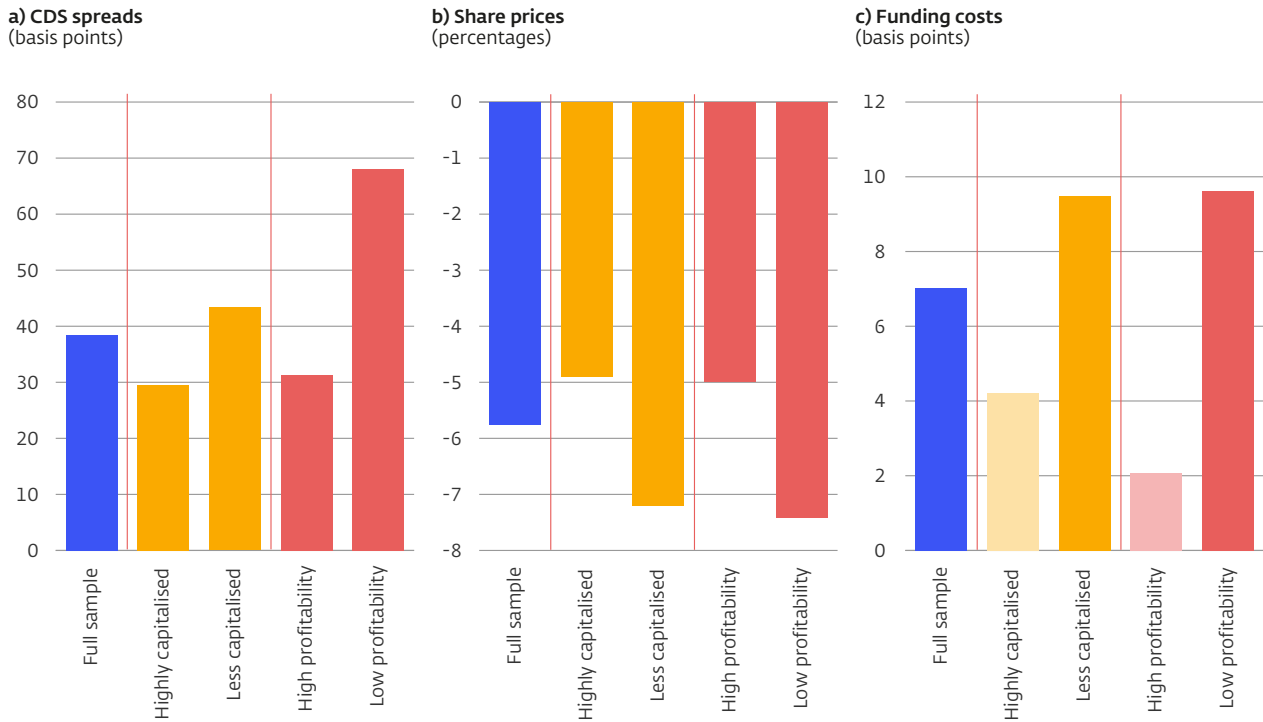
**Uncertainty, risk aversion and capital restrictions can also have adverse effects on financial institutions' funding costs.** Recent ECB research shows that an increase in geopolitical risks is associated with a rise in European bank bond yields, implying that it is more expensive for banks to raise new market funding.<sup>32</sup> Also, risk premia on credit default swaps (CDS) of European banks go up when geopolitical risks increase. For financial institutions that are less capitalised or for those that are less profitable these effects are much more pronounced, as Figure 4 shows. In addition, an increase in geopolitical risks could lead financial institutions to rely more on short-term funding, creating potential refinancing risks. Higher funding costs, increased risks and heightened uncertainty may then make banks more reluctant to extend new credit. This, in turn, could result in tighter financing conditions for firms and households. Divergent developments in financial markets and the real economy can thus be mutually reinforcing, with the combination of higher funding costs, lower credit demand and deteriorating loan portfolios adversely affecting banks' profitability.

<sup>30</sup> See Caldara, D. and Iacoviello, M. (2022) [Measuring geopolitical risk](#).

<sup>31</sup> IMF (2023) [Geopolitics and financial fragmentation: implications for macro-financial stability](#).

<sup>32</sup> ECB (2024) [Financial Stability Review: Turbulent times: geopolitical risk and its impact on euro area financial stability](#).

Figure 4 Stronger market reaction among less capitalised banks



Note: The coefficient estimates in this figure show the effect on CDS spreads, equity prices and funding costs of a one-standard deviation increase in the ECB-constructed geopolitical risk index (GPR index) at the bank level. The GPR index is a news-based measure of geopolitical risk, in which a higher value reflects a higher probability or intensity of adverse geopolitical risk (see Caldara and Iacoviello (2022)). To obtain a bank-level GPR index, the ECB weighted the country-level GPR using ECB supervisory data on the geographical exposure of bank assets. The coefficient estimates are based on a panel regression on a sample of 34 significant institutions for CDS spreads, 31 institutions for equity prices and 37 institutions for funding costs, for the period from the first quarter of 2015 to the third quarter of 2023. Banks with a capital ratio above the median are categorised as high capitalisation, banks with a capital ratio below the median as low capitalisation. For profitability, too, the distinction is based on the median observation. All coefficient estimates are statically significant at a 10% significance level, except for the lightly displayed estimates. A more detailed explanation can be found in ECB (2024).

Source: ECB (2024)

### 2.3 Geopolitical uncertainties underline the importance of proper risk management

**The importance of timely identification and adequate management of risks is underscored by increased geopolitical tensions and uncertainties.** DNB expects financial institutions to understand and manage all material risks, which requires them to embed geopolitical

risks in their strategy, risk appetite and risk management cycle. This applies to both financial risks, which have been covered in this chapter, and non-financial risks, which are discussed in more detail in the following chapters. Such comprehensive embedding is important, as geopolitical developments can affect institutions through diverse and mutually reinforcing (risk) channels. The ECB and the three European



supervisory authorities for financial institutions have also recently pointed this out.<sup>33</sup> Embedding requires, among other things, that tasks and responsibilities for the monitoring and control of geopolitical risks are appropriately and explicitly assigned in an organisational structure, in line with the risk profile. It is equally important that an institution's policymakers have sufficient knowledge, experience and skills in the area of geopolitical risks to be able to assess the institution's exposures to these risks and make balanced decisions about them.

