

The present note is a preliminary summary of research carried out on current and emerging trends in acquisition- and ownership-related policies put in place to safeguard countries' essential security interests. It has not yet been discussed or approved by the countries that participate in OECD-hosted policy dialogue on international investment policies. Its sole purpose is to inform participants in an [OECD conference on acquisition- and ownership-related policies to safeguard essential security interests](#), scheduled to be held on 12 March 2019 in Paris. The present document should not be reported as representing the official views of the OECD or of its Member countries. The opinions expressed and arguments employed are those of the authors.

The European Union co-finances the work under which this research note has been prepared.

This document and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area. The statistical data for Israel are supplied by and under the responsibility of the relevant Israeli authorities. The use of such data by the OECD is without prejudice to the status of the Golan Heights, East Jerusalem and Israeli settlements in the West Bank under the terms of international law.

To contact the authors, please write to Joachim Pohl, Joachim.pohl@oecd.org or call +33 1 45 24 95 82.

Table of contents

Context and purpose of this note.....	4
Current and emerging trends in acquisition- and ownership-related policies to safeguard essential security interests.....	7
1 Constituting elements of acquisition- and ownership-related policies to manage risks for essential security interests	9
2 Whether and which policies to manage risks associated with acquisition or ownership are warranted remains controversial	12
3 Policies continue to show little convergence towards common criteria and procedural designs	14
4 Perceptions evolve further of which assets are sensitive and how threats may materialise	16
Changes in the perceptions of sensitive assets	16
Additional transmission channels for threats emerge.....	18
5 Four traditional features fade	18
Acquisition and ownership.....	19
Foreign and domestic acquirers.....	19
Controlling stakes vs any interest.....	20
Inward investment vs any trans-border asset transfer	20
6 Risks to essential security interest originating in non-ownership transactions come to the fore	22
Leases, concessions and public procurement	22
Use of equipment in privately- or publicly owned sensitive infrastructure assets and supply chains.....	24
International research cooperation and global allocation of venture and human capital	25
7 Interaction increases between acquisition- and ownership-related policies and other norms of domestic and international law	26
8 Dilemma situations emerge from policy practice.....	27
9 International cooperation – from harmonisation to mutual recognition – may become increasingly critical	29

Figures

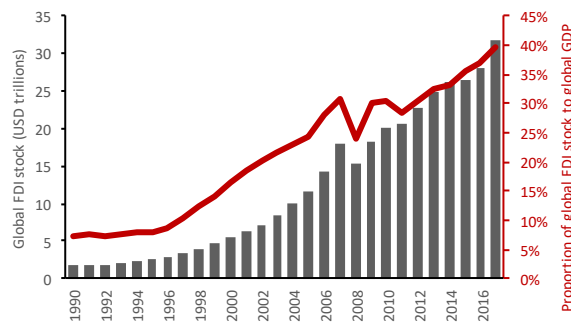
Figure 0.1. Introduction of first- and second-generation policies over time – number of new policies per year and trend in the repartition among types	12
Figure 0.2 Evolution of acquisition-related policies to manage essential security interest since 1990.	13
Figure 0.3. Regulatory Restrictiveness for FDI and presence of a second generation acquisition-related policies to safeguard essential security interests.....	14

Context and purpose of this note

1. Over the past decades, many countries have eliminated most barriers to trans-border capital flows. This openness has created vast economic opportunities for home and host economies as well as for businesses. With these opportunities came occasional risks, not least potential risks for the host country’s essential security interests. International investment instruments and many investment treaties or investment content in regional trade agreements explicitly recognise countries’ rights to manage such risks.

2. Many countries have established some restrictions on foreign ownership or authorisation requirements in certain areas or sectors. Often, these policies date back several decades. As international investment took essentially place among allies and had much smaller proportions of FDI to GDP than today – in 1990 only 7% – such policies received little attention.

3. Today, many parameters are different: the proportion of world FDI to world GDP has increased six-fold, reaching 40% in 2017 (see insert). Privatisation of infrastructure assets that many advanced economies carried out during the 1980s and 1990s created potential for foreign investment, but also fears in some countries that malicious owners could sabotage or withhold access to this “critical infrastructure”.



Source: OECD calculations based on IMF World Economic Outlook database; IMF Balance of Payments Database; OECD Foreign Direct Investment statistics database.

