



Exploring a “Green List” for EU-China Economic Relations

Exploring a “Green List” for EU-China Economic Relations

Report prepared by the Rhodium Group
for the Bertelsmann Stiftung

Agatha Kratz, Matthew Mingey, and Daniel H. Rosen

Table of Contents

Executive Summary	6
Introduction	8
A Checklist for Green Listing EU-China Economic Exchanges	12
Presentation of Results	20
Mitigation Principles for Enhancing the Green List	32
Conclusion	41
Appendix 1 - Green-List Categories	43
Appendix 2 - Methodological Addendum	46
Imprint	52

Executive Summary

- Mounting evidence that China is not converging with the liberal market economy principles of European and other OECD countries has triggered a range of policy responses and a broader debate, amplified by the COVID-19 crisis, about how much economic engagement with China is desirable and safe.
- This study by Rhodium Group for the Bertelsmann Stiftung aims to strip the geopolitical emotion out of this debate and provide a fact-based, transparent framework for assessing which areas of the EU's trade, investment and broader economic relationship with China are benign. We call this the "green list."
- The study also shows how the EU can broaden the scope of this green list, preserving substantial portions of the economic relationship with China, through a range of targeted mitigation measures.
- Among our conclusions is that, based on 2019 data, much of the EU-China trade relationship can be preserved without the need for mitigation. Some 56% of EU exports to China are completely benign, while 83% of China's exports to the EU qualify as "green." On this list are sectors that are at the heart of EU trade relations with China, such as motor vehicle parts, food and drinks, luxury goods and a healthy portion of machinery and industrial goods.
- We find that FDI vulnerabilities are more acute. In the absence of mitigation measures, some 46% of China's FDI in the EU and 32% of the EU's FDI in China in 2019 do not make it onto the green list. Investments with potential security implications can be found in the areas of sensitive individual data, critical infrastructure and emerging computing technologies.
- These results are a first and exploratory attempt at green listing EU-China economic interactions. Our findings are not meant to be definitive, nor should they be considered normative.

- We show besides that through credible mitigation measures, the green list can be substantially extended to cover more of the EU's trade and relations with China.
- The study makes three recommendations for EU policymakers. First, the EU needs to state clearly that some aspects of its economic relationship with China pose security risks, while others do not. Only by acknowledging this dichotomy can it credibly keep the door open to benign economic engagement and mitigate the risks in areas that are potentially problematic.
- Second, the EU needs to have a frank and open debate about what areas of its economy are relevant for its national security. At the moment, no European consensus exists on this question. Without clear definitions, Europe will struggle to defend its point of view in talks with other countries and could find itself in a position where foreign definitions of national security are imposed upon it.
- Third and finally, the EU needs to launch a reflection on credible mitigation measures, in order to ensure that the scope of mutually beneficial economic interactions with China remains as broad as possible.
- This study presents a framework for understanding the areas of the EU's economic relationship with China that pose no security risks. More granular analysis is required to reach definitive conclusions about whether certain dual-use, emerging technologies or "essential goods" are risk-free or not. Due to the rapid pace of technological advances in some sectors, and quick evolution of related debates, the cost-benefit calculus is likely to evolve rapidly, requiring a flexible, dynamic approach.
- The EU "green list" also needs to be benchmarked against the approaches of other OECD countries in order to achieve the highest possible degree of alignment on this issue.

Introduction

For more than half a century, industrial democracies have taken as a given that international economic engagement will continue to deepen. The lesson of the twentieth century was that rational interests would steer countries' economies toward openness and global integration. The end of the Cold War appeared to entrench these norms. While economists and policymakers debated how quickly economic systems would converge, the idea that convergence was positive – if not inevitable – was not widely disputed.

With surprising rapidity, the assumptions underpinning this belief have frayed, largely due to uncertainty about China. Two factors ground the current rethink. The first is geopolitical. As recently as five years ago, most observers believed that Beijing still intended to make its economic model compatible with liberal market economy principles. Today there is mounting evidence that China's leadership has a different model in mind, one that is at odds with the concept of deeper engagement based on these principles. This has triggered reactions in Europe and other advanced economies, from a wave of tighter FDI screening regulations, to a debate about the use of Chinese suppliers for next generation 5G networks. There is now a consensus in OECD economies that the relationship with the world's second largest economy needs to be reassessed.

The second shock to assumptions about engagement and integration came more suddenly, with the outbreak and spread of COVID-19. The virus triggered a sudden breakdown of supply chains, adding urgency to a debate in European and other OECD countries about China's economic model and the risks associated with unlimited economic engagement. In short order, the negative side effects of economic interdependence – mainly with China, but also with other countries that locked down medical equipment and pharmaceuticals for domestic use – became readily apparent. It was not surprising to see China commandeer materials and equipment to address a national emergency. But it was a shock for European and other OECD countries to discover how much they depended on China for medical supplies that are vital to *their* national security, and to watch China leverage this power by distributing equipment as political favors.

Our understanding of the risks associated with relying on supply chains based in China has evolved rapidly. These risks are not limited to rare crises or supply

shocks like COVID-19. They are also geopolitical and include the possibility that China could disrupt trade and economic interactions for political and strategic reasons. The virus has shown that there are formidable costs to relying on foreign suppliers for critical inputs. Yet reducing these risks is not so simple. Globalization, including interaction with China, has delivered massive international welfare gains and it is not possible or desirable to drastically reduce or eliminate economic ties. How to resolve this dilemma will turn on political and philosophical principles as well as economic ones. At its core are two urgent questions: How should economic engagement with China be adjusted? And what is the price of doing so?

Deciding where to reduce Europe's exposure to China is a complex question. Evaluating this during the COVID-19 crisis is even harder. This report, prepared for the Bertelsmann Stiftung, helps make this challenge more manageable by making it smaller. We do this by identifying areas of economic interaction between the EU and China that require no special handling because they pose no security risk. In a next step we look beyond what we refer to as the "green list" and examine how we can address potential concerns in other areas of economic engagement through a variety of mitigation measures, thus extending the range of "safe" sectors and preserving a broad base of economic interaction between the EU and China. A detailed assessment of how to mitigate risk is a challenge for another study, but this report will make it vastly easier by separating out the large body of commerce that does not require further policy attention. This will conserve time and resources for the important work of mitigating and resolving vulnerabilities in other areas.

Some might react negatively to this study's objectives, fearing that a public debate about economic interactions with China will fuel protectionist instincts, giving momentum to "decouplers" who want to shut down economic interactions with China for the wrong reasons. As longtime advocates of economic engagement with China, we share this trepidation. But the reality is that a debate about the benefits and risks of trade and investment dependence is already underway, in advanced and developing economies alike. Failure to objectively assess Europe's economic relationship with China will not preserve the status quo. On the contrary, it may increase the risk that the debate will be hijacked by those that support maximalist policies.

Others will ask whether this study can be "weaponized," providing grounds to argue that any EU-China economic interaction with even tangential security relevance – that is, everything aside from our "green list" – should be immediately and fully shut down. But we demonstrate the opposite: that many areas of concern can be managed. We believe that it is important to distinguish trivial concerns from material security concerns with maximum transparency and frankness. We also believe that it is wrong to pretend that just because certain sectors of the economy were seen as non-sensitive a few years ago, there is no reason for closer scrutiny today. Trends like the weaponization of social media, the deployment of new forms of telecommunications infrastructure, and the intensifying competition for high-tech assets around the world demand that policymakers take a closer, fact-based look at possible risks. The objective must be to acknowledge that some concerns exist and to manage them in fiscally prudent, socially responsible, and strategically sustainable ways. This study seeks to advance that effort, by paring down the areas that require discussion and focusing policy attention where it belongs.

Finally, the screenings we develop in this study identify the set of activities and products that require minimal further attention. They do not say anything about the remainder of trade and investment flows, other than that with some attention, we can continue to enjoy the benefits of economic openness while addressing security misgivings.

Overview of the report

While most studies have approached the question of reassessing EU-China economic ties as if they were compiling a “red list” – pinpointing those sectors which pose a problem – this study looks at the question from the opposite perspective. We propose a framework for identifying the parts of our economic relationship with China that do not pose any strategic risks, and the areas where those risks can be easily mitigated. We call this the “green list.”

We find that most of the EU’s current trade ties with China make it on to the green list, without the need for any mitigation measures. These include key elements of the EU-China trade relationship, such as motor vehicle parts, most luxury goods and fashion items, foods and drink products, and a healthy portion of two-way exchanges in machinery and industrial goods.

While most EU-China trade in 2019 can be seen as benign, a not insignificant share of two-way foreign direct investment last year presented potential security risks. This included half of inbound deals, and a third of outbound transactions. Still, FDI activity that does raise security concerns need not be pared back entirely. Much of it can be brought back to the green list through mitigation steps. We propose an initial illustrative list of measures to address security risks, hence increasing the scope for benign bilateral economic interaction.

This first approximation of green-listable areas (with and without mitigation) is not meant to be definitive. It is a preliminary effort to identify sectors where risk-free engagement with China is possible, based on a broad overview of economic security issues. It is not an exhaustive analysis of technical security concerns in every subsector of the EU economy.

Our categorizations are likely to change over time. As national security concerns evolve with technological advances, policymakers must reassess which mitigation tools are appropriate so as to preserve a broad scope for EU-China economic interactions.

Yet this report shows that extreme, far-reaching disengagement on security grounds is unnecessary and that many aspects of the EU-China economic relationship do not raise strategic concerns. We note that there are issues of economic fairness in EU-China economic relations that may present other grounds for closing doors, but those arguments are not the subject of this study. Our findings are complemented by an analysis of mitigation avenues that limit risk while preserving economic exchanges. Indeed, there are attractive alternatives to disruptive decoupling for national security grounds.

As a methodological experiment in understanding the sensitivity of current EU-China economic exchanges, this study is aimed first and foremost at spurring a sober, clear-eyed debate about the EU's economic relationship with China. Its results are not meant to be normative or taken as a roadmap for policy-making. They are merely a snapshot of current EU economic exchanges with China, mapped against the EU's own definition of national security.

The study does, however, raise three policy considerations.

First, the EU needs to state loudly and clearly that while some aspects of its economic relationship with China pose security risks, others do not. Only by acknowledging this dichotomy can it credibly keep the door open to benign economic engagement and mitigate the risks in areas that are potentially problematic. In the absence of clear definitions, there is a risk that the entire relationship comes under scrutiny, as it has in the United States.

Second, the EU needs to have a frank and open debate about what areas of its economy are national security relevant. The definitions used in this report stem from existing EU documents, regulations and statements. This is a list that includes critical infrastructure, emerging technologies, and the broad use of data. Yet we encountered significant difficulties identifying a clear European consensus on many of these issues. This suggests that significant work is still needed to align member states and build a unified European view on this crucial question. Only with a clear definition in place will Europe be able to engage with partners, or rivals, and defend its own point of view. Failing that, the EU could find itself in a position where foreign definitions of national security are imposed upon it.

Third and finally, the EU needs to launch a reflection on credible mitigation measures, to ensure that mutually beneficial economic interactions with China remain as broad in scope as possible.

This report proceeds as follows. Section 2 introduces our framework – a checklist for green listing economic interactions with China. Section 3 presents the result of our coding of economic sectors. Section 4 proposes a series of mitigation principles for bringing certain risk sectors back onto the green list, and applies these principles to our coding of EU-China trade and investment relations. Section 5 concludes with a series of caveats, final comments and recommendations.

A Checklist for Green Listing EU-China Economic Exchanges

We aim to identify sectors and types of economic interaction that do not present any security concerns for EU member states, and thus should be kept fully open for business. **How does one determine that an activity is not security relevant?** We adopt a three-pronged approach to answering that question:

- **First, we define key national security concerns for the EU and its member states.** National security policies throughout the OECD now acknowledge the need to protect not just military assets and the goods/products or infrastructure that are directly connected to military readiness, but also certain key economic and political activities. These include, for example, the construction and operation of critical transport or telecommunication infrastructure, the production and transportation of essential goods such as energy and food, and equipment tied to the organization of national elections. We include all these aspects in our framework.¹
- **Second, for each of these areas of potential concern, we draw up a list of specific risks (e.g. supply disruption or sabotage) to EU national security.** These are identified from the academic literature, EU policy documents, broader OECD publications and debates, and interviews with relevant stakeholders.
- **Third, for each risk we develop a simple question to evaluate a sector's national security relevance.** For each question, we propose criteria for responding positively or negatively. The output for each question is a decision to exclude or include sectors in our green list. In answering questions, we differentiate between four types of economic interaction (trade, FDI, procurement and R&D), as some may raise more concerns than others.

Our approach has two key characteristics:

- **It is maximalist.** If a sector meets the criteria of security relevance for *any* one question, it is *not* eligible for the green list. However, where possible, the dismissed sectors or types of interaction will be considered alongside specific

¹ Note that we leave out environmental and human security, however, which is tied to general human welfare and is not generally associated with specific foreign state actors.

mitigation measures. We discuss these measures in the latter half of this report (see section 4).