**Forward-looking instruments, including stress tests and scenario analyses, are helpful in identifying (operational) vulnerabilities, concentration risks and the effectiveness of business strategies.** Periodically conducting stress tests with geopolitical scenarios that include effects on economic growth, inflation and interest rates helps to identify the impact of various geopolitical risks on an institution's financial soundness. Several banks, insurance firms and pension funds have also gained experience with this in recent years. The scenarios of these stress tests should be carefully chosen, considering the nature of institutions' activities and vulnerabilities. Extreme but plausible scenarios with severe economic headwinds offer them by far the most insights into potential vulnerabilities. For example, a scenario of further escalation of the tensions between China and Taiwan could be considered. Complementing these stress tests with targeted scenario analyses can also provide insights into risks that cannot be captured by credit and market risk models, such

as scenarios in which sanctions lead to the forced cessation of operational activities. This helps to identify operational vulnerabilities and the impact of geopolitical developments on business model resilience. Supervisors have a role to play in challenging institutions' stress tests and scenario analyses. Conducting their own stress tests helps them enrich their own insights and identify vulnerabilities and promotes transparency and market discipline.

**In addition to identifying geopolitical risks, it is important that financial institutions can also manage them.** Managing geopolitical risks requires, among other things, that institutions in their investment and lending policies consider the extent to which firms to which they are exposed manage geopolitical risks. Diversification – both in terms of geographical spread, and across different sectors, customer groups and products offered – will always be an essential part of a robust business strategy. In addition, institutions should not only develop credible capital, liquidity and funding plans that take into account uncertain prospects, but also be able to adapt them to changing risks in a timely manner. By extension, financial institutions also need to have plans ready to responsibly cease operations in vulnerable jurisdictions. This requires that they have the necessary capacity and resources to implement such plans, with the right priority. Finally, it is important that institutions have adequate buffers to cope with materialising financial risks. Shock-resistant and well-capitalised institutions are better able to maintain market access in times when geopolitical risks materialise.

<sup>33</sup> See ECB (2024) [Global rifts and financial shifts: supervising banks in an era of geopolitical instability](#) and the EBA, EIOPA and ESMA report (2024) [ESAs warn of risks from economic and geopolitical events](#).

# The changing cyber threat landscape gives rise to risks

Due to a combination of geopolitical developments and increasing digitalisation, the overall cyber threat is growing, and the threat landscape is becoming more complex. Financial institutions are exposed to operational risks, including through (critical) suppliers, which can have wider implications for the financial system through contagion and a loss of trust. The changing threat landscape highlights the need for operational resilience of institutions, their supply chain partners and market infrastructures. Besides keeping cyber security in order, continuity measures for a smooth and safe recovery also require attention.

## 3.1 The changing threat landscape gives rise to increasing cyber risks

**The threat landscape is becoming more dynamic due to geopolitical developments combined with increasing digitalisation.**

Recent years have seen a global increase in both the number and the severity of cyber-attacks.<sup>34</sup> This is due in part to the further digitalisation of society and increased technological capabilities. Geopolitical developments likewise translate into an increased cyber threat and a changed threat landscape. For example, ECB research shows that the number of cyber-attacks increases in times of mounting geopolitical tensions.<sup>35</sup> Moreover, cyber-attacks carried out by state actors have become the new normal, according to the NCTV.<sup>36</sup> Box 3.1 discusses this in greater detail.

**Financial institutions are a potential target of cyber-attacks, including those of state actors.**

This is driven by their assets and sensitive customer information and the pivotal role they play in society,

which makes financial institutions an attractive target for cyber-attacks. Data from the European Network and Information Security Agency (ENISA) on cyber-attacks reported in the media show that almost 10% of all cyber-attacks target the financial sector.<sup>37</sup> The vast majority of cyber-attacks with a potentially high impact on the financial sector are financially motivated. They are conducted by organised criminal groups. Examples include ransomware attacks, such as the ransomware attack on the US subsidiary of the Industrial and Commercial Bank of China (ICBC), which temporarily disrupted clearing services in the US Treasury market.<sup>38</sup> The financial sector is also an interesting strategic target for state actors and hacktivists because of the potentially large impact that disruptions can have.<sup>39</sup> Some of the cyber-attacks aim to cause (societal) disruption. DDoS attacks accounted for the vast majority of these types of attacks, which had little or no impact. The DDoS attacks carried out by pro-Russian hackers on Dutch and other European banks are a case in point.

<sup>34</sup> See the CISSM Cyber-attacks Database, which provides insight into cyber-attacks carried out since 2014. It should be noted that attacks carried out on US companies are over-represented in this database. The increase in cyber incidents may also be partly due to a higher reporting frequency. At the same time, the number of actual cyber incidents is likely to be underestimated, partly because of reluctance to report incidents or because they have (as yet) gone undetected. See Harry, C. and Gallagher N. (2018) *Classifying cyber events* for more details about this database.

<sup>35</sup> ECB (2022) *Towards a framework for assessing systemic cyber risk*.

<sup>36</sup> See also NCTV (2023), *Cyber security landscape in the Netherlands, 2023*.

<sup>37</sup> ENISA (2024) *Threat Landscape 2024*.

<sup>38</sup> The Banker (2023) *The significance of the ICBC FS hack on the US Treasury market*.

<sup>39</sup> State actors may also have other motives, such as amassing financial resources. The cyber-attack on the central bank of Bangladesh, attributed to North Korea, in which \$81 million was stolen, is a prime example. (Financial Times, 2019).

Box 3.1

**State actors increasingly operate in the digital domain**

**State actors are taking a more prominent place in the cyber threat landscape.** State actors and state-affiliated actors, whether as part of hybrid warfare or not, deploy cyber-attacks to influence, spy, disrupt and sabotage, or to take the preparatory steps to do so. Cyber-attacks are attractive because of their comparatively low cost, potentially long-lasting effects and because it can be difficult and complex to track down a perpetrator of a cyber-attack. State actors often use sophisticated attack techniques and typically have time, capacity and resources available.<sup>40</sup> This also allows them to carefully plan attacks and strike at the most strategic moments. For example, the FBI discovered a dormant network of Chinese hackers in the United States that had compromised hundreds of routers and was on standby to launch an attack.<sup>41</sup> It is also common for states to employ cyber criminals, to tolerate their activities, or to encourage them to attack specific targets. This blurs the distinction between state actors and cyber criminals.

