Annex – Implications of new cyber security measures in Germany

08 September 2023

Strong cybersecurity measures in Germany are important, but they need to be designed carefully to avoid imposing unnecessary costs on end-users and the wider economy

Cyber-attacks impose substantial costs on the economy and wider society. This threat will increase further as the uptake of connected devices increases and new technologies are developed. This means that all stakeholders, including governments, businesses, suppliers of digital goods and services, and consumers, have a strong interest in combating cyber threats.

The European Commission has addressed the threat with a suite of proposals including the NIS2 Directive, which aims to provide a common, transparent and risk based approach to implementing cybersecurity measures across the European Member States. The NIS2 Directive extends the 2016 NIS Directive and complements other cybersecurity policies such as the Resilience of Critical Industries Directive, 5G Security Toolbox and Digital Operational Resilience Act (DORA). At the time of writing, the NIS2 Directive is currently being implemented by the German Government and other Member States into their country specific cybersecurity laws and legislation.

Cybersecurity measures, when designed appropriately, should enhance the strength and resilience of cybersecurity practices, thereby ensuring that businesses and consumers can benefit from a reduction in the losses and frequency of security incidents. While enhanced cybersecurity measures are welcome, it is important to recognise that cybersecurity regulations can also impose substantial costs on businesses and the wider society depending on how it is implemented. This report estimates that the costs to implement the NIS2 Directive for Germany would amount to the following:

- an increase in costs for businesses of **€7.3 billion** to implement new regulations;
- higher downstream prices for the directly affected sectors but also higher prices in other sectors The NIS2 Directive provides a degree of discretion for policy makers to implement their country specific cybersecurity regulations. In implementing cybersecurity policies, there is a risk that Member States could impose obligations and restrictions which are either stricter than those envisaged by the NIS2 Directive or apply to a wider set of sectors than implied in the NIS2 Directive. This risk is heightened if cyber security policy is unduly influenced by unrelated policy goals (e.g. if cybersecurity regulation is used to achieve

geopolitical objectives or industrial policy goals rather than address the technical nature of the risks).

Policy makers in Germany have implemented cybersecurity policies that are proportionate and targeted at the technical nature of the risks. However, there is a concern that some of the recently implemented cybersecurity policies could lead to policy makers relying on non-technical factors (e.g. geopolitical factors) when assessing the cybersecurity risk of foreign vendors. This will have a negative net impact on consumers as these policies will lead to higher costs (e.g. lower competition and innovation) but it will not address nor mitigate the technical nature of the cyber-risks. This report estimates that the potential impact of vendor screening could amount to the following:

- a reduction in extra-EU exports of **€4.9 billion** and extra-EU imports of **€3.2 billion**; and
- a reduction in GDP of **€8.8 billion.**

Given this, policy makers in Germany should focus on "technical factors" when assessing the degree of risk (i.e. factors that directly relate to the technical cyber risk) as this will ensure that any regulatory action is targeted and proportionate.

There is also a risk that under-resourced cybersecurity authorities will resort to "easy to implement" policies (such as vendor screening bans based on non-technical criteria) which can impose significant costs on end-users. This is particularly important as new cybersecurity legislation[1] will expand the role of, and increase demands on, the Bundesamt für Sicherheit in der Informationstechnik (BSI). It will create more complex notification procedures (which the BSI must in turn examine and process in a timely manner). The German Government should therefore ensure that its cybersecurity authorities are sufficiently resourced to take on the additional responsibilities under the NIS2 Directive and address any concerns in a proportionate and targeted manner.

Germany has, in general, implemented cybersecurity policies in a proportionate manner but there is a concern that some of the recent policies have gone beyond the European Directives

German sector-wide cybersecurity regulations were first introduced within the IT Security Act (IT-SIG) 1.0 in 2016, which imposed cybersecurity obligations on businesses that operate within a range of sectors.[2] The German government subsequently updated these regulations

[1] IT-Sicherheitsgesetz 2.0 ("IT SIG 2.0"). https://www.bsi.bund.de/EN/Das-BSI/Auftrag/Gesetze-und-Verordungen/IT-SiG/2-0/it_sig-2-0_node.html