- **It is EU-specific.** Wherever a relevant EU definition was available (e.g. for critical infrastructure), we based our checklist criteria on it. In the few cases where the EU has no clear definition, we used a composite definition, drawing on relevant principles of EU law, EU-commissioned expert studies or high-level working group papers, principles contained in EU member state legislation and regulation, and/or interviews with EU stakeholders (all definitions are gathered in the methodological appendix). This allows us to place EU-specific concerns at the center of our framework.

Six caveats should be mentioned up front:

- **First, while green list sectors are considered benign in terms of national security, some (many in fact) might be a cause for economic concern and/or a source of commercial risk to EU businesses.** Yet tools to deal with those economic risks should be sought beyond countries' national security policy toolkit (for suggestions, see our previous report, *Beyond Investment Screening*). Note that some of these sectors might also have ethics or human rights implications, including, for example, surveillance technologies. Where these overlap with EU definitions for national security, they are included in our analysis.
- **Second, we chose not to include economic competitiveness as a dimension of national security.** In its most extreme form, nations like the United States have come to define economic security as encompassing the competitiveness of domestic firms, making commercial success a national imperative. Under this maximal definition, almost any economic link could be justifiably severed or conditioned. We leave out this definition because it is not shared widely by EU member states.
- **Third, we do not take into account decoupling costs as a criterion for green listing industries.** Such costs are relevant for policymakers assessing avenues for further EU-China economic engagement or disengagement, but they are irrelevant to the discussion of whether a sector is benign in terms of national security and public order. Hence, we rely only on national security principles and criteria for formulating our green listing framework.
- **Fourth, we take a sectoral approach to defining the green list, which comes with drawbacks.** In particular, dual-use goods are context and case-specific, and controlled dual-use goods are defined by their technical specifications, capabilities, and intended use or application. This makes it difficult to assign them to a single sector for purposes of analysis. Similarly, data and digital technologies, as well as emerging technologies, are hard to assign and code to a single sector as they are most often cross-sectoral. Though imperfect, the sectoral approach was the most straightforward way to develop this first estimate of an EU-China green list, and the most practical lens for comprehensively addressing all national security concerns and risks outlined later in this report.

- **Fifth, we do not code for intermediate value chains and inputs, and instead focus exclusively on finished products and related sectoral categories.** Some lower-tech and less sensitive components might of course be crucial for higher-tech, more sensitive or essential goods, and value chain resilience is a key aspect of a nation's national security. We touch upon these issues, but they are unfortunately too broad and complex to untangle within the scope of this report. The same is true of valued-added trade dynamics, including intra-industry goods trade, which we are unable to isolate despite their high business relevance.
- **Finally, we do not distinguish between state-owned and private Chinese firms as trade, investment or R&D partners of European companies, or as participants in EU procurement markets.** Several recent Chinese laws – and especially China's National Intelligence, National Security and Cyber Security laws – are blurring the line between state-owned and private firms *in terms of national security*, by exposing the later to potential state influence and scrutiny.

Based on these principles, we propose the following checklist for green listing EU-China economic exchanges:

Checklist

A) Weapons, dual-use technologies, and defense supply chain risks

Risks include:

- An economic exchange increasing strategic competitors' military capacity and power, through the transfer of sensitive military or dual-use goods or services (including weapons and advanced technology);
- An economic exchange with the potential to disrupt EU member states' military readiness and capacity through the destruction or compromise of military systems and/or infrastructure.

Q1: Does the sector/subsector provide goods or services that qualify as weapons or arms, or related to the country's nuclear material production capacity?

If yes: dismiss for trade/FDI/R&D/procurement; if no:

Q2: Does the sector/subsector provide goods or services that qualify as dual-use?

If yes: dismiss for trade/FDI/R&D/procurement; if no:

Q3: Does the sector/subsector involve other “critical technologies” relevant to military-based national security?

If yes: dismiss for trade/FDI/R&D/procurement; if no:

Q4: Does the sector involve goods and services directly related to military infrastructure and systems?

If yes: dismiss for military procurement and monitor for investment; if no: continue to the next section.²

B) Intelligence gathering and compromise of key personnel

Risks include:

- An economic exchange with the potential to cause intelligence breaches, either through the use of personal or sensitive data to recruit or compromise personnel, or through direct access to sensitive information.

Q5: Does the sector involve collection, storage or transmission of intelligence or intelligence-related data that would directly compromise EU security?

If yes: dismiss all channels for NACE 84.2 sectors (foreign affairs; defense activities; justice and judicial activities; public order and safety activities); for other sectors, dismiss for intelligence-related procurement and monitor for investment;³ if no:

Q6: Does the sector involve the collection, storage or transmission of personal data that might be accessed by foreign state actors to identify and compromise military or intelligence personnel?⁴

If yes: dismiss for trade (including cross-border data flows)/investment/R&D/procurement (see Box 1); if no: continue to the next section.

² Our examination of direct threats to military readiness focuses on defense, defense-adjacent or dual-use sectors, goods, services, infrastructure or systems. But other sectors often provide low-tech or anodyne products and services to military actors where those goods and services themselves are not weapons and do not have dual-use capacity, and/or military procurement is a small portion of the overall sector activity (i.e. furniture, building construction, food, clothing or non-military software). These sectors are not dismissed in full as potential security threats here (though they may qualify as security relevant later on in the checklist) as discrete mitigation measures are easily implemented, for example forbidding procurement of equipment or services to military sites or infrastructure by Chinese or Chinese-owned providers or contractors. Such mitigation measures do, however, require retaining a diversity of (non-Chinese) providers for such goods and services – and hence scrutiny on inbound investment that might lead to excessive concentration.

³ Same note as Q4.

⁴ For digital technologies and businesses, both Chinese acquisition of data-heavy businesses and European acquisitions of such businesses in China are an issue if they lead to the transfer or storage of European personal data to/in China. Note on IoT devices and wearable consumer tech: These technologies would naturally make their way onto the above list. If these are utilized by military and intelligence personnel, they are security relevant. However, these security concerns – because they are focused on a small number of key stakeholders – can be mitigated via non-systemic responses (encryption standards, restrictions on use by personnel, etc.) rather than broad decoupling measures (trade restrictions, investment screening).

C) Critical economic goods, inputs and infrastructure

Risks include:

- An economic interaction that could lead to the disruption in provision, or outright denial, of goods needed for survival or basic economic life of all citizens;
- An economic interaction that could lead to the disruption of a country's critical infrastructure or key IT and information systems.

Q7: Does the sector/subsector involve the provision of "basic economic goods" or "critical inputs"?

If yes: monitor for investment and R&D⁵; if no: continue to the next section.

Q8: Does the sector qualify as a sector of critical infrastructure (CI) or essential network and information system (NIS)?

If yes: dismiss for inbound FDI/import/procurement/R&D⁶; if no: continue to the next section.

D) Political influence and public opinion manipulation

Risks include:

- An economic interaction that can disrupt electoral systems and/or political infrastructure (direct election interference);
- An economic interaction that can result in the manipulation of public opinion or outright propaganda;
- An economic interaction that can lead to undue influencing of key decision makers/stakeholders, via the use of sensitive personal data.

5 Overreliance on imports and foreign value chains for the provision of basic economic goods or critical inputs is a security concern as it puts countries at risk of supply disruption or cutoff at critical junctures. The COVID emergency made obvious that scenarios exist in which reliance on foreign supplies can lead to sudden interruption of basic goods and critical inputs access.

Yet abruptly severing trade and supply chain ties would cause costly disruption for Europe. Hence, this particular risk calls for the EU to maintain openness (in trade, R&D and, to some degree, investment) while actively seeking a diversification of international suppliers, increasing domestic production or stockpiling where necessary, and close monitoring of investment concentration to avoid any one actor controlling an excessive share of supply. We therefore keep related sectors on our green list but highlight them in our coding as sensitive in the long-term and necessitating further consideration and strategic planning (see section 3). Key questions for identifying excessive concentration in key sectors should include the following: Is the sector highly fragmented, with multiple sources of supply? Does the majority of supply originate within the EU or friendly countries? Are there substitutes to this good, fulfilling conditions set by the two previous questions? Excessive reliance on Chinese intellectual property for any of these sectors should also be monitored. And of course, economic interactions affecting Europe's ability to channel such essential goods and critical inputs to Europe should also be scrutinized (see Q8 on critical infrastructure).

6 CI and NIS are typically situated in Europe. Hence, issues related to these infrastructures are mostly around inbound flows: investment in EU CI/NIS, and procurement or import of CI/NIS goods and services from Chinese counterparts.

Q9: Does the sector provide technology for services for EU electoral infrastructure, including election technology?

If yes: dismiss for inward investment/import/procurement/R&D⁷; if no:

Q10: Can the sector be used to spread disinformation (“deliberately false, distorted or misleading information”) or propaganda (“content that is not subject to verification, such as biased or exaggerated opinions or manipulated content aimed at misleading the audience, especially content inciting negative emotions”)?⁸

If yes: dismiss for import and inbound investment; if no:

Q11: Does the sector involve collection, storage or transmission of personal data that might be accessed by Chinese state actors to identify and compromise key decision makers/stakeholders?

Definition: Same as question 6.

If yes: dismiss for trade (including cross-border data flows)/investment/R&D/procurement.

⁷ Electoral infrastructure is typically situated in Europe. Hence, issues related to these are mostly around inbound flows.

⁸ Freedom of expression is a core principle of the European Union and its member states and is enshrined in the European Convention on Human Rights. The line between advocacy, reporting and disinformation is not always clear in the above sectors, and the aim should be to preserve a plurality of views in Europe. Therefore, though we dismiss most of these activities at this point for national security reasons, we propose a series of mitigation avenues (including considerations on the scale of viewership/readership/usership of media owned by Chinese players) in Section 3. Note that here again concerns are mostly about inbound activities.

BOX 1**Data and national security: The risk of overreach**

The use of advanced computing and data technology by European firms – whether in manufacturing, retail or services – presents a challenge to EU actors concerned about possible Chinese threats to European security. EU firms across almost all sectors now generate and transmit large amounts of industrial, commercial and personal data that could be leveraged by hostile PRC security actors.

As such, data-related risk is a horizontal rather than sectoral consideration, and hard to integrate into our framework. Blanket restrictions on activities involving data, both personal and industrial, might be tempting, but they would affect a wide majority of (largely non-sensitive) European businesses and activities. There is therefore a clear risk of overreach.

Our framework focuses on two types of data that we consider to be security relevant. The first is “personal” data, which may contain personally identifiable information (PII) and/or information about sensitive individual activity, including financial condition, personal health or sexual preference. The second is consumer data (especially aggregate consumer data), which may be used to infer relevant personal information from economic interactions, e.g. from retail behaviors, and hence similarly be used for hostile purposes.

Our framework purposely leaves out data obtained through hacking activities or external network compromise. While the security threat associated with such activities is real, it is not one that relies on common economic interactions: Malicious actors may hack EU data sources without any underlying trade, investment, R&D or other economic relationship. This report, instead, explores the sensitivity of lawful economic exchanges.

Our examination of security threats from legally acquired data focuses on one key benchmark: Is the data in question directly exploitable by PRC actors?

In the case of personal data, the answer is a clear yes. PII could be used (and has empirically been used by intelligence actors) to coerce or otherwise compromise key personnel. Concern is even greater for highly sensitive personal data that indicates religious, political or sexual orientations, and which can be used to compromise key political, military or intelligence stakeholders.

Yet a wide array of non-sensitive or personal consumer data (i.e. individual-related) can also be used to infer personal information or generate a broad personal profile of specific individuals. Past studies have shown that ostensibly harmless information such as energy consumption or daily internet usage pattern can be used to build highly accurate personal profiles. Such profiles could in turn be utilized either to influence individuals or to engage in political influence operations of the type used by Russia in US elections and the Brexit campaign.

The actionability of most consumer data introduces a high risk of overreach. Can all consumer-data-generating interactions be considered security sensitive? And/or are they risky enough to justify heightened scrutiny? Probably not.

To avoid overreaching, we propose an approach that takes into account the distance of each consumer-data-generating sector to potential weaponization. In fact, as consumer data gets harder and costlier to weaponize, hostile actors might favor alternative leverage. Using this logic, we argue that the easiest type of data to act upon is of course sensitive PII, as well as commercial data involving direct information on an individual's financial or relational situation.

Other types of data are important but not as directly exploitable. Internal production data from a company producing cereal, for example, are not directly relevant to either personal or widespread influence operations. There are two potential risks attached to such data.

First, some analysts have argued that access to wide amounts of any type of data might contribute to the strengthening of China's AI military capabilities. We would argue that although such concerns are legitimate, quantity is already a key characteristic of China's digital ecosystem, and hence that Chinese access to large amounts of European data is not likely to contribute to a material increase in its military readiness.

Second, as more and more industrial (and consumer) data are used for policy-making purposes (monitoring energy consumption, for example), the integrity and reliability of such data is crucial for good and safe policy-making – and data that has been tampered with could lead to damaging decisions. Yet relevant data in this case is typically produced by critical infrastructure sectors (energy, transport, health, etc.) which are covered in our assessment of strategically important sectors.

As a result, our focus is on tackling the first two types of data (personal and commercial), leaving aside the third, on our checklist.

Presentation of Results

This section presents the results of our coding of economic sectors and interactions for national security concerns. We apply the above checklist to the EU-NACE list of economic sectors at the 4-digit level, representing approximately 600 sectors, to produce an illustrative list of China-EU exchanges that can safely (and hence should) be kept fully open *without any sort of mitigation*.