**Just like other European countries, the Netherlands is continuously faced with offensive cyber-attacks and espionage,** the MIVD and AIVD indicate.<sup>42</sup> Although conducting cyber operations against Ukraine – for example, mapping the locations of Ukrainian military equipment and sabotaging vital infrastructure – is the top priority for Russian state actors, the MIVD indicates that 2023 also saw an increase in cyber operations by Russian state actors against European and NATO-allied targets.<sup>43</sup> According to the MIVD, their main motive is to obtain a digital position within the Netherlands' vital infrastructure. Russia is also attempting to use cyber espionage to detect shipments of Western military assistance both inside and outside Ukraine. According to the MIVD, the intensity with which Chinese state-sponsored hacking groups spy on the Netherlands and other EU Member States also increased last year. Chinese cyber activities are focused on gathering information on intellectual property, personal data and inside information on political and administrative decision-making. In 2023, several Dutch government agencies, firms and defence contractors were targets of espionage by Chinese cyber units.<sup>44</sup>

**There has been a resurgence of hacktivism, or ideologically motivated cyber-attacks, since the war in Ukraine.** Many cases, according to the European Network and Information Security Agency (ENISA), involve DDoS attacks. According to ENISA, the effects of these attacks are usually short-lived and limited. However, some of them have become larger and more complex in recent years.<sup>45</sup> Examples include DDoS attacks by pro-Russian hacker groups on government and corporate websites from countries that have imposed sanctions on Russia, including the United States, Italy, Norway and

40 ENISA (2023) [Threat landscape 2023](#).

41 New York Times (2024) [F.B.I. Director Warns of China Hacking Threat](#).

42 AIVD (2023) [Annual Report 2022](#) and MIVD (2024) [Annual Report 2023](#).

43 MIVD (2024) [Annual Report 2023](#).

44 Ministry of Defence (2024) [MIVD reveals modus operandi of Chinese spies in the Netherlands \(Dutch\)](#).

45 ENISA (2023) [Threat landscape 2023](#).

Japan, and attacks on banks in the Netherlands, Germany, the Czech Republic and Poland, among others.<sup>46</sup> Pro-Russian hackers have also called for DDoS attacks on Dutch hospitals. In fact, several Dutch hospitals have been the victims of such attacks, some of which resulted in their public website to go down for a short time.<sup>47</sup> Hacktivism is also resurging elsewhere. For example, Taiwanese government websites faced a surge in DDoS attacks ahead of a visit of the Speaker of the US House of Representatives.<sup>48</sup> The growing network of hacktivist groups could play into the hands of state actors by allowing them to pose as hackers in the future, Germany's federal security agency has warned.<sup>49</sup>

**Moreover, financial institutions are exposed to cyber risks through their critical IT suppliers.**

This happens because financial institutions are increasingly using third parties for their critical business processes, these can be cloud service providers or IT firms delivering other specialized tools. Poorly executed critical services or processes can have material consequences for an institution's soundness, continuity, or reputation, for example. Although larger IT service providers tend to have a lot of expertise and high standards for cyber and information security, the outsourcing of critical services or processes by financial institutions leads to increased dependency and added complexity. Cyber attackers are aware of these supply chain dependencies. According to ENISA, in recent years there has been a shift in the nature of cyber-attacks conducted by state and state-affiliated actors. Increasingly, third parties in the supply chain are being targeted.<sup>50</sup> The hack of US software company SolarWinds in 2020, from which several US government agencies and firms purchased services and was attributed to Russia, illustrates the potential consequences of such

attacks.<sup>51</sup> Although not a cyber-attack, the global communications technology outage caused by a software update flaw at US-based CrowdStrike is another example of chain dependencies. It affected an estimated 8.5 million Windows devices in the summer of 2024 and led to flight cancellations and postponements of hospital surgeries across the globe.<sup>52</sup> Finally, outsourcing can lead to concentration risks. A limited number of IT service providers serve a large number of financial institutions, while at the same time IT services are often not easily substitutable. With three major US players holding almost three-quarters of the European market for cloud-services, the heavy reliance on US cloud service providers is striking.<sup>53</sup>

**In case of contagion or a wider loss of trust, cyber incidents can also affect the financial system as a whole.** In comparison to other operational risks, cyber incidents are unique in the speed and scale with which they can spread within an institution and across institutions, sectors, and countries. The rapid, global spread in 2017 of the NotPetya malware is a case in point.

46 See ENISA (2023), Reuters (2023) and Center for Strategic & International Studies (2024).

47 See also NCTV (2023), *Cyber security landscape in the Netherlands, 2023* (Dutch).

48 ENISA (2023) *Threat landscape 2023*.

49 BSI (2023) *The state of IT security in Germany 2023*.

50 ENISA (2022) *Threat landscape 2022*.

51 ENISA (2021) *Threat landscape for supply chain attacks*.

52 Financial Times (2024) *Companies around the world hit by Microsoft outage*.

53 Gomes, A. and Okano-Heijmans, M. (2024) *Too late to act? Europe's quest for cloud sovereignty*.

It caused government systems in Ukraine to fail and triggered problems at Ukrainian power plants. Danish container carrier Maersk also suffered substantial damage.<sup>54</sup> Cyber-attacks can also rapidly spread through the financial system, for example because many institutions depend on underlying market infrastructures and share payment and capital market transaction systems. Cyber incidents can cause financial and reputational damage to an individual institution, as well as legal risks, in case unauthorised access to data is not reported in time or turns out to be the result of the institution's own negligence. A cyber incident's impact can spread to other institutions, for instance if it causes a wider loss of trust and an outflow of deposits. Institutions can also be adversely affected through the interconnectedness of the interbank payment system. This may be the case if banks face liquidity problems because other banks are unable to make payments because of a cyber incident. This also makes cyber risks relevant from a financial stability perspective, as recently explained in our Financial Stability Review.<sup>55</sup>

**(Cyber) incidents in other sectors, such as telecom and energy, could have potentially far-reaching consequences for the financial sector.** Like internet and data services and the production and distribution of electricity, payment transactions are classified as vital processes in the Netherlands.<sup>56</sup> Failure, (digital) disruption or

manipulation of vital infrastructure, whether deliberately caused or not, can compromise national security or lead to social disruption. Thus, in the event of a prolonged electricity supply outage, many chain effects in other sectors can be expected.<sup>57</sup> Substantial chain effects also occur in the case of prolonged disruption of telecom services, leaving users without access to internet and telephone services, with potential knock-on effects on the financial sector.<sup>58</sup> Although no actual digital disruption or physical sabotage of vital infrastructure has been reported in the Netherlands to date, according to the AIVD, MIVD, NCTV vital processes in the Netherlands are potentially vulnerable to state activities.<sup>59</sup> They point to the threat to submarine infrastructure, such as cables and pipelines, the activities Russian entities are undertaking to map this infrastructure, and the preparatory actions they are taking for possible disruption and sabotage. The Advisory Council on International Affairs (AIV) also points to the vulnerabilities associated with the large quantities of internet and electricity cables and gas pipelines in the North Sea and the high concentration of data flows over networks in the Netherlands.<sup>60</sup> There are also concerns elsewhere about the vulnerability of vital infrastructure. These have been prompted in part by suspicious incidents such as the sabotage of internet cables in France, GPS disruptions in Finland and the risk of dormant hacker cells in vital infrastructure in the United States as