4. Broader concerns and a formal policy response to these concerns began to emerge only as of the mid-2000s, fuelled by the additional factor of consistently high oil prices, which drove an acquisition boom from oil-exporting economies that were not traditional allies of advanced economies and that often involved less-than-transparent sovereign wealth funds (SWFs). A few, but only a few, countries introduced formal policies to respond to newly identified potential threats in a broader set of sectors. Subsequently, internationally agreed standards of behaviour of SWFs – the [Santiago principles](#) –, as well as [OECD Guidelines for recipient country investment policies related to National Security](#), and the [OECD Declaration on SWFs and Recipient Country Policies](#) and changing global economic conditions with the advent of the financial and economic crisis attenuated attention to this policy area.

5. Fifteen years after the emergence of wider interest in investment policies motivated by national security concerns associated with foreign ownership, a second, much broader reconsideration of this policy area is currently underway. Ever more countries complement their traditional ownership caps in narrow sectors with new policies that capture risks to broader sets of sectors; some countries that have adopted such policies earlier are making significant adjustments to their mechanisms.

6. The introduction of new policies is driven by several factors – and heightened awareness –, including:

- technological developments and digitalisation that have turned personal data – and companies that possess such data – into sensitive assets that may be subject to misuse or malicious manipulation;

- interdependencies and a shift of global economic weights that has created new dependencies, interests, and threats;
- heightened sensitivity over the control of assets that constitute critical infrastructure; and
- new and more widely shared concerns, in addition to espionage and sabotage, in particular about diversity of suppliers, and access to advanced technology, today and in the future.

7. These changes coincide with broader efforts to avert newly identified risks to essential security interests that are transmitted through other channels than ownership, such as vulnerabilities of networks to espionage and sabotage or attacks on data integrity, among others. Policies that seek to manage risks resulting from ownership are one among several responses to threats that malicious actors may pose to societies.

8. In the face of uncertainty and risk, diligent design of policies is paramount. In 2009, countries that had participated in the OECD-hosted dialogue on international investment policies adopted [Guidelines for recipient country investment policies relating to national security](#). The adoption of these guidelines was preceded by intensive policy dialogue and analysis,¹ and summarised what the policy community at the time considered good policy in this area. The Guidelines have since served as a benchmark for policy design beyond the 38 governments² that have formally adhered to the instrument.

9. Under the OECD investment instruments and as a follow-up process to the Guidelines, the OECD-hosted international investment policy community continues to receive notifications of new policies, and discussed a comparative study of countries' policies in this area in 2015.³ That report covered 17 of the now 62 economies that are invited to participate in the OECD-hosted policy dialogue.⁴

10. Much has changed in this policy area since the release of the first comparative study of investment policies related to national security by the OECD in 2016. In the past two years alone, nine out of the world's largest ten economies have modified or introduced new, comprehensive

¹ Some studies that supported and resulted from the conversations at the time are publicly available, including: [Identification of foreign investors: A fact finding survey of investment review procedures](#), May 2010; [Security-related Terms in International Investment Law and in National Security Strategies](#), May 2009; [Accountability for Security-Related Investment Policies](#), November 2008; [Transparency and Predictability for Investment Policies Addressing National Security Concerns: A Survey of Practices](#), May 2008; [Proportionality of Security-Related Investment Instruments: A Survey of Practice](#), May 2008.

² Adherents to the Guidelines include all OECD Members as well as Argentina, Colombia and Kazakhstan.

³ The document is publicly available as Frédéric WEHRLÉ/Joachim POHL, "[Investment Policies Related to National Security: A Survey of Country Practices](#)", OECD Working Paper on International Investment 2016/02.

⁴ The economies that are invited to participate in the dialogue include: Argentina, Australia, Austria, Belgium, Brazil, Bulgaria, Canada, Chile, China, Colombia, Costa Rica, Czech Republic, Denmark, Egypt, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, India, Indonesia, Ireland, Israel, Italy, Japan, Jordan, Kazakhstan, Korea, Latvia, Lithuania, Luxembourg, Malaysia, Mexico, Morocco, Netherlands, New Zealand, Norway, Paraguay, Peru, Poland, Portugal, Romania, Russian Federation, Saudi Arabia, Singapore, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Thailand, Tunisia, Turkey, Ukraine, United Kingdom, United States, Uruguay, and the European Union.

policies to manage acquisition- or ownership-related risk to essential security interests in response to a profound reassessment of risks and vulnerabilities.