The resulting list is not exhaustive, but an illustration of how much of the economic relationship can be kept open without any concern of compromising national security. We present coding results question by question, provide an indication of the weight of each question's coded sectors in EU-China 2019 trade and investment ties (we do not have data for R&D and procurement, unfortunately), and then present a final green list of sectors and interactions.

Question-by-question results

Q1: Does the sector/subsector provide goods or services that qualify as weapons or arms, or related to the country's nuclear material production capacity?

Coding for this question reveals 12 NACE categories out of 615 as sensitive. The EU continues to maintain the arms embargo against China first imposed in 1989,⁹ and China is subject to the "eight criteria" contained in the EU's 2008 common rules governing control of exports of military technology and equipment, which include "respect for human rights" in weapons-purchasing states and national security of member states and EU allies.¹⁰ Hence, with only a few exceptions, the EU does not export goods, services or technologies related to these sectors to China.¹¹

⁹ "Frequently Asked Questions on EU-China Relations," European Commission, 1 June 2017, accessed April 6, 2020, https://ec.europa.eu/commission/presscorner/detail/en/MEMO_16_2258.

¹¹ Council of the European Union, "Council Common Position 2008/944/CFSP of 8 December 2008 Defining Common Rules Governing Control of Exports of Military Technology and Equipment," accessed April 6, 2020, <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:335:0099:0103:EN:PDF>.

¹¹ Historically, EU member states have offered differing interpretations of the embargo. Though there is agreement it covers weapons and lethal equipment, France and the UK have exported dual-use equipment, including radar systems and unarmed helicopters. "EU Arms Embargo on China | SIPRI," accessed November 7, 2019, https://www.sipri.org/databases/embargoes/eu_arms_embargoes/china.

Q2: Does the sector/subsector provide goods or services that qualify as dual-use?

Coding for this question reveals 96 NACE categories out of 615 as sensitive. Under the terms of EU export control and dual-use rules, notably Council Regulation (EC) No 428/2009, licenses are required for EU member states to export 1) any dual-use item listed in Annex I of the regulation and 2) any other dual-use item if the importing country is under an arms embargo.¹² However, as the EU's arms embargo predates the Maastricht Treaty, this catch-all does not directly apply to China.¹³ Dual-use exports to China are thus left mostly in the hands of member states, with substantial differences in interpretation and export license by country. Accordingly, we cannot easily estimate how much of total EU bilateral trade and investment dual-use goods represent, though we would expect exchanges to be limited.

Q3: Does the sector/subsector involve other “critical technologies” relevant to military-based national security?

Coding for this question reveals 35 NACE categories out of 615 as sensitive. The NACE categories that *contain* “critical technologies” relevant for Q3 comprise approximately 35% of EU exports to China and 37% of EU imports from China. However, these “critical technologies” do not represent the entirety of these 35 NACE categories: For example, the category that includes sensitive acids and rare earth compounds also contains 22 non-sensitive items. Critical technologies also made up 8% of two-way FDI. The main sectors concerned are advanced manufacturing and robotics, electronic circuits and semiconductors, and advanced materials for medical application and pharmaceutical applications.

Q4: Does the sector involve goods and services directly related to military infrastructure and systems?

No sector coded (see Methodological Appendix).

Q5: Does the sector involve collection, storage or transmission of intelligence or intelligence-related data that would directly compromise EU security?

Coding for this question reveals 6 NACE categories out of 615 as sensitive. These represent an extremely limited portion of EU-China trade and investment ties.

Q6: Does the sector involve the collection, storage or transmission of personal data that might be accessed by foreign state actors to identify and compromise military or intelligence personnel?

Coding for this sector reveals 19 NACE categories out of 615 as sensitive. These represented about 17.6% of bilateral FDI deals in 2019. The biggest inbound FDI transaction was the acquisition of UK cloud data center company Global Switch by Jinagsu Shagang Group. There is unfortunately no good data available to assess the extent of EU-China cross-border data flows in these sensitive sectors.

12 Specifically, Regulation (EC) No 428/2009 requires licenses for dual-use items “if the purchasing country or country of destination is subject to an arms embargo” decided by a common position or a joint action. (Reg. EC No 428/2009, Article 4(2)). This was amended in 2011 to include countries subject to arms embargoes arising from “a decision or a common position.”

13 May-Britt U. Stumbaum, *Risky Business? The EU, China and Dual-Use Technology*, Occasional Paper / European Union Institute for Security Studies 80 (Paris: European Union Inst. for Security Studies, 2009).

Q7: Does the sector/subsector involve the provision of basic economic goods or critical inputs?

Tentative coding of NACE sectors for categories that include such critical goods highlights roughly 70 categories, primarily codes in agricultural production and food manufacturing, but also categories related to pharmaceuticals, surgical and medical devices, personal protective equipment, and a handful of sectors containing relevant raw materials from the EU's "Critical Raw Materials" list. These represented about 5.6% of EU imports from China in 2019, and approximately 1.0% of inbound investment.

It is worth pointing out, however, that the fact that a NACE sector is identified as critical does not necessarily mean it is at risk of supply disruption from China. Bilateral supply risk depends on the share of Europe's total consumption of a given good supplied by Chinese imports (as compared to domestic supplies and supplies from third countries).

Our level of analysis is too broad to identify supply vulnerabilities. At the 4-digit level, none of the coded Q7 categories turn out to be sectors for which Europe relies on imports for more than half of its consumption, or for which China is a key (>30%) source of supply. To identify susceptibilities, one would need to adopt a more granular level of analysis.¹⁴ Other reports, drawing upon more detailed datasets, offer some indication of risks. Of 27 raw materials in the most recently released inventory of EU critical raw materials (2017), 13 meet both of our criteria. Similarly, CN/HS trade data illustrates the EU's reliance on China for specific traded products.¹⁵ In 2018 for example, the EU relied on China for 50% of imports of medical personal protective equipment (PPE), including gloves (38% of all imports of those products), face shields (49%) and goggles and visors (58%).¹⁶ However, we are unable to reliably identify the share of these imports in EU domestic consumption of such goods.

Q8: Does the sector qualify as a sector of critical infrastructure (CI) or essential network and information system (NIS)?

Coding for this sector reveals 73 NACE categories out of 615 as sensitive. These sectors represented about 12% of inward FDI deals in 2019. Our critical infrastructure definition includes energy and gas generation and transmission sectors, including the 2019 acquisition of the UK's National Grid gas distribution unit by CIC, as well as several solar project acquisitions in Greece. Transport and logistics networks are also included, thus covering several acquisitions by Sinotrans involving assets of logistics provider KLG Europe. Because critical infrastructure is not covered in CPA/NACE trade statistics at the 4-digit level, we are unable to describe related trade dynamics. The one exception is telecommunications equipment,

¹⁴ This report is a preliminary attempt to highlight risks around essential goods and critical input. The authors intend to elaborate this in future work.

¹⁵ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the 2017 list of Critical Raw Materials for the EU, COM(2017) 490, September 13, 2017, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017DC0490>.

¹⁶ Chad P. Bown, "COVID-19: China's exports of medical supplies provide a ray of hope," Petersen Institute of International Economics (PIIE), March 26, 2020, <https://www.piie.com/blogs/trade-and-investment-policy-watch/covid-19-chinas-exports-medical-supplies-provide-ray-hope>.

which we are able to flag given its direct relation to telecom networks (including 5G networks) and NIS. This sector made up approximately 13 percent of EU imports from China in 2019.

Q9: Does the sector provide technology for services for EU electoral infrastructure, including election technology?

Coding for this sector reveals 4 NACE categories out of 615 as sensitive. The NACE category that *contains* voting machines represents only about 0.66% of EU imports in 2019 (the category is much broader than voting machines, encompassing all kinds of office machinery). We found no Chinese investment in these sectors for 2019.

Q10: Can the sector be used as a means of disinformation (“deliberately false, distorted or misleading information”) or propaganda (“content that is not subject to verification, such as biased or exaggerated opinions or manipulated content aimed at misleading the audience, especially content inciting negative emotions”)?

Coding for this sector reveals 21 NACE categories out of 615 as sensitive. It can be hard to measure the weight of media in cross-broader trade, especially online media sources and digital trade. In fact, especially where no subscription fees are involved, European consumers browsing or using a foreign media website does not get registered in trade data. NACE/CPA trade statistics only provide information for traditional media trade (films, book publishing, etc.). In 2019, these made up 0.05% of imports from China. We estimate however that altogether, sectors covered in Q10 represented about 17.3% (USD 2.21 billion) of inward FDI deals in 2019.

Q11: Does the sector involve collection, storage or transmission of personal data that might be accessed by Chinese state actors to identify and compromise key decision makers/stakeholders?

Same results as Q6.

Building the green list

After applying the many filters in the questions above, we are left with our initial green list of sectors that are not concerning from a security point of view, even without any kind of mitigation. A full version at the 4-digit level is available in the Appendix, but Table 1 summarizes 40 sectors *for which 100% of sub-categories qualify as green*.

Many more sectors are included in the green list at a more granular level. In total, 408 NACE categories out of 615 qualify as green (some of the sectors coded overlap across questions). Key among them for the EU–China relationship are motor vehicle parts, various luxury goods and fashion categories, and machinery and industrial goods like boilers or electrical and electronic equipment.

Analyzing green list sectors by channels offers a more granular picture (Figure 1 to 4).

TABLE 1 Simplified Green List by NACE(/CPA) Division (2-digit)

Sectors highlighted in blue are essential goods or critical input, covered in Q7

Crop and animal production, hunting and related service activities
Forestry and logging
Fishing and aquaculture
Mining of coal and lignite
Mining of metal ores
Other mining and quarrying
Mining support service activities
Manufacture of food products
Manufacture of beverages
Manufacture of tobacco products
Postal and courier activities
Accommodation
Food and beverage service activities
Real estate activities ^A
Legal and accounting activities
Scientific research and development
Other professional, scientific and technical activities
Veterinary activities
Rental and leasing activities ^B
Employment activities
Manufacture of wood and of products of wood and cork, except furniture
Manufacture of paper and paper products
Manufacture of coke and refined petroleum products
Remediation activities and other waste management services
Construction of buildings
Civil engineering ^C
Specialized construction activities
Wholesale and retail trade and repair of motor vehicles and motorcycles
Wholesale trade, except of motor vehicles and motorcycles
Retail trade, except of motor vehicles and motorcycles
Travel agency, tour operator and other reservation service
Education ^D
Creative, arts and entertainment activities
Libraries, archives, museums and other cultural activities
Gambling and betting activities
Sports activities and amusement and recreation activities
Repair of computers and personal and household goods
Activities of households as employers of domestic personnel
Undifferentiated goods- and services-producing activities of private households for own use
Activities of extraterritorial organizations and bodies

A Real estate activities may be considered problematic if they concern property located near critical and/or military infrastructure where they might be used for intelligence, observation or disruption of those facilities/installations. The EU's FDI screening guidelines (Regulation (EU) 2019/452) address this eventuality, specifying that "land and real estate crucial for the use of such infrastructure" (Art. 4(1)(a)) can be considered by member states.

B As described throughout the checklist, joint R&D activities might, however, be sensitive in certain sectors.

C Except in critical infrastructure sectors.