54 See, for example, NCTV (2018) and Wired (2018) and Maersk (2017).

55 See also DNB (2024) Financial Stability Report, Autumn 2024.

56 The assessment of whether a particular process or service is vital is made by Dutch ministries, in consultation with the NCTV. This involves analysing whether the disruption, failure or manipulation of a process or service could have consequences serious enough to harm national security. Currently, the following processes and services have been identified as vital (see [here](#)). The government is currently going through a policy cycle to consider which processes or providers are to be identified as vital (Dutch central government, 2024).

57 See, for example, National Security Analyst Network (2022) [Theme Report on Threat to Vital Infrastructure \(Dutch\)](#).

58 Box 2 in DNB (2024) Financial Stability Report, Autumn 2024, describes a scenario in which a cyber-attack on vital infrastructure could cause systemic risks to the financial sector.

59 AIVD, MIVD and NCTV (2022) [Threat assessment of state actors 2](#).

60 Advisory Council on International Affairs (2024) [Hybrid threats and societal resilience](#).

highlighted by the FBI.<sup>61</sup> The Netherlands, like other EU Member States, may face chain effects of sabotage of vital processes in other countries.

**In addition to cyber-attacks, financial institutions may face disinformation, which has the potential to create liquidity risks.**

The risk of disinformation has been evident, during the COVID-19 pandemic, in the run-up to and during the war in Ukraine, and during recent elections. Where in all cases a variety of state actors regularly disseminated deliberately misleading information. It is quite conceivable that the spread of disinformation will further increase in scope and intensity in the coming years. Developments in generative artificial intelligence help to create and disseminate credible disinformation in textual, visual and audio form more quickly.<sup>62</sup> Financial institutions, too, may face the spread of disinformation. For instance, malicious actors could spread fake news about the financial position of one or more banks to stir up unrest among depositors to cause social upheaval. In particular, they could find fertile ground with depositors when confidence in a bank and/or the financial sector is already under pressure.<sup>63</sup> The potential risks involved are illustrated by the spread of fake news about the financial health of Bulgarian banks in 2014, which led to depositor withdrawals of around 10-20% of the total assets of two major Bulgarian banks.<sup>64</sup>

**Finally, insider threats also warrant attention.**

Financial institutions have strengthened their cyber defences in recent years to fend off external

attacks, increasing the possibility of malicious insiders gaining access to critical systems and sensitive data. Recruiting or positioning employees willing to provide malicious actors with access to financial institutions is an alternative to the efforts required to breach an institution's cyber defence. This risk is already visible in the tech sector, where insider threats are mostly motivated from gaining access to high-value technological knowledge. Because of this increased risk, tech companies in Silicon Valley have announced they are stepping up their staff screening.<sup>65</sup>

**3.2 Strengthening operational resilience requires constant effort**

**The changing threat landscape highlights the need for resilience of institutions and their supply chain partners. The entry into effect of the European Digital Operational Resilience Act (DORA) is a welcome development.**

Although attention to cyber risks in financial institutions is growing and steps have been taken in recent years to improve resilience, further efforts are necessary to bring information and IT security to the desired level of maturity. For instance, supervisory examinations show that banks, insurance firms and pension funds still have steps to take to put basic cyber hygiene measures in place, such as installing system updates and patches timely. There is also room for improvement in managing risks related to the outsourcing of critical processes and in running drills and preparing for cyber-attacks.<sup>66</sup> With DORA entering into effect in January 2025, European policymakers

61 Pillai, H. (2023) [Protecting Europe's critical infrastructure from Russian hybrid threats](#) and Financial Times (2024) [FBI warns Chinese malware could threaten critical US infrastructure](#).

62 See, for example, AFM and DNB (2024) and Bontridder, N. and Poulet, Y. (2021).

63 Bateman, J. (2020) [Deepfakes and synthetic media in the financial system: assessing threat scenarios](#).

64 Merler, S. (2014) [Fact of the week: A spam newsletter caused a bank run in Bulgaria](#).

65 Financial Times (2024) [Silicon Valley steps up staff screening over Chinese espionage threat](#).

66 See DNB (2023) for the outcomes of these supervisory examinations for banks and payment institutions, DNB (2023) for insurance firms, DNB (2023) for the pensions sector, and DNB (2023) for cyber strategy.

aim to further strengthen the digital operational resilience and IT security of financial institutions and harmonise it at European level. For instance, DORA requires financial institutions to report serious IT-related incidents to the competent supervisory authority and provides a mechanism to exchange information on incidents between supervisory authorities. Furthermore, threat-led penetration testing will become mandatory for the largest financial institutions. DORA also imposes stricter requirements for managing IT and cyber risks in outsourcing chains, including requiring institutions to conduct due diligence on potential IT providers and to develop exit strategies for critical IT service providers.<sup>67</sup> DORA also identifies concentration risks and introduces an oversight framework under which European supervisory authorities can conduct inspections at critical third-party IT service providers in tandem with national supervisory authorities. Together with the AFM, DNB will monitor that institutions implement the requirements arising from DORA.

**In addition to having, maintaining, and regularly testing robust IT and cyber security, it is important that institutions have the resilience to start up and continue services securely and smoothly after incidents.** There is no such thing as complete digital security, which is why it is important that institutions have the agility required to respond and recover securely and smoothly after an incident, even in the event of disruption to IT systems. This helps to ensure continuity of services and mitigate potential loss of trust and contagion risks. While the financial sector is increasingly focusing on strengthening its resilience and taking measures to ensure the highest possible

continuity of essential services, the results of the ECB's recent cyber stress test show that there is still room for improvement.<sup>68</sup> Key ingredients for an effective response are a culture where cyber incidents are quickly detected and reported, as well as clearly defined roles and responsibilities among management. It is also important to have playbooks in place, which are periodically reviewed, updated where necessary and subjected to practice drills. The entry into force of DORA also imposes new requirements on institutions' continuity plans and backup policies. Given the changing threat landscape, it is also prudent for financial institutions - and by extension, regulatory authorities, and governments - to prepare for scenarios in which they become the target of disinformation. This also requires thinking about an appropriate communication strategy for such scenarios. In conclusion, institutions also bear indirect responsibilities for the resilience of the entire market infrastructure. Financial institutions are often linked directly or indirectly, either through partnerships or subsidiaries, to critical market infrastructure parties. Because of these links, financial institutions have an important responsibility in terms of resilience, as the market infrastructure is fundamental to the functioning of the entire financial system. Given the changing threat landscape, DNB therefore encourages institutions to keep prioritising their ability to recover quickly in the event of digital or physical disruptions, whether intentional or not.