[2] This includes the energy, information technology and communications, transport and traffic, health, nutrition, finance and insurance sectors. This regulation imposed stronger obligations on sectors with "critical infrastructure" and these include the energy, water, food, and information technology and telecommunications sectors. See

in May 2021 by introducing the IT Security Act (IT-SIG) 2.0.[3] These regulations strengthened the existing framework by increasing the powers of the regulatory authority to detect and defend against cyber-attacks and introducing provisions to prohibit the usage of certain components.[4] [5]

In general, policy makers in Germany have implemented cybersecurity policies under the IT Security Acts in a proportionate manner as the regulations are focused on targeting and addressing the technical nature of the cybersecurity risks. However, there is a concern that the vendor screening policy and certification requirements under IT-SIG 2.0 could lead to substantial costs that outweigh the benefits of these policies.

IT-SIG 2.0 requires the German Government to screen and prohibit the use of components for operators of critical infrastructure based on a range of technical and non-technical factors. These non-technical factors include whether the manufacturer is controlled by the government of a third country and whether the use of component is consistent with the policy objectives of Germany, EU or NATO. The vendor screening policy further sets out different obligations on businesses in relation to new and legacy critical components.

- **New critical components** – IT-SIG 2.0 requires operators to notify the Federal Ministry of the Interior for Construction and Home Affairs before using and installing the component. The Ministry (in consultation with other ministries) will then determine whether to prohibit the use of a critical component or only permit use under a specified set of conditions.

- **Legacy components** – IT-SIG 2.0 allows the Government / Authorities to prohibit the continued use of critical components if the supplier is untrustworthy and/or the continued use of these components will have a negative impact on the public order and security of Germany.

https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s1324.pdf%27%5D__1670950604617

[3] See https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s1122.pdf%27%5D__1670950641581

[4] IT-SIG 2.0 further increased the number of sectors to include municipal waste management businesses and other sectors with special public interest entities (SPIEs) (e.g. arms manufacturers)

[5] There have further been amendments to other sector-specific laws which include provisions that are relevant to the security of IT systems. These include amendments to the Radio Equipment Act, the Telemedia Act, the Telecommunications Act, the Energy Industry Act and the Banking Act. See https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/germany

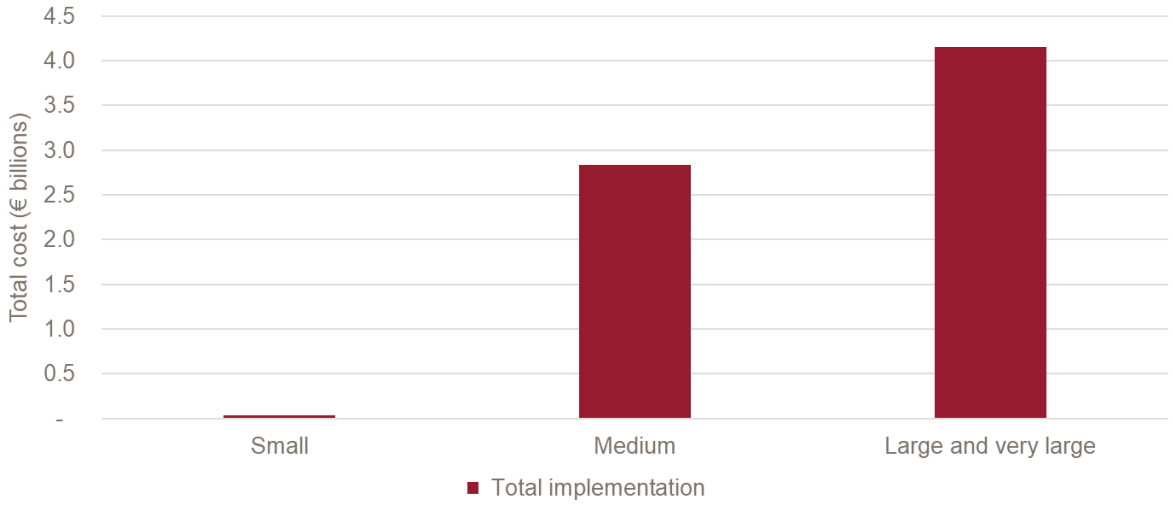
IT-SIG 2.0 also introduced mandatory certification obligations for operators of critical infrastructure[6] and special public interest entities (SPIEs)[7] to obtain / present certifications to demonstrate that their IT systems are secure.