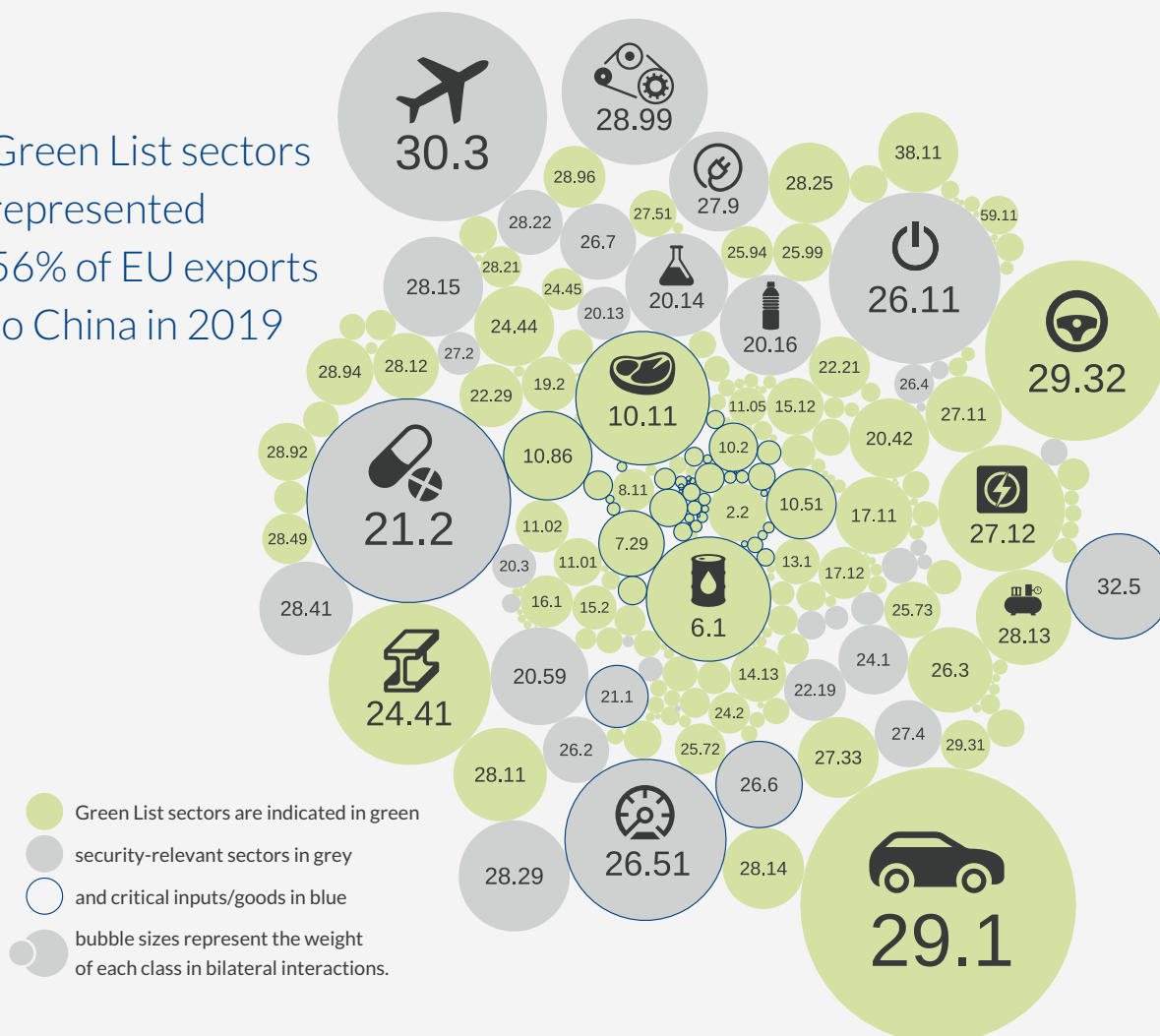
D Chinese actors' involvement in EU educational institutions has been controversial. Official and media reports have especially scrutinized research funding to EU academics and the establishment of "Confucius Institutes" for Chinese language training targeted at European students. The inclusion of education in our green list reflects our methodology and the fact that, despite such controversy, education is still not identified clearly as a key national security risk in existing EU policies, documents and official statements.

Source: Rhodium Group research.


| BertelsmannStiftung

FIGURE 1 Green List by Channel and NACE/CPA Class (4-digit) – EU exports to China in 2019

Green List sectors represented 56% of EU exports to China in 2019



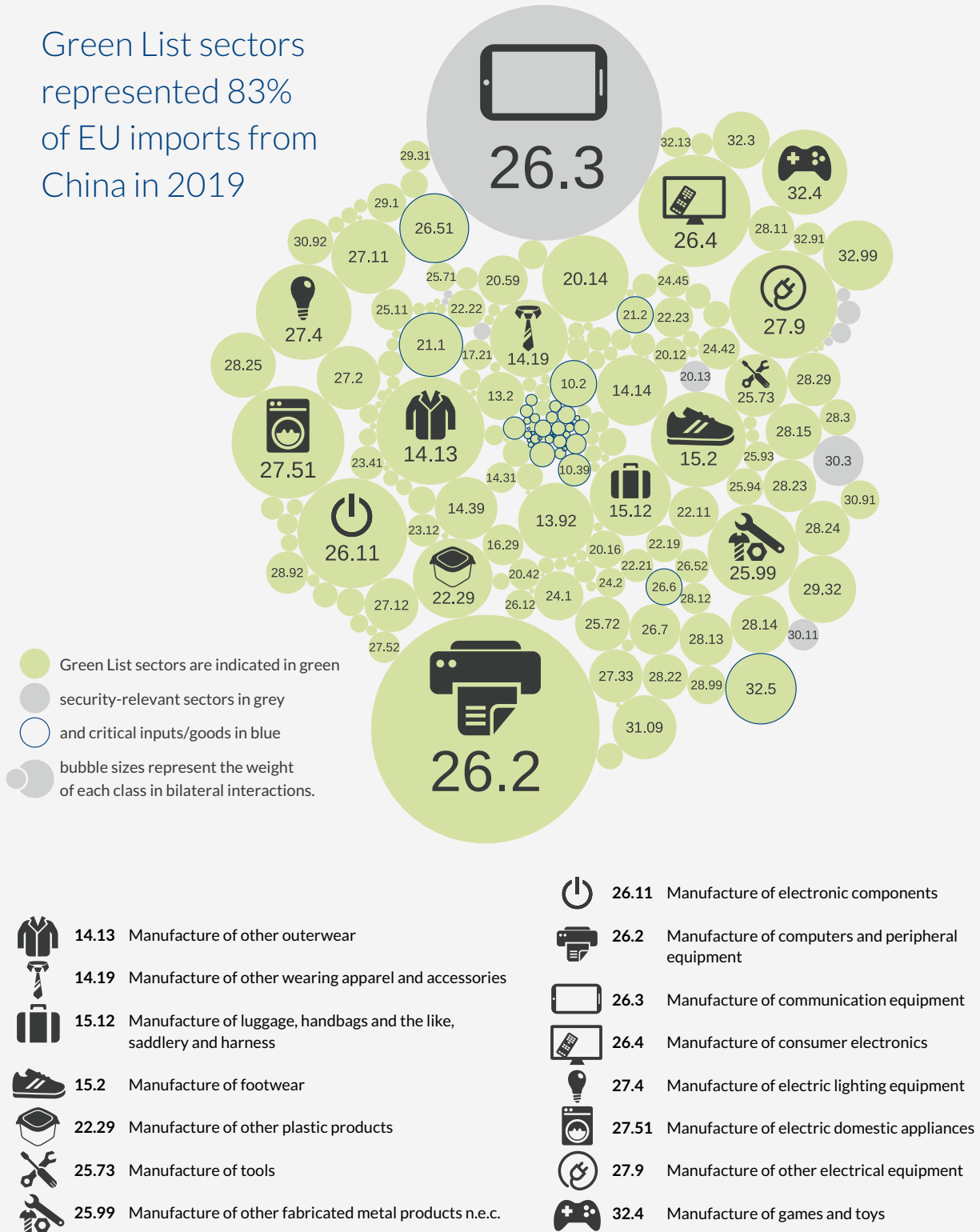
- Green List sectors are indicated in green
- security-relevant sectors in grey
- and critical inputs/goods in blue
- bubble sizes represent the weight of each class in bilateral interactions.

 6.1	Extraction of crude petroleum	 27.12	Manufacture of electricity distribution and control apparatus
 10.11	Processing and preserving of meat	 27.9	Manufacture of other electrical equipment
 20.14	Manufacture of other organic basic chemicals	 28.13	Manufacture of other pumps and compressors
 20.16	Manufacture of plastics in primary forms	 28.99	Manufacture of other special-purpose machinery n.e.c.
 21.2	Manufacture of pharmaceutical preparations	 29.1	Manufacture of motor vehicles
 24.41	Precious metals production	 29.32	Manufacture of other parts and accessories for motor vehicles
 26.11	Manufacture of electronic components	 30.3	Manufacture of air and spacecraft and related machinery
 26.51	Manufacture of instruments and appliances for measuring, testing and navigation		

Source: Rhodium Group research.

FIGURE 2 Green List by Channel and NACE/CPA Class (4-digit) – EU imports from China in 2019

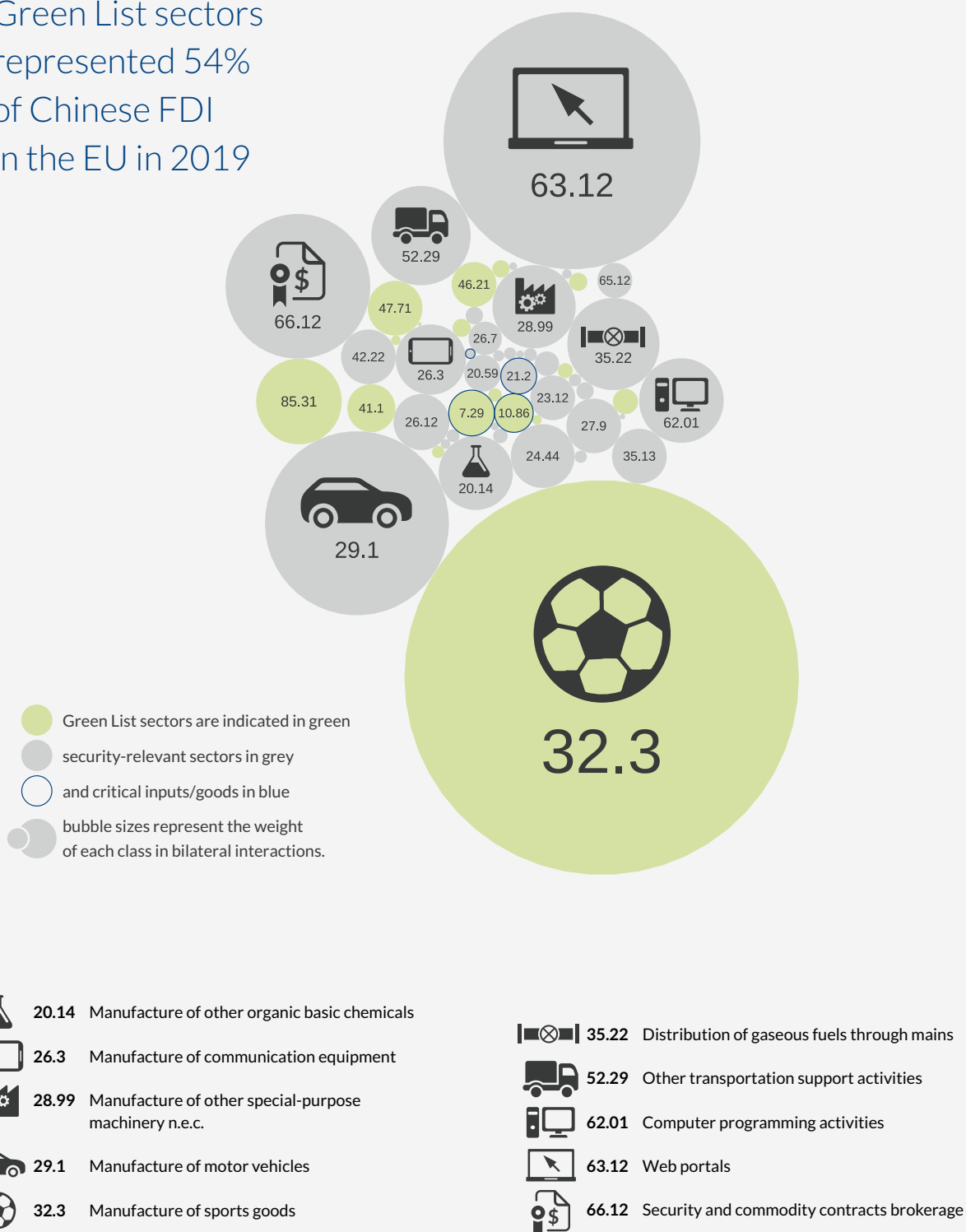
Green List sectors represented 83% of EU imports from China in 2019



Source: Rhodium Group research.

FIGURE 3 Green List by Channel and NACE/CPA Class (4-digit) – Chinese FDI in the EU in 2019