**Resilient vital infrastructure requires central government leadership and strong public-private cooperation.** Firms and financial institutions are responsible for taking the necessary preventive and mitigating measures to ensure the continuity

<sup>67</sup> Official Journal of the European Union (2022) [Regulation 2022/2554 on digital operational resilience for the financial sector](#).

<sup>68</sup> ECB (2024) [ECB concludes cyber resilience stress test](#).

and resilience of their processes and services. This also applies for firms and financial institutions that are part of the vital infrastructure.<sup>69</sup> At the same time, efforts undertaken in the private sector may be insufficient to achieve the socially optimal level of protection. Furthermore, the exchange of information, cooperation and coordination between sectors and across borders do not come naturally.<sup>70</sup> This is why bolstering resilience also requires the government to take the lead, designing proactive policies and setting the pace for implementation.<sup>71</sup> In this context, recent European legislative initiatives - such as the Network and Information Security Directive (NIS2), which imposes a duty of care and notification on a much wider range of organisations than is currently the case, the Cyber Resilience Act, which aims to improve the cyber security of hardware and software, and DORA, which is specifically aimed at the financial sector - are important, positive developments that deserve to be vigorously implemented and operationalised. Sectoral regulators, including DNB and the AFM, are tasked with ensuring adequate compliance with the

resulting obligations and will also need to collaborate closely. As part of our cyber strategy, DNB is putting this collaboration into practice by also supporting, where appropriate within our mandate, the vital sectors most critical to the financial sector, such as the energy and telecom sectors.<sup>72</sup> Finally, there is also a role for government to take the initiative in large-scale exercises involving scenarios where multiple critical sectors face simultaneous incidents and require the activation of national contingency measures, with operational coordination provided by the National Cyber Security Centre (NCSC). This has been done before in several ISIDOOR crisis drills.<sup>73</sup> Importantly, the insights gained during such drills must then be fed back to increase resilience. Recent assessments show that key issues include the effective and efficient exchange of information between critical infrastructure providers, the distribution of roles and responsibilities in the event of a scale-up to national contingency measures, and the mobilisation of scarce cyber security knowledge and expertise in the event of major cyber incidents.<sup>74</sup>

69 Parties offering processes and services whose continuity is vital to Dutch society are referred to as vital providers. Ministries are responsible for designating such vital providers (see [here](#)).

70 Specifically for the financial sector, the tripartite crisis management body (TCO) is in place in the Netherlands. It engages in sector-wide crisis management to deal with operational disruptions in payment and securities systems. See also DNB (2023) [Cyber strategy](#).

71 See also CSR (2024) [Cyber Security Council calls on new cabinet: Netherlands must invest more in digital security](#).

72 DNB (2023) [Cyber Strategy](#).

73 Over 120 public and private sector organisations participated in the 2023 ISIDOOR cyber exercise (see NCSC, 2023).

74 See NCSC (2024) [Simulating a cyber crisis makes our country more resilient](#). Likewise, WRR (2024) [The Netherlands in a Fragmenting World Order](#) contains recommendations regarding the strengthening of cyber resilience.



# The changing sanctions landscape: challenges and risks for financial institutions

The number of sanctions imposed by (Western) governments in response to heightened geopolitical tensions is rising sharply. This is particularly true for financial sanctions. Financial institutions have an important responsibility in implementing these sanctions, which exposes them to reputational and legal risks. These risks are larger when sanctions compliance is inadequate, underlining the importance of well-designed operations. The changing sanctions landscape also poses risks due to the exposures and operations of institutions in potentially vulnerable jurisdictions, the extraterritorial effect of US sanctions, and potential backlash from sanctioned countries. It is therefore important that institutions have risk management in place to adequately identify and manage the risks arising from the growing number of sanctions.

## 4.1 Changed sanctions landscape gives financial institutions a more prominent role

**Western governments are increasingly imposing sanctions, particularly financial sanctions.** Sanctions are an attractive policy instruments for governments. Firstly, for upholding the international rule of law or standing up for peace and security, for instance when diplomatic efforts are insufficiently effective and military intervention is considered undesirable. Increasingly, sanctions are also used to pursue (strategic) interests at home and influence the policies of other jurisdictions.<sup>75</sup> The number of sanctions imposed has shown an upward trend for years, as shown in Figure 5. This development has a major impact both on the financial sector and on other sectors in the Netherlands.<sup>76</sup> Moreover,

especially since the 11 September 2001 terrorist attacks, sanctions have become increasingly ‘targeted’ or ‘smart’, thereby of a more financial nature.<sup>77</sup> Sanctions packages have since been focused more on restricting access to financial services or freezing assets to hurt specific regimes. Previously, sanction packages consisted mainly of embargoes against countries, which often had harmful side effects on local populations.<sup>78</sup> In response to Russia’s 2022 invasion of Ukraine, the EU, the United States and the United Kingdom, among others, have imposed a host of financial sanctions against Russia and Belarus, reflecting the reliance on financial sanctions. Assets of legal entities and individuals were frozen, and bans were imposed on providing financial services. The assets of the Russian central bank, thereby other Russian banks as well, were also frozen

75 See, for example, Wittmann & Teichmann (2022), Hoff & Hoff (2023) and Caytas (2017).  
 76 CBS (2023) *Dutch Trade in Facts and Figures, 2023*  
 77 See, for example, Rodriguez, F. (2023), Yotovm Y. et al. (2020) and Drezner, D.W. (2011).  
 78 See Ahn, D. (2019), GIATOC (2023) and Drezner, D.W. (2015).