Cybersecurity imposes direct costs on businesses affected

The cost of implementing the NIS2 Directive in Germany is estimated to be **€7.3 billion**. At a time where Germany's economy is undergoing low or stagnant growth[8] there may be limited scope for firms to absorb the increase in costs by increasing IT budgets. Instead it is likely that firms will reallocate existing budget by cutting back on planned investment which could in turn have knock on impacts on IT capabilities.

Figure 1 below further shows that the NIS2 Directive will have a proportionately larger impact on smaller businesses as the implementation costs as a percentage of business turnover is higher for small businesses than for larger businesses.

Figure 1 Cost of implementing NIS2 by business size



Source: Frontier Economics

The increase in implementation costs for the affected sectors could further have implications on downstream prices of both the affected sectors and other sectors – this is because businesses within the affected sectors may need to raise downstream prices in order to offset

[6] These include businesses within the energy, information technology and telecommunications, transport and traffic, health, water, food, finance, insurance and municipal waste disposal sectors.

[7] These refer to defence manufacturers and other operators of considerable economic importance to Germany (in terms of domestic value added) who are not operators of critical infrastructure.

[8] At time of writing (H2 2023) Germany's economy is expected stagnate in 2023 and grow by 1.3% in 2024. Eg see: https://issuu.com/oecd.publishing/docs/germany-oecd-economic-outlook-june-2023?fr=sNDI0MjUwNTY2MTA

the rise in compliance costs while other sectors that purchase inputs from the affected sectors may need to increase downstream prices in order to offset the rise in input costs.

Cybersecurity measures cause economic frictions which lead to costs

The imposition of NIS2 measures can in addition cause "frictions" in how firms trade with each other which has real costs to the economy. As discussed above, the cybersecurity measures add to the cost base of companies transacting in the EU, whether that be local firms serving the domestic market, looking to supply outside the EU, or be foreign suppliers serving the EU. In each of these cases, costs and prices will increase. However, there is no direct effect on a foreign supplier serving non-EU markets. This has potential to create a 'bifurcation' in the market, where suppliers from outside the EU find it more attractive serving non-EU markets and configure operations in that direction. With this reduction in imports from outside the EU, EU-based suppliers facing reduced competition will orientate more towards serving their 'home' market rather than non-EU markets. As a result, there is reduced trade between the EU and rest of the world with reduced benefits in terms of international competition and access to innovation and the full range of product offerings.

Discriminatory cybersecurity trade measures to exclude vendors will impose substantial costs

Discriminatory policies which "screen" which firms can supply goods and services will impose costs on businesses.[9] As discussed above, there is a risk that policy makers in Germany will use non-technical factors to screen potential vendors. This will likely have a negative net impact on consumers as these policies could lead to higher costs (e.g. lower competition and innovation) but it will not address nor mitigate the technical nature of the cyber-risks. This is especially the case as the usage of non-technical criteria will likely lead to error and inefficiency in the identification and treatment of cyber risks. Given this, policy makers in Germany should focus on using technical factors when assessing the degree of risk as this will ensure that any regulatory action is targeted and proportionate.

Discriminatory cybersecurity measures will increase costs of doing business within Germany

Even where screening measures do not 'bite', they impose additional compliance costs to prospective suppliers who must engage with the screening process, and add to regulatory uncertainty. Where the uncertainty is sufficiently large, this has the potential to outright deter

[9] Analysis by the OECD to quantify barriers to services trade using the Services Trade Restrictiveness Index (STRI) considers the impact of screening alongside a whole raft of other measures thought to be trade-restricting, such as barriers to foreign entry, movement of labour and barriers to competition. The STRI is weighted according to a consensus of expert judgement. In various empirical literature the STRI is found to have a negative effect on trade, so that screening has a negative effect alongside these other types of restriction.

investment, as there is a risk that the investment costs will not be recouped, and that the project is no longer viable. Transaction costs may have a disproportionate impact where there are already transaction costs related to doing business, such as sunk costs incurred in tailoring products to meet the specific needs of local markets. Local suppliers will also face impacts as a result of building relationships and transacting with parties who may subsequently be barred. So the chilling effect of discriminatory measures will affect both foreign and domestic suppliers.