Green List sectors represented 54% of Chinese FDI in the EU in 2019

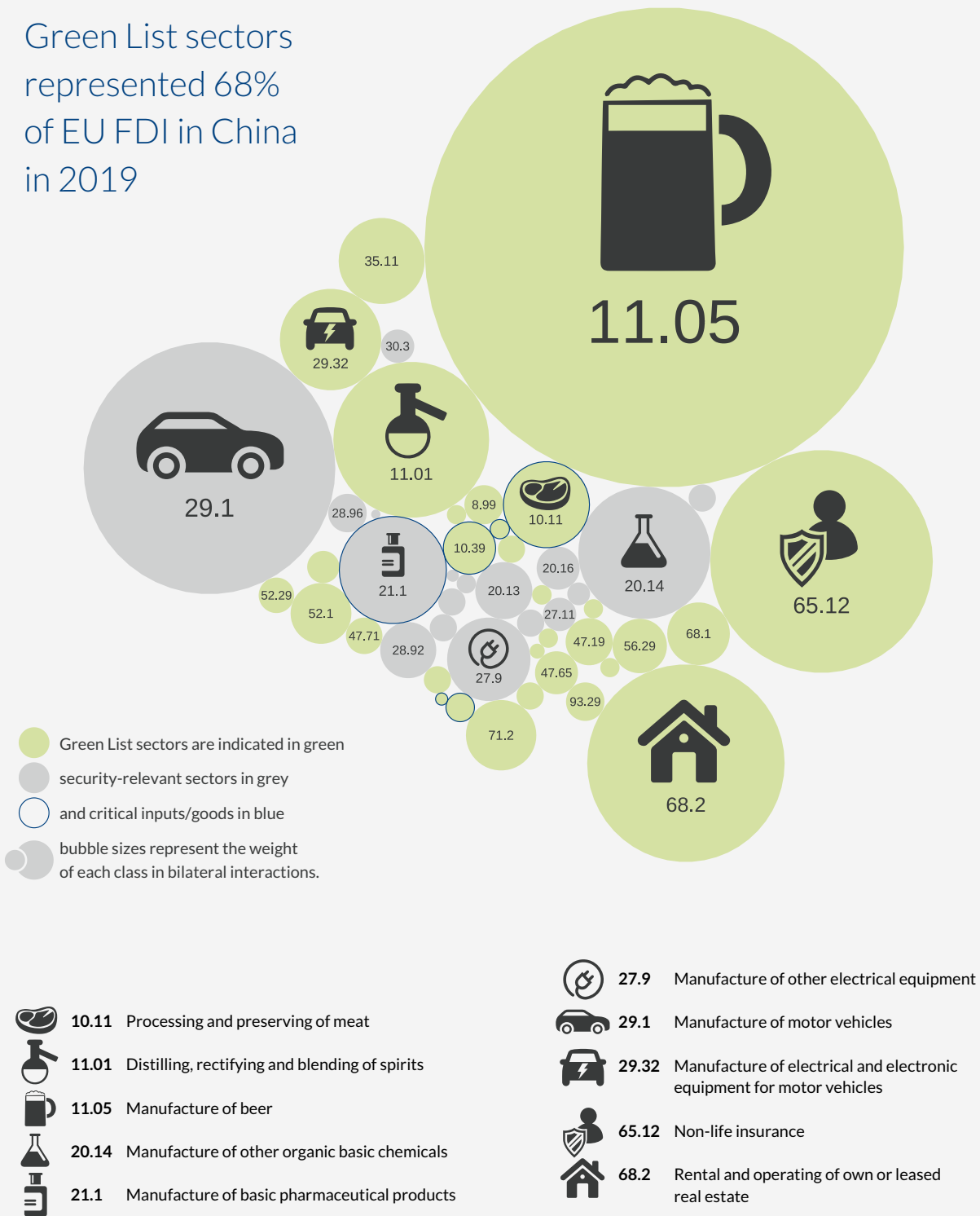


Source: Rhodium Group research.

| BertelsmannStiftung

FIGURE 4 Green List by Channel and NACE/CPA Class (4-digit) – EU FDI in China in 2019

Green List sectors represented 68% of EU FDI in China in 2019



Source: Rhodium Group research.

| BertelsmannStiftung

TABLE 2 Top Sector In and Excluded from the Green List by Channel and NACE/CPA Class (4-digit)

	TOP SECTORS IN THE GREEN LIST	TOP SECTORS DISMISSED FROM THE GREEN LIST (and relevant screening question)
EU exports to China	Manufacture of motor vehicles	Manufacture of air and spacecraft and related machinery (Q1)
	Manufacture of other parts and accessories for motor vehicles	Manufacture of pharmaceutical preparations (Q3)
	Precious metals production	Manufacture of electronic components (Q3)
	Processing and preserving of meat	Manufacture of instruments and appliances for measuring, testing and navigation (Q3)
	Manufacture of electricity distribution and control apparatus	Manufacture of other special-purpose machinery n.e.c. (Q3)
EU imports from China	Manufacture of computers and peripheral equipment	Manufacture of communication equipment (Q8)
	Manufacture of electric domestic appliances	Manufacture of air and spacecraft and related machinery (Q1)
	Manufacture of consumer electronics	Building of ships and floating structures (Q1)
	Manufacture of electronic components	Manufacture of other inorganic basic chemicals (Q1)
	Manufacture of other outerwear	Book publishing (Q10)
Chinese FDI into EU	Manufacture of sports goods	Web portals (Q10)
	General secondary education	Manufacture of motor vehicles (Q2)
	Retail sale of clothing in specialised stores	Security and commodity contracts brokerage (Q8)
	Development of building projects	Other transportation support activities (Q8)
	Mining of other non-ferrous metal ores	Distribution of gaseous fuels through mains (Q8)
EU FDI into China	Manufacture of beer	Manufacture of motor vehicles (Q2)
	Non-life insurance	Manufacture of other organic basic chemicals (Q2, Q3)
	Rental and operating of own or leased real estate	Manufacture of basic pharmaceutical products (Q2, Q3)
	Distilling, rectifying and blending of spirits	Manufacture of other electrical equipment (Q2, Q3)
	Manufacture of other parts and accessories for motor vehicles	Manufacture of other inorganic basic chemicals (Q1, Q2, Q3)

Source: Rhodium Group research.

| BertelsmannStiftung

In 2019, EU-China trade was overwhelmingly composed of non-sensitive activities. In total, 56% of EU exports to China and as much as 83% of imports from China make it on to the green list, confirming the idea that a substantial portion of bilateral trade can be kept open without raising specific national security concerns.¹⁷ Key "green" exports include parts and accessories for motor vehicles, and food and perfumes; key "green" import categories range from textiles, luggage and toys to, again, parts and accessories for motor vehicles. Potentially sensitive imports include communication equipment, some consumer electronics, and certain organic chemicals, while sensitive export sectors cover certain types of motor vehicles, pharmaceuticals and electronic components – most linked to issues of potential dual-use or advanced/emerging technology applications. That a sector is coded as security relevant does not necessarily mean that it should be removed from bilateral trade. Instead, mitigation measures can be identified for many of these categories (see section 4).

Coding of investment activities offers a less straightforward picture. Here, 54% of China's FDI to the EU and 68% of the EU's FDI to China in 2019 qualifies as "green." Sectors of potential concern for Chinese FDI into Europe include web assets and software, natural gas networks and securities brokerage. These sectors are listed primarily for their relevance to critical infrastructure (including network infrastructure), but also because of the prospect of personal data acquisition and deployment. Several EU investments into China in the insurance and pharmaceuticals sector might also raise concerns, though for each of these transactions, further analysis would be required to understand if the products and assets at stake are in fact sensitive. "Green" transactions include sporting goods and textiles, construction and real estate, and the food and drink industries.

As explained throughout this report, this list is best understood as a rough first assessment of security-relevant sectors. It is possible that we have overestimated the number of these sectors by taking a conservative approach: NACE sectors (at the 4-digit level) with a majority of sub-categories qualifying as sensitive automatically get dismissed from the green list. Hence many sub-categories could have qualified as green if we broke down sectors to a more granular level. Besides, many of the dismissed sectors might be brought back through mitigation. This means a longer green list than generated from this first take.

In other cases, we may undercount security-relevant sectors. The largest undercounts likely relate to dual-use and critical technologies like cloud-computing and artificial intelligence (Q2/Q3), which are difficult to assign to a single sector for coding. In reality, such technologies deploy components from several different sectors, but we are unable to systematically and reliably identify them.¹⁸ Additionally, our coding focuses on security risks *from trade and investment* but it is possible that activities through other channels (like R&D) may be security-relevant as well, even if those do not appear on our current estimates for the green list.¹⁹

17 Note that this only includes a coding of categories for which trade data was available by NACE code.

18 See Meia Nouwens and Helena Legarda, "China's pursuit of advanced dual-use technologies," December 18, 2018, <https://www.iiss.org/blogs/research-paper/2018/12/emerging-technology-dominance>.

19 For examples and further description, see the recent Rhodium Group-MERICS joint report: <https://www.merics.org/en/papers-on-china/chinese-fdi-in-europe-2019>.

Critical and emerging technologies are one of the sectors with the most potential for future expansion. They represented only about 8% of two-way FDI in 2019, but that percentage could grow as definitions and policy sensitivity expand. Applying more expansive definitions such as US' ECRA would lead to a higher proportion of two-way trade to be designated as security relevant. US pressure to align and broaden lists of technologies that are considered security relevant may shorten a European green list.

Information on cross-border data flows is extremely limited, probably leading us to underestimate risks in digital industries. Besides, official EU definitions of concerning digital sectors are in flux, and our own criteria leave out many types of commercial data (Box 1). Nevertheless, the sector sees intense bilateral interaction: As much as 17.6% of bilateral FDI deals in 2019 were in sensitive data-related sectors. Our coding also leaves out R&D partnership, where there are problematic cases as well, linked, for example, to geo-localization or voice and face recognition technologies.²⁰ Here, an additional problem is the high level of competitiveness of many Chinese digital firms, which makes tie-ups extremely attractive to European players looking to close the capacity gap or tap China's digital market.

Our coding does not cover procurement and trade in critical infrastructure-related services either, due to a lack of data on both fronts. A quick look at information released by TED, the EU's open platform for public procurement, shows that among the over 5 million public procurement record entries from 2009-2018, only 304 involved a contract won (jointly or solely) by a China-domiciled bidder. Yet such data is widely incomplete.²¹ Hence, the picture we draw here is a partial one concentrated on buyouts of European critical infrastructure companies by Chinese firms.

Finally, we find that 5.6% of EU imports from China in 2019 involved basic economic goods and critical inputs – but risks attached to these sectors and products cannot be properly assessed based on volume (see Box 2). It is enough that a single item making up a negligible proportion of EU-China trade is disrupted at a time of crisis (PPE during the COVID-19 health emergency) for EU member states' national security to be put at risk. Neither does identifying a NACE sector as potentially critical necessarily mean it is at risk of supply disruption as Europe might be procuring only a portion of its needs from China, while receiving a larger share from other countries or European producers. Flagging these sectors is only a first step. A second necessary step entails asking the following questions: Is the sector highly fragmented, with multiple sources of supply? Does the majority of supply originate within the EU or friendly countries? And are there substitutes for the goods in question that help fulfill the conditions set by the two previous questions?

20 For examples, again see Rhodium Group and MERICS' latest joint report: <https://www.merics.org/en/papers-on-china/chinese-fdi-in-europe-2019>.

21 TED data comes from voluntary filing by public tendering bodies, includes only contracts over a certain threshold and does not include separate information on Chinese firms participating in procurement through their EU subsidiary. Besides, we conducted a quick check using rail contracts and found substantial gaps in coverage.

Mitigation Principles for Enhancing the Green List

In many national security relevant sectors it is possible to sustain engagement through *credible mitigation*. This involves much lower implementation costs and less disruption to EU producer and consumer interests than more radical disengagement measures.

Mitigation has long been a path to address security concerns that arise through economic engagement. FDI screening authorities, for example, have often favored asset reorganization instead of the outright veto of transactions. And various existing agreements or regulations, such as the Wassenaar Arrangement, already permit EU member states to mitigate for risks highlighted in our checklist (questions 1 and 2 around arms and dual-use goods export control).

Mitigation can be undertaken through broad measures at the national level (strategic resource stockpiling), through policies aimed at certain end users (military procurement regulations) or through sector-specific steps (telecommunications). It is an important avenue for preserving economic interactions and limiting the cost of disengagement. For it to be effective in preventing concerns around EU-China interactions, these measures of course need to be widely seen as *credible*.

This section describes 15 avenues for mitigation and offers a framework to compare and rank them. It then applies some of these steps to sectors highlighted in section 4 as sensitive. By doing so, we aim to show that the EU-China green list can be broadened, and that our findings in section 3 should be seen as a “floor,” rather than ceiling, for safe economic interactions.

Key principles and avenues for mitigation

1. Regulations on data usage

General or sector-specific regulation to limit transfers and harmful usage of personal data.

Example risks: Social media profiles and/or derived data could be transferred to PRC authorities for use in political influence and/or direct compromise of intelligence and policy personnel.

Mitigation: Data protection regulations and/or restrictions on cross-border data transfer (e.g. GDPR) limit ability of PRC-acquired company to provide usable data to PRC authorities.

2. Specific regulations on investment

Official review of inward investment activities for national security purposes by national or transnational authorities, and restrictions on foreign ownership levels in certain companies or nationwide sectors.

Example risks: Acquisition by PRC-controlled firm of an advanced AI firm whose technology has potential dual-use value for military systems; or acquisition of a series of media outlets which altogether would confer owner excessive market share.

Mitigation: Investment review via national mechanism to condition or deny transaction based on sensitivity, concentration or ownership-stake criteria.

3. Technical standards

Deployment of “specifications and other technical information,” including standards and requirements for interoperability, that “products, materials, services, and processes” must meet in order to be compliant with EU and national regulations.

Example risks: Use of PRC equipment or technology in train control operations systems, a component of critical infrastructure, which might risk compromise of those systems.

Mitigation: Requirement of certain technical standards to ensure systems are not vulnerable to outside compromise and meet EU system parameters.

4. Procurement regulations for military or intelligence infrastructure or systems

Restriction of military and intelligence procurement to approved suppliers, possibly excluding suppliers of a specific national origin.

Example risks: Surveillance of key security agencies via compromised devices (“bugged equipment”) from PRC-based or PRC-owned suppliers.

Mitigation: Restriction of supply for defense/government/intelligence agencies to approved, EU-based or EU-aligned suppliers.

5. Restrictions for specific users

Limits on use or purchase by military/political/intelligence personnel of products/services to approved suppliers.

Example risks: Compromised mobile handsets of intelligence personnel used to gather intelligence or penetrate secure networks.

Mitigation: Restrictions on use of personal electronic devices by intelligence personnel to specific manufacturers and specifications (e.g. biometric security, end-to-end encryption); use of government-issued devices; encryption of key communications.