11. The OECD Secretariat is currently preparing an up-to-date overview of policies that 62 countries and jurisdictions that are invited to participate in OECD-hosted policy dialogue on this matter have currently in place to manage acquisition- and ownership-related risk for their essential security interests. This report is expected to become available in the latter half of 2019.

12. The present note, which is part of this work, summarises current and emerging trends in this policy area. Its main purpose is to identify the contours of the class of policies that address acquisition- and ownership-related risk, retrace the overall trends and evolution of these policies, position acquisition- and ownership-related policies in relation to adjacent areas, highlight challenges that policy design and implementation meet, and set out how reforms and future initiatives could help respond to these challenges.

13. The information presented in this note is drawn from notifications required under certain OECD instruments,⁵ information made publicly available by governments, and other material provided by government or non-government sources. The findings and interpretations presented in this note do not necessarily reflect the views of the OECD, its Member countries or non-Members that participate in OECD-hosted policy dialogue on international investment policy.

14. Developing a complete and static picture of a very dynamic policy area with many confidential elements comes with particular challenges. While all reasonable care has been taken in the preparation of this note, available information may not always be complete and up-to-date and policy documents referred to and linked in this paper may no longer be available. Also, while special care has been taken to identify authoritative sources, some information is based on reports by third parties, in particular media sources in certain cases; these quotes do not represent endorsements but merely document the context in which certain information has been brought into the public domain.

⁵ Countries that have adhered to the [OECD Declaration on International Investment and Multinational Enterprises](#) are required to notify their investment policies related to national security. The policies are recorded in the [List of measures reported for transparency, which is annexed by country to the National Treatment instrument](#). Adherents to the OECD Codes of Liberalisation are required to notify measures that have a bearing on the Codes, but while this information is available to the OECD Secretariat and Members, it is not always instantly available to the public. Further information was drawn from the [policy monitoring](#) that the Secretariat carries out, as well as from sources accessed by the OECD Secretariat in its independent research.

Current and emerging trends in acquisition- and ownership-related policies to safeguard essential security interests

15. Governments manage a great number of risks to essential security interest on a permanent basis. To fulfil this role, they have a broad set of instruments at hand, which include the possibility to restrict or condition the acquisition of ownership of assets by certain individuals. Restrictions on the acquisition or ownership of weapons and drugs are common examples for risk management by the means of restricting access or withholding ownership of certain items or assets. Some countries also have policies in place that restrict the acquisition or ownership of enterprises and some other types of assets that they deem sensitive, and where they believe that acquisition- and ownership restrictions are an adequate means to manage risk. These restrictions on acquisition and ownership of enterprises and a small group of other assets are the subject of this report.

16. Policies that seek to manage risk to countries' essential security interests by managing acquisitions and ownership of certain assets such as enterprises are an almost universal phenomenon in advanced and transition-economies, but have led an almost invisible existence for decades. As "investment policies related to national security", they consisted essentially of foreign-ownership caps or authorisation requirements in a few specified sectors. Other risks were managed "behind-the-border", by licensing requirements or other forms of regulating riskier assets.

17. Broader interest in acquisition-based policies to manage risk emerged in the mid-2000s, when Gulf-States' sovereign wealth funds (SWFs) made significant investments in advanced economies following an extended period of high oil prices, and in a context of heightened awareness about national security risk stemming from international terrorism, as illustrated by the public controversy in the United States about the acquisition of US-port facilities in 2006 by a UAE-investor.

18. By the time of these developments, advanced economies had widely opened up their economies to foreign capital – which at that time typically originated in other advanced economies – and now became concerned about the new prospective owners of certain assets or industries, as these acquirers were often less than transparent and may have had other than only economic motivations.

19. In 2008 and 2009, host economies participating in OECD-led policy dialogue agreed on standards designed to mitigate concerns and to reconcile openness with means of safeguarding national security.⁶ Shortly after, the financial and economic crisis drew attention to other issues, putting interest in investment policies related to national security to a temporary rest.