Discriminatory cybersecurity trade measures will reduce competition and lead to increased costs

Discriminatory cybersecurity trade measures will likely create "economic frictions" that negatively affect trade, reduce competition and slow down innovation. Screening policies tend to have a negative net impact on consumers. This is because these screening policies will reduce the number of suppliers and could further deter potentially acceptable foreign suppliers from operating and investing in Germany as they may not consider it worthwhile to deal with the uncertainties and the processes. This could subsequently reduce competition and increase prices for a range of sectors (that will be additional to the costs highlighted above). These impacts can be felt in any sector where the need for specialised equipment means that there are limited supply of vendors, whether energy, medical devices or telecommunications equipment. For example, a recent report highlighted that vendor bans on 5G equipment could increase 5G equipment cost for Germany by **€479 million** per year over the next decade and reduce GDP by **€6.9 billion by 2035.** [10]

Discriminatory cybersecurity trade measures can deter innovation

Markets for digital devices and services rely on businesses investing a significant amount of funds in research and development. Screening processes could deter or slow down innovation to the detriment of consumers and wider society. This is because the process could reduce investment from foreign vendors who are prohibited from doing business in Germany or they may no longer wish to do business in Germany due to the uncertainties that this policy will generate. Screening processes could further reduce investment from other local businesses due to higher input costs and lower competition.

This impact could be particularly harmful for certain sectors such as:

- sectors that rely on highly specialised equipment or services as there may already be limited supply of alternative suppliers that have invested in the necessary research and development to provide alternative inputs; or,
- sectors that tend to also have a complex multi-layered supply chain of vendors as the introduction of discriminatory trade measures (based on non-technical factors) could

[10] See https://www.oxfordeconomics.com/resource/the-economic-impact-of-restricting-competition-in-5g-network-equipment/

drastically increase the level of uncertainty as these rules will require the cybersecurity authority to assess the full range of input components.

There is a further risk the requirements to obtain certification could slow down / deter innovation from both domestic and foreign businesses as this may be too time consuming for businesses to test and launch new products. At the extreme, businesses may choose to focus their investments on other locations where they consider their returns will be maximised and risks minimised.

The impact on innovation on the overall economy could be illustrated by exploring the impact of vendor screening on productivity, since productivity gains are the result of investments in innovation. Vendor screening could be considered as an increase in the tariff on imports as it restricts the number of vendors, thereby leading to higher prices. Recent work by the IMF showed that a percentage point decrease in tariffs is associated with a 2% increase in economy wide productivity.[11] Taking into account the mix of inputs used by other sectors, the vendor screening measures would equate a **reduction in German GDP of around €2.2 billion**.[12]

Germany spends around 3.14% of its GDP on R&D (significantly higher than the average across the European Union of 2.3%).[13] An increase in the use of vendor screening measures could reduce German R&D expenditure. Indeed, a recent study found that an increase in German import tariffs by 10% could lead to a dampening of R&D investment by 5-15%.[14]

Impacts on trade and economic output

Discriminatory cybersecurity trade measures that rely on non-technical measures will reduce trade and economic output. The impacts on trade are summarised in Figure 2 below. The bars show the trade impacts in absolute terms, while the marked line expresses these impacts as a percentage of total trade. The shading of the bars shows the impact attributed to screening and compliance costs respectively. Overall, the usage of non-technical factors to screen vendors could lead to a **€793 million** reduction in extra-EU exports and **€855 million** reduction in intra-EU exports. There is also reduction in domestic output as the compliance requirements impose pure costs on producers. As can be seen, the bulk of the impact is driven by incremental economic frictions associated with implementing the new regulations.