6. Stockpiling

Maintaining strategic stockpiles of key inputs or imports to cover a certain period of expected use in the event of a supply disruption or cutoff. Stockpiles may be public/national (e.g. EU stocks of crude oil under the Oil Stocks Directive 2009/119/EC) or private.

Example risks: Cutoff of rare earth imports from PRC-based or -owned suppliers, harming productive capacity in key industries and advanced technologies (e.g. batteries).

Mitigation: Establishment of EU-wide rare earths stockpile and/or policy support for private stockpiling by manufacturing and technology companies.

7. Supplier diversification

Use of multiple, interoperable suppliers to reduce reliance on a single foreign source of inputs or imports.

Example risks: Cutoff of European imports of non-sensitive but necessary inputs into military, intelligence or key economic sectors (e.g. specific paints for missiles).

Mitigation: Maintaining a diverse network of suppliers including several "friendly" ones and limiting Chinese acquisition of such suppliers if it causes excessive market concentration. Mitigation may also involve some degree of industrial or other policy to actively promote new suppliers and a more diversified market.

8. End-use identification

Evaluation of end-use conditions of product: Where product capabilities and/or end-user environment do not pose potential security threat, economic interaction can proceed.

Example risks: Smart-home (IoT) devices could offer backdoor access to personal or sensitive data.

Mitigation: For certain IoT devices like network-functional lighting or heating systems, end use conditions do not offer direct access to sensitive personal data, and thus economic interaction can proceed.

9. Supervisory boards

Establishing independent security evaluation boards to review and monitor possible security risks involving the use or procurement of technology from the PRC or PRC-owned manufacturers.

Example risks: Access to actionable personal or other sensitive military/intelligence/political data via compromised telecommunications systems (e.g. 5G).

Mitigation: Use of joint security review board to manage code/technical disclosure and continually evaluate security risk (e.g. Huawei Cyber Security Evaluation Centre, UK).

10. Fail-safe conditions

Implementing redundancies in critical infrastructure systems (and/or individual technological systems, like self-driving cars) so that systems can continue to operate in the event of compromise or revert to a fail-safe state.

Example risks: Compromising of self-driving car, to endanger driver and passengers.

Mitigation: Put in place fail-safe systems allowing driver to revert to self-driving.

11. Technological frontier

Evaluation of the current technical gap between PRC and EU manufacturing or technological capabilities in sensitive sectors. For advanced technology sectors (non-dual-use or military), interactions may proceed for all goods or services for which Chinese firms already possess the same technology at home, as they would not lead to the transfer of more advanced technology to Chinese players. Interactions might also proceed for all technologies considered one or two generations behind leading (European) edge.

Note: A companion and more offensive mitigation approach would be to secure and/or increase tech and R&D funding in Europe to make sure European industries and firms remain leaders in their fields.

Example risks: Sale of an EU firm to a PRC buyer that manufactures robotics technology risks spread of advanced technology products with possible *future* dual-use or military application.

Mitigation: If PRC firms already possess similar tech, or if the technology at stake is two generations behind most advanced EU tech in the industry, interaction may proceed.

12. Due diligence

Due diligence of Chinese partners' links, proximity or potential to be influenced by the Chinese state can mitigate some of the risk, as can security- and ownership-specific due diligence on PRC companies during investment proposals, procurement evaluation, or other economic interactions.²²

Example risks: Sale of a small European insurer, owing consumer financial data, to a PRC firm.

²² Recent PRC regulation of course is blurring the line between state-owned and public actors, but not all actors are under equal influence, and legal recourses – for example for authorities to get access to a firm's consumer data – are more costly and lengthy even for PRC authorities in the case of private actors.

Mitigation: If PRC firm is private, listed, with international and diverse management and board of directors, transparent financial accounts, and branches and activities in various countries, sale may potentially proceed (under certain conditions).

13. Divestment or sheltering of sensitive activities

Member states' investment screening authorities require investment target to divest certain sensitive subsidiaries, assets or functions upon acquisition by PRC investor; or require that "firewalls" between sensitive and non-sensitive company functions be put in place.

Example risks: A PRC firm wishes to buy a large stake in an EU-domiciled insurance firm, which offers both specialty risk insurance for infrastructure, as well as more common term life insurance. The life insurance practice has regular access to PII and sensitive personal data.

Mitigation: The life insurance subgroup may be spun off or divested as a condition for sale to the PRC firm.

14. State ownership in critical infrastructure

Ensure state participation in certain critical infrastructure sectors via board seats, golden shares or other ownership structures.

Example risks: A PRC firm wishes to buy a minority stake in an EU-domiciled grid operator.

Mitigation: Recipient state benefits from golden shares that allows it to prevent PRC investor to acquire majority share, if deemed too risky.

15. Media oversight

Regulatory oversight of the media industry (including through the Audiovisual and Media Services Directive, AVMSD), notably in the form of content oversight; internal and sector-specific codes of conduct, such as France's *Code de déontologie*, to promote strong and unbiased practice; strong journalist unions limiting shareholders' influence on publication tone and content.

Example risks: A PRC media group applies for a commercial broadcast license to establish over-air news channel in several member states; the media group is partially owned by PRC government interests.

Mitigation: A revised AVMSD code may provide for restrictions of purely propagandist or misleading content.

These 15 measures are a first attempt to list credible mitigation steps, and are in no way a comprehensive list of such measures. Some of these policies are sectoral or product-specific, and others more wide-ranging. Some might also be more effective than others at eliminating underlying risks. And some are easier to implement for policymakers, and cheaper for European stakeholders, notably the companies involved (Table 2). But they are a first illustration of the large toolbox at the dis-

posal of European policymakers to preserve more of the bilateral relationship, under certain conditions.

TABLE 3 Comparing Mitigation Measures

	SCOPE	EFFECTIVENESS	EASE OF IMPLEMENTATION	COST
Regulations on data usage	●	●	●	●
Specific regulations on investment	●	●	●	●
Technical standards	●	●	●	●
Procurement regulations	●	●	●	●
Restrictions for specific users	●	●	●	●
Stockpiling	●	●	●	●
Supplier diversification	●	●	●	●
End-use identification	●	●	●	●
Supervisory boards	●	●	●	●
Fail-safe conditions	●	●	●	●
Technological frontier	●	●	●	●
Due diligence	●	●	●	●
Sheltering of sensitive activities	●	●	●	●
State ownership in critical infrastructure	●	●	●	●
Media oversight	●	●	●	●

Table description

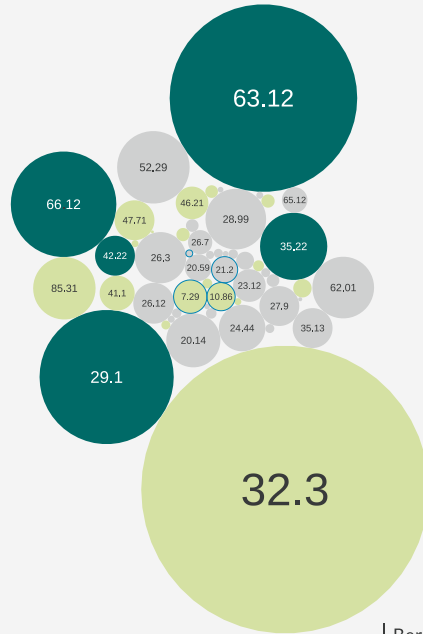
- Wide scope, high effectiveness, ease of implementation, or low cost.
- Moderate scope, effectiveness, cost or ease of implementation.
- Narrow scope, limited effectiveness, difficulty of implementation, or high cost.
- Scope Wide means measure spans across many sectors; narrow means single subsectors or products concerned.
- Effectiveness High effectiveness means almost all related risks are addressed thanks to this measure.
- Implementation Ease of implementation indicates low bureaucratic burden/ease of policy-making.
- Cost Cost relates to financial cost for European firms, consumers and taxpayers.

Source: Rhodium Group research.

| BertelsmannStiftung

FIGURE 7 Mitigating Chinese FDI in the EU

Inbound FDI has received the most EU policy attention in recent years, through member state and EU-level initiatives to tighten or implement investment screening mechanisms. Key sensitive sectors here include web development (web portals), security and commodity contracts brokerage, and gas distribution. All are related to critical infrastructure (or network information systems), which is an area already covered by Europe's investment screening regimes. Potential mitigation measures include the restructuring of proposed transactions, or state or joint-venture participation. Standards to mitigate the risk of catastrophic disruption could be deployed to secure all critical infrastructure, not just targets of Chinese investment. Other sectors include motor vehicles, which produces a small subset of dual-use goods that might be leaked – but may not be applicable to all investment targets or greenfield investment.

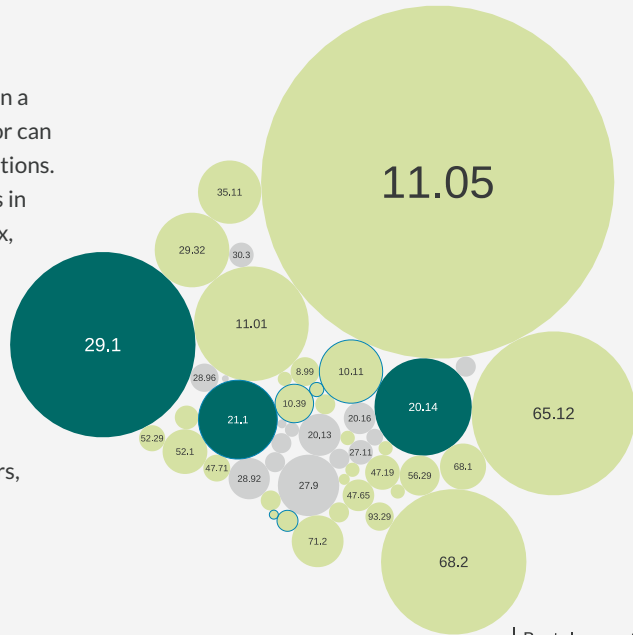


Source: Rhodium Group research.

BertelsmannStiftung

FIGURE 8 Mitigating EU FDI in China

Mitigating the risks associated with outbound investment in a small number of dual-use goods in the motor vehicles sector can be primarily achieved by enforcing existing dual-use regulations. Mitigating the transfer of advanced/emerging technologies in pharmaceutical applications and chemicals is more complex, as China is still a key manufacturing and R&D hub for firms in many technological applications. EU (and other OECD) firms already attempt to mitigate some security risks by controlling IP and technology deployed in China to avoid leakage. This is one case where last-generation technology (the "technological frontier") or activity sheltering may be utilized. However, for cutting-edge R&D in emerging sectors, or for critical goods supplies, due diligence and scrutiny of investment partners and governance structures, as well as internal data transfer rules, will also be needed.



Source: Rhodium Group research.

BertelsmannStiftung

In short, many mitigation measures are available that are available that can broaden the scope of the green list. These range from closer end-user monitoring, in the case of exports, to procurement restrictions for imports. By using these steps, governments can preserve areas of bilateral interactions that pose some risks which are manageable. To avoid costly disengagement in these sectors, these measures will, however, need to be credible and convincing enough to lift concerns and avoid knee-jerk reactions from the public, politicians or allies.

BOX 2**Mitigation for essential goods: The example of pharmaceuticals**

The COVID-19 pandemic has highlighted the critical role of pharmaceutical and medical supply chains in national health and security. Supplies of vital medical equipment in Europe, especially personal protective equipment (PPE), depend heavily on imports. This has led to acute shortages in several EU member states at the height of the coronavirus crisis. Meanwhile, the drive to develop and produce COVID treatment drugs or a vaccine²³ has raised the specter of competitive investment and IP acquisition, highlighted when media reports, citing German government officials, suggested that the United States had made overtures to a German pharmaceutical company in a bid to secure exclusive rights to a disease vaccine. In response, the European Commission has encouraged the collective procurement of drugs and medical supplies, backed scrutiny of inward investment in critical sectors, discouraged export restrictions even of "essential goods," and is considering regulatory actions to support increased manufacturing capacities, e.g. through speeding up the approval of a new manufacturing line or site.²⁴

Under normal conditions, reliance on imports of pharmaceuticals and medical or protective equipment would not present a direct security threat. However, when conditions change rapidly as they have in the past couple of months, security risks attached to such imports can emerge quickly. Cost pressures and a lack of domestic manufacturing capacity raise the specter of an overreliance on China for finished or intermediate goods, including active pharmaceutical ingredients, medical devices and other medical tools like testing kits. Beyond goods, long import supply chains might result in an excessive reliance on Chinese-based labs and firms for key pharmaceutical IP and/or drug research.

The COVID crisis has illustrated how an abrupt interruption in supply can affect Europe's medical readiness. There are several options for mitigating such risks, without a wholesale severing of ties in the sector. A diversification of suppliers and import countries can help minimize supply disruption risks presented by any one nation – but allow important interactions with China to continue. Where suppliers or import countries are too few, the EU can also encourage selective relocation for medical, pharmaceutical and equipment firms in order to shorten supply chains. This might involve reshoring to the EU itself, or to third countries (the EU's neighborhood, for geographical proximity, or in "like-minded countries" for strategic and ideological proximity). Additionally, the EU can utilize existing FDI screening mechanisms to scrutinize inward transactions and ensure adequate healthcare and R&D capacity remains EU-owned. For certain non-perishable pharmaceutical products, stockpiling might also be an option, as might stand-by production facilities – though both come at a high cost. For each of these mitigation steps, Europeans policymakers would need to prioritize most essential drugs for cost management, i.e. investing most resources for diversification in products deemed most essential, while maintaining most existing interactions, in their current form, with China for less pressing needs and goods.