(via Euroclear), transactions with this central bank were banned, and a number of Russian banks were excluded from the international messaging system for payments (SWIFT). This development, where global competition and international powerplay use (parts of) the financial infrastructure as a weapon, is sometimes described as *the weaponisation of finance*.<sup>79</sup>

**Financial institutions have an important role in the implementation of sanctions, given their pivotal role in the payments system, their status as gatekeepers to financial services, and their position as investors.** Financial institutions are required by law to be able to identify on an ongoing basis whether their customer relationships or investment parties are subject to sanctions regimes. They should verify whether services and transactions they provide relate to individuals, firms or other entities that are subject to sanctions regimes. This is on a continuous basis, not only when an individual or firm wants to become a customer or buy a new service, it also applies to existing customers. If customer due diligence reveals that a customer is

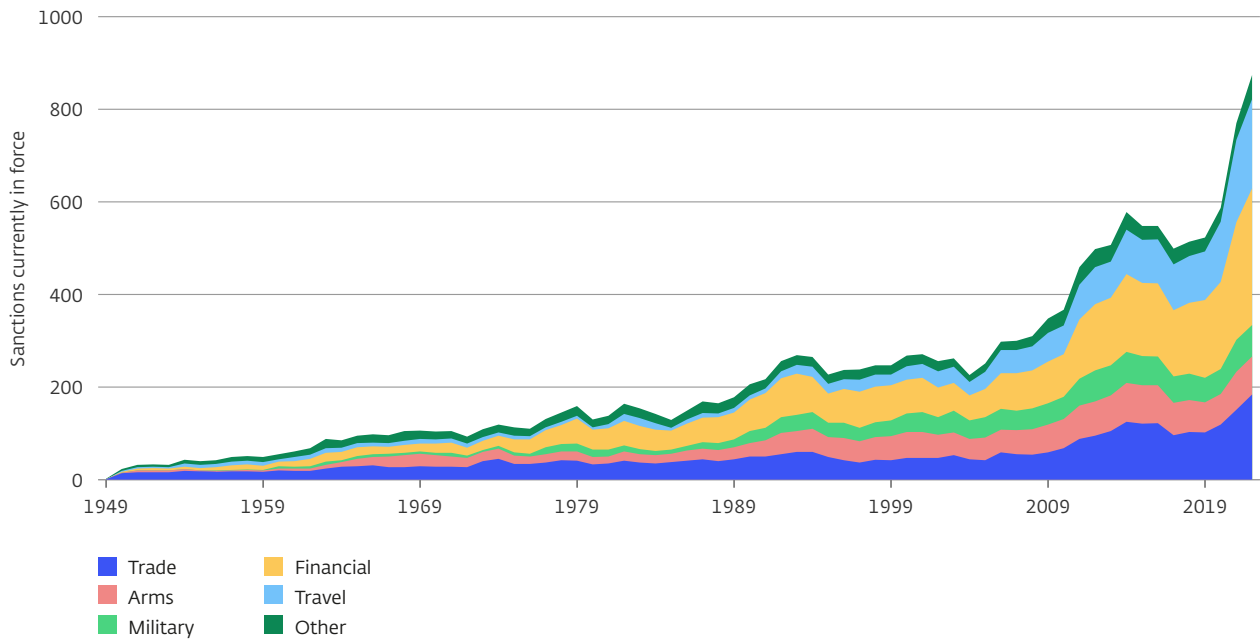
on sanctions lists, or that transactions - such as a funds transfer - to sanctioned parties are scheduled, a financial institution must immediately implement the sanction and submit a notification to DNB. It is not always possible to quickly check whether a particular customer is on a sanctions list. In the case of a firm, a financial institution will have to identify the ultimate beneficial owner (UBO) and determine who exercises de facto control over the firm. Financial institutions also have a role to play in other types of sanctions, such as import and export restrictions. This is because they may not be involved in transactions that do not comply with sanctions regimes. In the successive sanction packages against Russia and Belarus, a large number of bans and restrictions on the provision of financial services for military goods, goods for internal repression and dual-use goods<sup>80</sup> have been introduced. This has increased the importance of transaction monitoring and other detection measures. More broadly, financial institutions should be on their guard against the circumvention of sanctions. One of the ways in which this can occur is when goods are exported to another country before reaching sanctioned parties.<sup>81</sup>

79 See Financial Times (2022) *Weaponisation of finance: how the west unleashed 'shock and awe' on Russia*. The report issued by the Netherlands Scientific Council for Government Policy (WRR), (2024) *Netherlands in a Fragmenting World Order*, shows that the weaponisation of finance can be seen as part of a global process of generally expanding spheres in which power is exercised. Based on other reports, the WRR refers to this phenomenon as the 'weaponisation of everything'.

80 Dual-use goods are goods, services or technologies that can be used for both civilian and military purposes. For example, certain flame retardants are used in the construction industry but also serve as a raw material for poison gas.

81 The Economist (2024) *The mysterious middlemen helping Russia's war machine*.

Figure 5 Governments are increasingly imposing financial sanctions



Note: The figure shows publicly declared sanctions in force between states and organisations by year and type of sanction.

Source: The Global Sanctions Data Base (GSDB, 2023).

#### 4.2 Implications of the changed sanctions landscape on financial institutions

**The rise in the number of sanctions imposed increases the legal and reputational risks faced by institutions.** Sanctions rules may be breached both by the bank’s own active decisions, such as extending credit to a sanctioned party, and by the behaviour of customers, such as those who wish to transfer money to a sanctioned party. The implications for institutions can be significant, depending on the specific circumstances. If institutions do not have sufficient adequate internal policies to implement sanctions regulations, DNB and the AFM can take

enforcement action under administrative law and impose penalties. Violation of the Sanctions Act qualifies as an economic offence as well, which allows for criminal prosecution and can result in penalties of up to 10% of annual revenues. In addition to the impact of these sanctions on an institution’s financial position, involvement in enforcement actions or criminal proceedings can also lead to reputational risks. Finally, legal risks may arise if third parties adversely affected by the implementation of sanctions, for example by being unable to carry out transactions, take legal action against a financial institution. Risks are potentially larger, when the interpretation of sanctions is not clear and unambiguous. Although

sanctions regimes contain clauses that limit the likelihood of liability<sup>82</sup>, the initiation of proceedings may expose an institution to reputational risks, even if litigation has little chance of success.