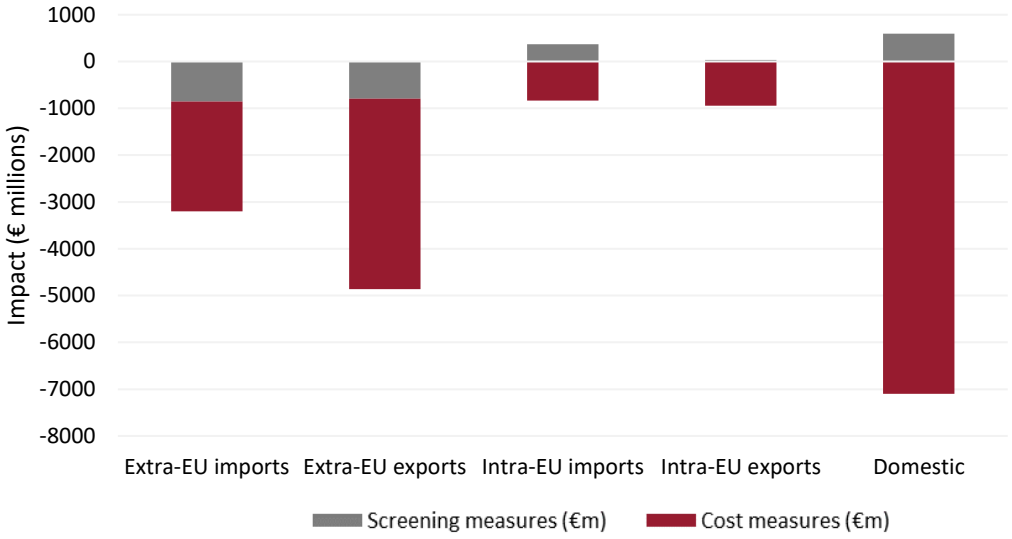
[11] See https://www.imf.org/en/Publications/WP/Issues/2016/12/31/Reassessing-the-Productivity-Gains-from-Trade-Liberalization-43828

[12] Note that there is potential double counting between the effects of vendor screening on GDP estimated here and the trade-openness approach that was used in the next section, as both will include effects on ICT as an input into other sectors

[13] See https://data.worldbank.org/indicator/GB.XPD.RSDV.GD.ZS?locations=DE

[14] See https://cepr.org/voxeu/columns/firm-rd-investment-export-market-exposure-and-trade-policy

Figure 2 Distortionary impact on trade as a result of cybersecurity and discriminatory measures



Source: *Frontier Economics*

The impact on extra-EU export on trade comes via two channels:

- **€4.1 billion** is due to the costs of implementing cybersecurity measures reducing the ability and willingness of firms to trade with the EU.
- A further **€793 million** is due to the discriminatory vendor screening measures which restrict the ability of firms to supply services, create uncertainty among suppliers and reduce transparency in regulatory decision making.[15] The effects of discriminatory measures reported here are likely to be highly conservative, as they are only estimated for direct effects on the telecoms and computer services sectors. However, these inputs are ubiquitous across the range of sectors, with ICT services representing around 1% - 2% of total output across these sectors. At a minimum we would expect the discriminatory measures to have a broad impact across a range of sectors, as the supply of these inputs becomes less competitive and more costly to procure. It may also reduce uptake and use of technology inputs, potentially resulting in adoption of less technology-intensive functional and business models, in extreme cases having more fundamental impacts in areas such as innovation or product offering. In turn, this will have impacts on the wider economy.

[15] For practical reasons, the modelling is only able to analyse discriminatory measures in the "direct" sectoral sense – for example the impact of screening for telecoms and computer services on trade for the same sector. This is in contrast to "cross-sectoral" effects – for example the effect of screening ICT inputs on transport operators – as these effects are much broader than the direct effects analysed, but are much more complex to estimate empirically.

The trade impacts will in turn affect GDP and productivity. Using relationships observed between openness to trade and productivity, GDP impacts can be estimated. Overall, for Germany, the measures would **reduce GDPworth around €8.8 billion, of which €7.6 billion is the impact due to the costs of implementing cybersecurity measures** and **€1.2 billion is due to discriminatory cybersecurity trade measures (such as vendor screening)**, noting the latter estimate is conservative in its sector coverage.

Conclusion

Enhanced cybersecurity measures are welcome but it is important for policy makers to ensure that the benefits of these measures outweigh the costs to consumers, businesses and the wider society. This means that the German Government should carefully manage this balance when implementing the NIS2 Directive into their country specific regulations.

In general, Policy makers in Germany have implemented cybersecurity policies that are proportionate and targeted at the technical nature of the risks (in line with the principles of the NIS2 Directive). However, there is a concern that some of the recently implemented cybersecurity policies could lead to policy makers relying on non-technical factors (e.g. geopolitical factors), which can lead to a negative net impact on consumers. Given this, policy makers in Germany should focus on technical factors when assessing the degree of risk as this will ensure that any regulatory action is targeted and proportionate. This will also ensure that any action will achieve an appropriate balance between the benefits that can be achieved from enhanced cybersecurity measures against the cost of implementing these cybersecurity measures on end-users and businesses