23 "U.S. Offered 'Large Sum' to German Company for Access to Coronavirus Vaccine Research, German Officials Say," New York Times, March 15, 2020. <https://www.nytimes.com/2020/03/15/world/europe/coronavirus-vaccine-us-germany.html>.

24 European Commission, "Coordinated economic response to the COVID-19 Outbreak," Communication from the Commission to the European Parliament, The European Council, the Council, The European Central Bank, The European Investment Bank, and the Eurogroup, COM(2020) 112, https://ec.europa.eu/info/sites/info/files/communication-coordinated-economic-response-covid19-march-2020_en.pdf; "EU authorities agree new measures to support availability of medicines used in the COVID-19 pandemic," European Medicines Agency, Press release, April 6, 2020. <https://www.ema.europa.eu/en/news/eu-authorities-agree-new-measures-support-availability-medicines-used-covid-19-pandemic>.

Conclusion

By developing a methodology for exploring the breadth of EU-China economic activity that is not of strategic concern, this study can enable better policy-making and corporate decision-making. It also provides a useful frame for thinking about the debate over moving certain production chains back to Europe that has been triggered by the COVID-19 catastrophe and the critical input shortages it produced.

Before summarizing our conclusions and caveats, it is important to reiterate our two starting premises. First, there is no such thing as a riskless world, whether the subject is China or other competitors. Second, trade-offs between security and economic welfare are not without costs. Engagement with China has brought with it security concerns for Europe which need to be more closely examined. It is important to note that this engagement does not bring only risks. It can also bring security benefits, for instance when European firms and researchers obtain cutting-edge insights through partnerships with Chinese counterparts. The benefits to be derived from foreign trade and investment are, after all, the reason why China opened its doors in 1978. This is the context within which our attempt to “green list” benign activity should be seen.

Our first conclusion is that most of the EU-China trade relationship, based on 2019 data, can remain open without any new mitigation measures. The biggest green-list items by trade value are electronics, accessories for motor vehicles, food processing and preserving, and diverse luxury and fashion items. Some of the benign sectors for trade are also critical ones for the EU economy, such as exports of motor vehicles and electrical components, and imports of consumer goods and electronics.

Second, we find that FDI vulnerabilities are somewhat more acute, involving about 46% of China's FDI to the EU and 32% of the EU's FDI to China in 2019. Investments with potential security implications involve sensitive individual data, critical infrastructure and emerging computing technologies.

Third, we find that reasonable mitigation options are available to help expand the green list, reducing the potential burden on governments and firms that are reassessing their trade and investment engagement with China. We discuss 15 varieties of mitigation, and we believe that others exist.

Various caveats should be considered when drawing conclusions from these results. First, this is an initial, experimental exercise. It was completed over six months by a small team of researchers without the benefit of peer review or a study group to offer critiques. Many of the criteria we apply are derived from idiosyncratic assumptions, and our checklist relies on definitions and policy guidance that are subject to rapid change.

Second, we have only undertaken the first-round assessment of a green list, and only at the 4-digit level for NACE categories. More granular analysis would be needed to determine exactly which dual-use or sensitive technologies are potentially problematic, and which essential goods and critical inputs might require further mitigation steps. In addition, we do not consider second-order effects of such interactions, for example technology or security externalities on other sectors, or broader welfare effects that might also impact national security indirectly.

Third, the real-world assessment of security vulnerabilities related to economic engagement with China is evolving fast, and this report is a picture in time and its findings set to evolve. There are ongoing debates in the EU about what constitutes essential goods or critical infrastructure. There is heavy US pressure on Brussels and EU capitals to align with new frameworks for defining critical technologies. The red lines we used to mark security concerns are not meant as an endorsement, just our interpretation of current thinking. Many emerging and foundational technologies could be determined to have national security implications in the future. Flexibility, therefore, is essential.

Fourth, the COVID-19 crisis has accelerated a debate about a range of concerning trade dependencies, especially as they relate to essential goods. Since the vulnerability-benefit calculus is liable to change fast, and it is too risky, costly and undesirable to preemptively disengage on a broad scale, member states will need to spend more time thinking about mitigation.

Finally, the EU-specific green list established in this report needs to be held up against the approach of other OECD countries. It is vital to compare perceptions and definitions of sensitive sectors, discuss potential vulnerabilities and, where possible, align policies, including on mitigation measures aimed at reducing the extent and cost of disengagement.

At the moment, the green list we have generated for the EU's interactions with China is an expansive one – broader, no doubt, than an equivalent US list of benign interactions with China would be. This reflects the EU's continued openness. Yet to keep doors open going forward, the EU will also need to launch a frank and open debate about the areas of its economy that it considers national security relevant today, and which sectors could meet this definition tomorrow. Although existing EU documents, regulations and statements are clear on some of these sectors, there is no evident European consensus on this crucial question. Only with clear definitions in place will Europe be able to engage with partners, or rivals, and defend its own positions. Failing that, the EU could find itself in a position where foreign definitions of national security are being imposed upon it. The EU needs to state clearly that some aspects of its economic relationship with China pose security risks, while others do not. Only by acknowledging this dichotomy can it credibly keep the door open to benign economic engagement and mitigate the risks in areas that are potentially problematic.

Appendix 1 – Green-List Categories

TABLE 4 Green List Categories (2-Digit Level, Full List)

SECTION	DIVISION	DESCRIPTION	GREEN-LIST CLASSES	GREEN LIST AS A % OF SUB-CATEGORIES	SCREENING QUESTIONS
A	1	Crop and animal production, hunting and related service activities	31	100%	
A	2	Forestry and logging	4	100%	
A	3	Fishing and aquaculture	4	100%	
B	5	Mining of coal and lignite	2	100%	
B	6	Extraction of crude petroleum and natural gas	None	0%	Q08
B	7	Mining of metal ores	3	100%	
B	8	Other mining and quarrying	6	100%	
B	9	Mining support service activities	2	100%	
C	10	Manufacture of food products	25	100%	
C	11	Manufacture of beverages	7	100%	
C	12	Manufacture of tobacco products	1	100%	
C	13	Manufacture of textiles	5	50%	Q02
C	14	Manufacture of wearing apparel	6	75%	Q02
C	15	Manufacture of leather and related products	2	67%	Q02
C	16	Manufacture of wood and of products of wood and cork, except furniture; manufacture of articles of straw and plaiting materials	6	100%	
C	17	Manufacture of paper and paper products	7	100%	
C	18	Printing and reproduction of recorded media	3	60%	Q10
C	19	Manufacture of coke and refined petroleum products	2	100%	
C	20	Manufacture of chemicals and chemical products	3	19%	Q01, Q02, Q03
C	21	Manufacture of basic pharmaceutical products and pharmaceutical preparations	None	0%	Q02, Q03
C	22	Manufacture of rubber and plastic products	2	33%	Q02, Q03
C	23	Manufacture of other non-metallic mineral products	16	67%	Q02, Q03
C	24	Manufacture of basic metals	6	38%	Q01, Q02, 03
C	25	Manufacture of fabricated metal products, except machinery and equipment	7	41%	Q01, Q02

C	26	Manufacture of computer, electronic and optical products*	1	10%	Q02, Q03, Q08
C	27	Manufacture of electrical equipment	1	10%	Q02, Q03
C	28	Manufacture of machinery and equipment n.e.c.	3	14%	Q02, Q03, Q09
C	29	Manufacture of motor vehicles, trailers and semi-trailers	2	50%	Q02
C	30	Manufacture of other transport equipment	4	50%	Q01, Q02
C	31	Manufacture of furniture	3	75%	Q02
C	32	Other manufacturing*	6	67%	Q02, Q03
C	33	Repair and installation of machinery and equipment	8	89%	Q01
D	35	Electricity, gas, steam and air conditioning supply	None	0%	Q08
E	36	Water collection, treatment and supply	None	0%	Q08
E	37	Sewerage	None	0%	Q08
E	38	Waste collection, treatment and disposal activities; materials recovery	2	33%	Q01, Q08
E	39	Remediation activities and other waste management services	1	100%	
F	41	Construction of buildings	2	100%	
F	42	Civil engineering	7	100%	Q08
F	43	Specialised construction activities	13	100%	
G	45	Wholesale and retail trade and repair of motor vehicles and motorcycles	6	100%	
G	46	Wholesale trade, except of motor vehicles and motorcycles	48	100%	
G	47	Retail trade, except of motor vehicles and motorcycles	37	100%	
H	49	Land transport and transport via pipelines	1	13%	Q08
H	50	Water transport		0%	Q08
H	51	Air transport	1	33%	Q08
H	52	Warehousing and support activities for transportation	1	17%	Q08
H	53	Postal and courier activities	2	100%	
I	55	Accommodation	4	100%	
I	56	Food and beverage service activities	4	100%	
J	58	Publishing activities	1	14%	Q10
J	59	Motion picture, video and television programme production, sound recording and music publishing activities	2	40%	Q10
J	60	Programming and broadcasting activities	None	0%	Q06, Q10
J	61	Telecommunications	None	0%	Q08
J	62	Computer programming, consultancy and related activities	None	0%	Q03, Q05, Q08
J	63	Information service activities	1	25%	Q08, Q06, Q10, Q09
K	64	Financial service activities, except insurance and pension funding	3	43%	Q08
K	65	Insurance, reinsurance and pension funding, except compulsory social security	1	25%	Q06, Q08
K	66	Activities auxiliary to financial services and insurance activities	4	57%	Q06, Q08
L	68	Real estate activities	4	100%	

M	69	Legal and accounting activities	2	100%	
M	70	Activities of head offices; management consultancy activities	2	67%	Q10
M	71	Architectural and engineering activities; technical testing and analysis	2	67%	Q08
M	72	Scientific research and development	3	100%	
M	73	Advertising and market research	1	33%	Q10
M	74	Other professional, scientific and technical activities	4	100%	
M	75	Veterinary activities	1	100%	
N	77	Rental and leasing activities	12	100%	
N	78	Employment activities	3	100%	
N	79	Travel agency, tour operator and other reservation service and related activities	3	100%	
N	80	Security and investigation activities	None	0%	Q01, Q06, Q10
N	81	Services to buildings and landscape activities	4	80%	Q04
N	82	Office administrative, office support and other business support activities	6	86%	Q06
O	84	Public administration and defence; compulsory social security	None	0%	Q05, Q05, Q08, Q09
P	85	Education	11	100%	
Q	86	Human health activities	None	0%	Q06, Q08
Q	87	Residential care activities	None	0%	Q06, Q08
Q	88	Social work activities without accommodation	2	67%	Q06, Q08
R	90	Creative, arts and entertainment activities	4	100%	
R	91	Libraries, archives, museums and other cultural activities	4	100%	
R	92	Gambling and betting activities	1	100%	
R	93	Sports activities and amusement and recreation activities	6	100%	
S	94	Activities of membership organisations	5	83%	Q10
S	95	Repair of computers and personal and household goods	8	100%	
S	96	Other personal service activities	4	80%	Q06
T	97	Activities of households as employers of domestic personnel	1	100%	
T	98	Undifferentiated goods- and services-producing activities of private households for own use	2	100%	
U	99	Activities of extraterritorial organizations and bodies	1	100%	

Source: Rhodium Group research.

| BertelsmannStiftung

Appendix 2 – Methodological Addendum

Q1: Does the sector/subsector provide goods or services that qualify as weapons or arms, or related to the country's nuclear material production capacity?

- **Definition:** Conventional arms as defined in Arms Trade Treaty (ATT) Art 2, to include: Battle tanks; Armored combat vehicles; Large-caliber artillery systems; Combat aircraft; Attack helicopters; Warships; Missiles and missile launchers; and Small arms and light weapons; in addition to nuclear weapons, nuclear material production capacity, and related technology.
- **Coding caveat:** We include in our coding nuclear assets and elements of nuclear fuel mining and production, as the provision and control of nuclear technology that may be directly or indirectly used to support weaponization is a clear security threat. On the inbound side, civilian nuclear projects have been the subject of Chinese investment, including the Hinkley Point nuclear power plant in the United Kingdom,²⁵ and EU firms have been active in building and supplying China's civilian nuclear power sector (including French firm Framatome, formerly Areva²⁶). These civilian exchanges are primarily concerning as they involve critical infrastructure but do raise the prospect that civilian technology could be used to advance military objectives. Note that these technologies may be subject to EU and member-state dual-use regulations (Q2) and/or critical infrastructure guidelines (Q7).

Q2: Does the sector/subsector provide goods or services that qualify as dual-use?

- **Definition:** EU dual-use controls, 2019 update.

Coding caveat: Our list of coded sectors is a partial, preliminary one for two reasons. First, it is based on our coding of the Annex I EU dual-use regulations (5,672 line-items).²⁷ For most of the list (72%; 4,033 items), we are able to obtain a

25 Adam Vaughan and Lily Kuo, "China's Long Game to Dominate Nuclear Power Relies on the UK," *The Guardian*, July 26, 2018, sec. Environment, <https://www.theguardian.com/environment/2018/jul/26/chinas-long-game-to-dominate-nuclear-power-relies-on-the-uk>.