**Besides European sanctions, sanctions imposed by the United States also have an impact on Dutch financial institutions.** Non-US parties are subject to the US sanctions regime in some cases, for example if they are involved in transactions with US parties or if the transactions involve US goods.<sup>83</sup> US sanctions have a de facto extraterritorial effect because a large proportion of international transactions are conducted in dollars. This provides the US authorities with a powerful policy instrument, which they frequently use.<sup>84</sup> The consequences of non-compliance with US sanctions laws can be substantial. In 2015, for example, BNP Paribas was condemned by US authorities for processing billions of dollars of transactions through the US financial system on behalf of Sudanese, Iranian and Cuban entities subject to US sanctions. BNP Paribas pleaded guilty and faced a fine of almost \$9 billion.<sup>85</sup> Several major Dutch banks were also subjected to investigations and reached settlements with US authorities. In addition to penalties, parties that act in violation of US sanctions laws run the risk of being denied access to the US financial markets and thus to dollar funding, or of being placed on sanctions lists themselves.<sup>86</sup> US authorities recently said they were keeping a close eye on whether European banks still operating in Russia were adequately complying with

US sanctions laws, warning that non-compliance could also result in banks themselves being sanctioned or denied access to dollar funding.<sup>87</sup> The ECB has repeatedly expressed its concerns about the slow progress of some banks in mitigating risks stemming from ongoing operations in Russia. These banks have therefore been urged to accelerate their exit strategies and reduce their holdings in Russia.<sup>88</sup> In addition to the ECB's own considerations, its call on banks is prompted by considerations related to US sanctions risks.<sup>89</sup>

**Financial and non-financial risks to institutions that were previously not on the radar have emerged from the changing sanctions landscape.** Although banks, pension funds and insurance firms had already largely run down their investments in Russia before the Russian invasion of Ukraine in spring 2022, they were forced to immediately write off their investments in Russian firms to (virtually) zero after the invasion. They were no longer allowed to trade in Russian assets because of European sanctions. Scenarios where investments in a jurisdiction become illiquid and (virtually) worthless overnight had not been previously considered. In addition, sanctions can also give rise to operational problems for institutions, as illustrated by the bankruptcy of Amsterdam Trade Bank (ATB) in 2022. Because of sanctions imposed by authorities in the United States and the United Kingdom on firms with Russian shareholders, IT service providers from

82 In this context, see also Article of [Regulation 269/2014](#).

83 See Amar, Y. and Bennink S. (2020) for more details of the US sanctions regime.

84 See Farrell H. and Newman A. (2024) *Underground Empire - How America weaponised the world economy*, Penguin Random House and Caytas, J. (2017) *Weaponising finance: US and European options, tools and policies*.

85 U.S. Department of Justice (2015) *BNP Paribas sentenced for conspiring to violate the International Emergency Economic Powers Act and the Trading with the Enemy Act*.

86 In 2018, for example, a Latvian bank faced a sharp outflow of deposits and a lack of access to dollar funding after US authorities announced that it had been designated as an institution with money laundering concerns under the US Patriot Act. As a result, the bank was in danger of collapsing, after which it was decided to liquidate it (see also ECB, 2018).

87 Reuters (2024) *European banks in Russia face 'awful lot of risk', Yellen says*.

88 Enria, A. (2023) *Letter to the members of the European Parliament*.

89 Financial Times (2024) *ECB pressures banks to speed up Russia exits on fear of US action*.

these countries were compelled to terminate their services. As a result, ATB could no longer have vital systems in place to meet its obligations to account holders and other counterparties and was forced to file for bankruptcy.

**More broadly, financial institutions may also face backlash from countries subject to sanctions.** European banks, still operating in Russia, are closely watched not only by European and US supervisory authorities (see above), but also by Russian authorities. They have recently threatened to seize the assets of banks operating in Russia that they deem ‘unfriendly’, subjecting them to additional, unexpected tax levies and restricting their ability to dispose of assets without loss.<sup>90</sup> Counter-reactions can also take other forms, such as pressuring third countries to adopt measures that reduce the earning power of Western banks operating there. Financial institutions can also become targets of cyber-attacks. For example, ENISA points out that Western sanctions against Russia provide an additional motive for Russian cyber criminals to carry out cyber-attacks against Western organisations, with these groups citing critical infrastructure as a potential target (see also Chapter 3).<sup>91</sup>

**Finally, the changing sanctions landscape may have broader implications for the functioning of the financial system at large.** Beyond the

sanctions that target legal entities and individuals, there has been an increase in sanctions that target or affect the full financial market and infrastructure. Examples such as the sanctions imposed on the SWIFT payment messaging system and the freezing of central bank deposits (by Euroclear), are illustrations of the weaponisation of finance. It is not inconceivable, and already becoming apparent, that applying such financial sanctions encourages other countries to develop their own infrastructure for settling cross-border transactions.<sup>92</sup> Russia, for example, developed its own messaging system for payments back in 2014 after being threatened with being cut off from SWIFT. The System for Transfer of Financial Messages (SPFS) is mainly used by banks in Russia and other countries from the former Soviet Union. China is also working on an alternative to SWIFT, the Chinese Cross-Border Interbank Payment System (CIPS), partly out of a desire to give its currency a more prominent role on the world stage.<sup>93</sup> In addition, France, Germany and the UK developed the Instrument in Support of Trade Exchanges (INSTEX) to continue to conduct transactions with Iran after the latter lost access to SWIFT due to US imposed sanctions.<sup>94</sup> Such initiatives reduce the interoperability of market infrastructure, making trade and financial transactions between different countries and regions more difficult, with potentially negative effects on global capital flows, international trade and global growth.<sup>95</sup> In addition, the use

90 See The Economist (2024) [European banks are making heady profits in Russia](#) and Financial Times (2024) [Western banks in Russia paid €800m in taxes to Kremlin last year](#).

91 ENISA (2022) [Threat landscape 2022](#).

92 Cipriani, M. et al. (2023) [Financial sanctions, SWIFT, and the architecture of the international payment system](#).

93 See, for example, Eichengreen B. (2022) [Sanctions, SWIFT, and China's Cross-Border Interbank Payments System](#) and Eichengreen B. & Kawai M. (2015) [Renminbi Internationalisation: Achievements, Prospects, and Challenges](#).

94 After the US pulled out of the Iran Nuclear Deal, European countries sought ways to continue facilitating transactions with Iran outside the US banking system (see, for example, Marineau, S. (2021) and CFR (2023)). Originally, INSTEX was not a success, but during COVID-19 it enabled European firms to supply humanitarian goods to Iran (The Economist, 2024). See also Batmanghelidj E. and Rouhi M. (2021) [The Iran Nuclear Deal and Sanctions Relief: Implications for US Policy](#).