26 "Framatome- Large Projects - Taishan 1 and 2," accessed April 14, 2020, <https://www.framatome.com/EN/businessnews-320/framatome-large-projects-taishan-1-and-2.html>.

27 Regulation (EC) No 428/2009. We utilize the 2019 Update to the EU Control List (October 17, 2019) as a basis.

translated CPA/NACE code using a series of concordance tables, which we then utilize for further analysis.²⁸ For 1,639 items, however, we are unable to derive a sufficiently accurate translated NACE code. We omit these dual-use items from our set and do not consider them.²⁹

Second, our coding does not allow us to distinguish between dual-use goods in the same way that regulators and exporters do. Our analysis requires us to evaluate dual-use trade and investment in aggregate, at the sectoral level. However, in practice, dual-use regulations are extremely dependent on the context of individual transactions. Similar goods, and even those which have the same statistical or trade codes, may be dual-use controlled in one transaction and unrestricted in another. This distinction depends on technical properties, where only items that meet criteria for e.g. tensile strength or power output require special controls. In other cases, regulations define dual-use goods by application, drawing a line between goods with specifically “civilian” or “laboratory” capabilities (non-controlled) and those that are designed or are modifiable for “military” or other purposes (controlled), even before consideration of the end-user. Because we consider dual-use items at the sectoral level, without the mitigating context and details that would be provided by a specific transaction, our intermediate list designates a large number of NACE sectors as security sensitive at the 4-digit level.

Of these sectors, many, however, include only a few individual goods or services that could theoretically qualify as dual-use. We therefore revise our list of dual-use sectors to better reflect actual levels of sensitivity. Where NACE 4-digit level categories include a small number of dual-use goods (for example, protective footwear for use in chemical/biological/nuclear applications) but a majority of non-sensitive ones (footwear and apparel) we manually bring the sector *back* to the green list.

Finally, it is worth noting that EU’s dual-use regulations are regularly updated and continue to evolve. They may notably be modified in the future to reflect increased pressure from the US and other OECD partners around certain key emerging or foundational technologies.³⁰ We do not include such potential changes in our coding for Q2. Additionally, because of presumed licensing requirements for dual-use exports as discussed in the report, we do not include Q2 items in our visualizations of the final green list by economic channel for exports, imports and OFDI.

28 We first translate dual-use (DU) codification numbers to CN (2020) trade codes using existing EU concordance tables. We then utilize Eurostat concordance tables (CN to CPA 2.1 [Classification of Products by Activity]) to obtain a product category code. By design, these CPA product categories are equivalent NACE sectors at the 4-digit level, allowing us to identify a final 4-digit NACE code (the “class” level in the NACE Rev. 2 system). For a similar approach and some other caveats, see SIPRI and Ecorys, “Final Report: Data and information collection for EU dual-use export control policy review,” November 6, 2015, https://trade.ec.europa.eu/doclib/docs/2016/september/tradoc_154962.PDF.

29 As a secondary check, we match CN codes to relevant PRODCOM codes again using Eurostat concordance tables. We omit codes that do not match this secondary check. These include some DU software and technical categories that are governed by specific Notes in Annex I, which highly depend on transactional context.

30 Although some cyber-surveillance tools, for example, are already enumerated on the Wassenaar Arrangement list, the US signaled it will pursue tighter controls as part of its broad export control and investment screening reform in 2019/2020. The Commission, Parliament and Council, while agreed that cyber-surveillance should be covered under export controls, have yet to reach consensus on whether the EU should match or exceed US standards, as well as what technologies should be covered. SIPRI, op. cit.

Q3: Does the sector/subsector involve other “critical technologies” relevant to military-based national security?

- **Definition:** European investment screening regulations (EU 2019/452), to include: Artificial intelligence; Robotics; Semiconductors; Cybersecurity; Quantum technologies; Energy storage; Biotechnology; Nanotechnology.
- **Coding caveat:** There is no universal definition of critical or so called “next-generation technology,” either at an international or an EU level, and concepts explored by the EU and even close allies like the United States often differ substantially. The definition we use here – based on the EU Key Emerging Technologies (KET) list, as well as codes where we could identify an analogue to technologies described in the EU investment screening – is therefore one of several possible options. Here again, NACE categories at the 4-digit level do not offer the level of granularity required to identify specific KET goods, especially in complex fields like biotechnology or batteries. In addition, the line is even blurrier in KET between civilian and military applications (“artificial intelligence” and machine learning software may be used to manage traffic patterns and guide military deployments and simulations). As done in Q2, we leave out *applications* and only focus on goods and services, and again keep on the green-list sectors where civilian goods and applications seem to represent a majority of the NACE subsector. Finally, the rapid growth and evolution of new technologies makes it almost impossible for analysts and policymakers to predict what existing technologies may *become* sensitive in the future, or to predict the ultimate capabilities of a set of existing products or services. We do seek to identify such potentially problematic technologies in our coding for Q2.

Q4: Does the sector involve goods and services directly related to military infrastructure and systems?

- **Definition:** “The buildings and permanent installations necessary for the support, deployment, and operation of a nation’s military, to include information systems.” (RAND)
- **Coding caveats:** Coding for services and goods provided to military and intelligence organizations is made difficult by the fact that such products most often involve otherwise innocuous activities like catering or clothing production for military units. These sectors are not inherently security-sensitive, but where the customer or client is a military (or government) institution, they may be considered a secondary security risk, from bugged equipment to knowledge of military infrastructure floor/organization plans. Our coding adopts the stance that even if these sectors present a secondary security risk, they should not be coded out of the green list, as this would result in an overstatement of security relevance for most of these sectors – unless they qualify under Q1, Q2 or Q3, of course. Most importantly, secondary security risks would most often be addressed by (already existing in many cases) client and customer-specific measures, including specific procurement regulations, bidder/contractor qualification procedures, security vetting of specific contractors and employees.

Q5: Does the sector involve collection, storage or transmission of intelligence or intelligence-related data that would directly compromise EU security?

- **Definition:** “Intelligence or intelligence-related data” is defined here as the standard for EU classified data (Commission Decision 2015/444), i.e. “...any [intelligence] information or material...the unauthorized disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States.” Specifically, this applies to sensitive data generated to the following NACE sectors (NACE 84.2): Foreign affairs; Defense activities; Justice and judicial activities; Public Order and safety activities.
- **Coding caveats:** Our framework includes NACE categories 84.21 (Police services, including border and special police forces), as well as 84.22 (which includes defense services and intelligence aspects of defense services). We consider coding computer and other services (including IT applications, hardware, software, cybersecurity and data services) as their use by intelligence organizations clearly presents a security risk, yet as we note for Q4, this would lead to dismissing the wide array of related goods and services *not* procured by military and related institutions – and therefore underestimate green list-able sectors. As this threat can be directly addressed through specific restrictions on procurement and security protocols and standards, we keep these sectors in at this stage. **However, our framework does encourage closely monitoring investment patterns in such sectors, for the purpose of enforcing those existing internal rules and security checks, and to ensure a diversity of suppliers.**

Q6: Does the sector involve the collection, storage or transmission of personal data that might be accessed by foreign state actors to identify and compromise military or intelligence personnel?

- **Definition:** from GDPR (Reg 2016/679) (Art 9): GDPR specifies how persons can be damaged by exposing of data related to: “racial or ethnic origin”; “political opinion”; “religion or philosophical beliefs”; “trade union membership”; “data concerning health...”; “...data concerning sex life”; “...criminal convictions and offences or related security measures”; and “...economic situation.” Hence, relevant sectors include: Healthcare and social care; Social media; Consumer financial operations; Activities of membership organizations (including trade unions); Public administration and services; Dating services.
- **Coding caveat:** Digital activities that produce *exploitable* personal data are generally difficult to match to a single NACE sector. Social media platforms, for example, provide online advertisements (63.12), operate “web portals” (63.11) and conduct “computer programming activities” (62.01, which covers essentially any kind of programming, whether hardware or software). For social media and similar companies, we include all relevant activities as potentially security relevant. For other activities involving data collection, we follow the principles described in Box 1 and Q6, and focus on sectors where data is most directly exploitable.

Q7: Does the sector/subsector involve the provision of “basic economic goods” or “critical inputs”?

- **Definition:** “Critical raw materials” (CRM) as defined by the Commission in its most recent “list of critical raw materials,” including rare earths and other key inputs for advanced tech. “Basic economic goods” are “essential goods and services” as defined by the EU Commission, to include food, energy, transport, electronic communications and financial services. Though pharmaceutical and other health-related goods are not included in the EUC’s list, we add the sector to the list in light of significant disruptions and related issues highlighted during the COVID-19 crisis.
- **Coding caveats:** Establishing a baseline for “critical goods” is difficult, especially given the wide variety of goods possibly included in definitions of criticality. Tentative coding of NACE sectors for categories that include such critical goods highlights roughly 70 categories, primarily codes in agricultural production (NACE 1) and food manufacturing (NACE 10), but also categories related to pharmaceuticals, surgical and medical devices, and personal protective equipment (including NACE 21 and 32.50), as well as a handful of sectors containing relevant raw materials from the CRM list.

Q8: Does the sector qualify as a sector of critical infrastructure (CI) or essential network and information system (NIS)?

- **Definition:** EU critical infrastructure/critical information infrastructure (2008/2009) and NIS (2016) categories: Energy (including energy production, transmission, and oil and gas); Transport (road/rail/air/waterways/ocean); Banking; Financial market infrastructure; Healthcare sector; Drinking water supply and distribution; Digital infrastructure (specifically for provision of internet services).
- **Coding caveat:** Our definition is based on two documents: the European Union’s Critical Infrastructure (CI) rules from 2008 (Dir 2008/114/EC, the “CI Directive”) and the Network and Information Systems (NIS) directive from July 2016 (Dir (EU) 20016/1148, the “NIS directive”). It is important to note that both are focused on identifying particular *installations, equipment* or *entities* as CI or NIS, rather than identifying broad *sectors* of concern. Our coding instead adopts a maximalist approach at this stage, covering whole sectors qualifying as either CI or NIS – including operations as well as equipment and contracting. We’ll show that some of these can be brought back to the green list through mitigation measures.

Q9: Does the sector provide technology for services for EU electoral infrastructure, including election technology?

- **Definition:** This includes, from EU Commission Recommendation C(2018) 5949: “networks and systems used for”; “registering voter rolls and candidates”; “collecting, processing and counting votes”; “publishing and communicating election results to the wider public”; as well as, from COM(2018) 637: “electoral processes, campaigns, political party infrastructure, candidates or public authorities’ systems.”

- **Caveat:** The identified sectors contain electoral equipment used in elections alongside numerous other non-relevant products. For example, the sector that includes manufacturing of voting equipment (NACE 28.23) covers all “office machinery and equipment,” and hence also contains calculators and staplers. Voting equipment is likely only a small subset of the total NACE sector. And the wide array of electronic and online tools used to administer elections, including to create and check electoral rolls, is classified under NACE 63 categories including data processing or software engineering.

Q10: Can the sector be used as a means of disinformation (“deliberately false, distorted or misleading information”) or propaganda (“content that is not subject to verification, such as biased or exaggerated opinions or manipulated content aimed at misleading the audience, especially content inciting negative emotions”)?

- **Definition:** Defined as sectors involving the ability to influence or harm the “freedom and pluralism of the media” (EU Final Report for EC Vice President Neelie Kroes, September 2012), or sectors subject to mass disinformation and opinion manipulation. Relevant sectors include: social media; book and newspaper publishing; motion picture, video, and television production; broadcasting; and public relations or lobbying.

- **Coding caveat:** Issues with defining social media-related sectors are the same as in Q6.

Q11: Does the sector involve collection, storage or transmission of personal data that might be accessed by Chinese state actors to identify and compromise key decision makers/stakeholders?

- **Definition and coding caveats:** Same as in Q6.

Imprint

© Bertelsmann Stiftung, Gütersloh
September 2020

Bertelsmann Stiftung
Carl-Bertelsmann-Straße 256
33311 Gütersloh
Germany
www.bertelsmann-stiftung.de

Responsible

Bernhard Bartsch, Senior Expert, Bertelsmann Stiftung
Anika Laudien, Project Manager, Bertelsmann Stiftung

Authors

Agatha Kratz, Associate Director, Rhodium Group
Matthew Mingey, Research Analyst, Rhodium Group
Daniel H. Rosen, Founding Partner, Rhodium Group

Graphic Design

Markus Diekmann, Bielefeld

Picture credits

©blackzheep – AdobeStock
©Matthias Enter – Fotolia

Printing

Hans Gieselmann Druck und
Medienhaus GmbH & Co. KG

The authors would like to thank

Lauren Gloudeman for her research support.
Thilo Hanemann for his substantive inputs.
All participants of the online roundtable
sessions between May and July 2020 for their
constructive feedback. All interviewees for
their time and insights.

Address | Contact

Bertelsmann Stiftung
Carl-Bertelsmann-Straße 256
33311 Gütersloh
Germany
Phone +49 5241 81-0

Program Germany and Asia
asien@bertelsmann-stiftung.de

www.bertelsmann-stiftung.de