95 See, for example, Greene, R. (2022) [How Sanctions on Russia Will Alter Global Payments Flows](#) and Cipollone, P. (2024) [Why Europe must safeguard its global currency status](#).

of the returns on Russian central bank assets or indeed the use of the frozen assets themselves, as earlier discussed by European policymakers, could have potentially far-reaching consequences. DNB, for example, has highlighted the economic and financial implications of using frozen Russian assets to support Ukraine, including the impact this could have on confidence in the euro and its attractiveness as a trading and reserve currency, and by extension euro-denominated assets for public and private parties outside Europe.<sup>96</sup>

### 4.3 Adequate compliance with sanctions regime while keeping a close eye on potential side effects

**Despite recent improvements, continued efforts are needed by financial institutions to ensure adequate sanctions compliance.**

**Financial institutions are bound by the Dutch Sanctions Act, which requires them to set up their operational management in such a way as to comply with sanctions regulations.**

Supervisory examinations conducted by DNB in 2023 and 2024 show that, although, institutions have taken the necessary steps in recent years, there are still shortcomings in the areas of screening, identification, risk management, and reporting of compliance with sanctions.<sup>97</sup> In addition, the maturity of sanctions compliance processes and systems varies across sectors. The overall performance of the banks examined appears to be adequate. However, there is still room for improvement, for example in the detection of dual-use items. Several shortcomings were found in the pension funds and insurance firms examined. For example, in the pensions sector, sanctions screening is regularly

outsourced, with insufficient safeguards to ensure that sanctions rules are actually complied with. Several insurance firms were found to be failing to properly carry out UBO screening. UBOs are not always identified, nor are they always screened against sanctions lists. DNB also found shortcomings among crypto service providers and in the trust sector, where the risk of sanctions circumvention is high. This is due to the large number of customers operating in the energy sector. DNB expects institutions to vigorously address the shortcomings identified and to reflect carefully on the experience of sanctions compliance in recent years, so that they are better able to respond to changes in the sanctions landscape. DNB will keep monitoring compliance closely.

**In addition to having adequate internal processes for sanctions compliance in place, it is important that institutions also identify and manage the potential risks arising from sanctions.** Rising geopolitical tensions are leading to rapid developments in the imposition of sanctions, which also means that the side-effects of sanctions - including counter-reactions from sanctioned countries - have the potential to occur rapidly. It is therefore important that they identify and manage potential risks associated with the implementation of sanctions and resulting adverse side effects. In particular, institutions will need to be mindful of their exposures in potentially vulnerable jurisdictions. and the same applies for their operational activities that take place, through outsourcing arrangements or otherwise, in those jurisdictions or that are vulnerable to potential backlash from sanctioned

<sup>96</sup> DNB (2024) [DNB joins Dutch House of Representatives roundtable over use of frozen Russian assets](#).

<sup>97</sup> See DNB (2024) [Integrity supervision in focus](#) and DNB (2023) [Sanctions Act examinations](#) for a more detailed explanation.

countries. Scenario analysis, which examines the impact of, for example, a significant haircut on the bank's own assets, those of its key customers, or on critical services or operational processes, can help identify vulnerabilities and provide starting points for the further development of exit and contingency plans.

**Institutions would benefit from further harmonisation of European sanction policy.**

While sanctions are laid down in European legislation, supervision and the policies that give effect to sanctions are a national matter. This means that EU Member States sometimes have different interpretations of sanctions, for example on the question of who has ultimate control of certain assets.<sup>98</sup> States also have the power to make exceptions to sanctions in special cases. The rules for making such exceptions are interpreted differently.<sup>99</sup> The lack of uniform interpretation of sanctions within the EU creates an uneven level playing field. In addition, institutions that operate in more than one Member State will have to take account of different interpretations. This can lead to legal and reputational risks as well as additional costs for institutions. Discrepancies also exist between Member States in terms of supervision and sanction enforcement. These include differences in the legal classification of non-compliance and the maximum penalties that can be imposed on offenders.<sup>100</sup> It is therefore a good thing that priority has been given to the harmonisation of the European policy on sanctions. The European directive adopted in the

spring of 2024, which requires member states to criminalise circumvention and breaches of EU sanctions, is a step in the right direction.<sup>101</sup> In general, institutions would benefit from closer harmonisation of sanctions policies, supervision and enforcement. An added benefit of such harmonisation is that sanctions can become more effective and sanctions compliance more efficient. It is therefore important for the Dutch Ministry of Foreign Affairs to continue working with the European Commission to further harmonise European sanctions policy. Ideally, policy and enforcement tasks could be entrusted to an independent European organisation, an option that merits serious exploration. If support for this option should be insufficient, our view is that Member States must commit themselves to a formal European interpretation of sanctions. The Q&As prepared earlier by the European Commission in this context are a step in the right direction. For this European interpretation to be sufficiently effective, it needs to be further formalised.

Finally, increased exchange between public and private organisations on sanctions reporting and circumvention can provide institutions with valuable information to improve sanctions compliance. The proposed International Sanctions Act (*wetsvoorstel internationale sanctiemaatregelen*), submitted for internet consultation in summer 2024 by the Dutch government, extends the obligation to report sanctions to more professions, including lawyers,

98 See, for example, recommendation 14 in Dutch central government (2022) Report of the National Coordinator for Sanctions Compliance and Enforcement, and CEPA (2024) *Europe's Russia Sanction Regime Cracks*.

99 See recommendation 16 in Dutch central government (2022) Report of the National Coordinator for Sanctions Compliance.

100 These differences complicate international cooperation between investigative agencies. They can only share data if the qualification of the non-compliance is the same in both Member States. In addition, data exchange can be problematic if the potential penalties for non-compliance differ widely between Member States.

101 [Directive \(EU\) 2024/1226](#)

civil-law notaries, and tax advisers. It introduces a central hotline for sanction notifications.<sup>102</sup> One of its tasks will be to collect and analyse reports which, combined with the extended reporting obligation, will give a more complete picture. This enables faster and better detection of patterns of sanctions evasion and circumvention. Sharing such information from this central hotline with financial institutions, where possible, is valuable. It provides institutions with starting points for improving sanctions compliance, thereby reducing risks for financial institutions. There seems to be scope for this as this information is not personal data. This also has the added benefit of making it more difficult for sanctioned parties to circumvent sanctions, which can increase the effectiveness of sanctions.

---

<sup>102</sup> Dutch central government (2024) [Proposed international Sanctions Act](#).




De Nederlandsche Bank N.V.  
PO Box 98, 1000 AB Amsterdam  
+31 (0) 20 524 91 11  
dnb.nl/en

**Follow us on:**

 LinkedIn

 Twitter

 Instagram

**DeNederlandscheBank**

EUROSYSTEEM