20. That period is over.

21. The reasons why this policy area has (re-)gained broad attention again now are in part reminiscent of circumstances that existed in the past: Concerns about investment originating in

⁶ These include the [Guidelines for Recipient Country Investment Policies relating to National Security](#) (2009), the [OECD Guidance on Recipient Country Policies Towards SWFs](#) (2008), and the [Sovereign Wealth Funds: Generally Accepted Principles and Practices](#) (2008), more widely known as "Santiago Principles".

less than transparent economies and by foreign State-controlled entities continue to play an important role in the risk assessment of open economies. New additional and aggravating factors are fuelled by technological change, the vulnerabilities created, transmitted or aggravated by advanced technology, and the dominance of data. A more assertive stance of some countries in global economic and strategic competition has likely also contributed to greater awareness and concerns about countries' interests and how they might be threatened.

22. Many aspects of this policy area are underexplored or controversial. This begins with the unadmitted uncertainty about the defining features of such policies and their position in governments' overall risk management strategies, especially where policies evolve rapidly and transcend boundaries of traditional categories. Section 1 clarifies the scope and defining features of acquisition- and ownership-related policies motivated by concerns about essential security interests.

23. Despite broadly similar economic conditions, degrees of openness and exposure to threats, there is no agreement among countries as to whether acquisition- and ownership related-policies that go beyond ownership restrictions or occasional authorisation requirements in narrow sectors are warranted to manage risks to essential security interests. Such decades-old foreign-ownership caps in a few narrow sectors aside, only about one third of the 62 advanced and emerging economies covered by this report had developed and at least somewhat detailed policies in early 2019. Despite continual policy dialogue for more than a decade, there are hardly any signs of convergence; if anything, perceptions about the merits of such policies appear increasingly polarised: The same countries that have introduced policies to address essential security risks associated with acquisition or ownership of specific assets are also those that pay regular attention to them as documented by frequent adjustments, while other countries continue to not consider the introduction of such policies (section 2).

24. Among countries that have advanced acquisition- and ownership-related policies, there are broad differences in approaches, criteria to identify risk, level of detail in formulated policy, procedures, as well as institutional and financial resources dedicated to the implementation of these policies. Even recently introduced policies or changes brought by recent reforms do not level these differences to the extent it could be expected given established peer-learning processes and available information (section 3).

25. In a subset of the countries surveyed for their policies in this area, some convergence appears with regard to new groups of assets and transmission channels of risk: While earlier policies had reflected concerns for essential security risks associated mainly with defence technology, and later with critical infrastructure, the most recent addition to the list of sensitive assets includes advanced technology and personal data; transmission channels through which threats are thought to materialise also become more diverse (section 4).

26. Policy designs have recently begun to diversify and are undergoing substantial innovations in some countries. Four traditional features that characterised the large majority of these policies in the past begin to fade: their activation at the time of an *acquisition*, their limitation to *foreign* acquirers, the focus on *controlling stakes*, and the limitation to *inward* investment into the country that applies the policies. More recently introduced policies tend to move away from these features, diversify and broaden the instruments to address risk beyond the traditional perimeter (section 5).

27. As part of a broader awareness and understanding of risks and types of exposure, transactions that are not acquisitions but may create similar exposure receive increasing attention in some countries: joint ventures, procurement, leases, use of certain equipment in critical infrastructure, and international research cooperation are among these transaction types. Against the background of these new scenarios, acquisition- or ownership-focused policies may increasingly appear as an insular solution to a broader challenge. The understanding of these

issues is still limited, and whether and which policy responses are warranted needs to be explored further (section 6).

28. The proliferation of acquisition- and ownership-related policies and their evolving design has brought about and revealed new challenges for policy making and implementation. Increasing interaction has been observed between these policies and obligations under domestic and international law. These interactions influence and occasionally constrain design and implementation of acquisition- and ownership-related policies, as set out in section 7.

29. Despite adaptable policies and continual reform, implementation of acquisition- and ownership-related policies have also brought to light a series of practical challenges. Dilemma situations have been observed in which seemingly straightforward rules and comprehensive powers to prohibit transactions may not lead to practical or desirable outcomes (see examples in section 8).

30. Finally, with the number of countries operating review mechanisms growing, the scope of their application expanding, and the complexity of value chains spanning ever more jurisdictions, the number of reviews that a single transaction needs to pass in individual jurisdictions and potentially contradicting mitigation measures may soon jeopardise the feasibility of major transactions overall. Alignment of criteria and procedures, cooperation or mutual recognition among review authorities may potentially offer solutions, following approaches and experience gained in other policy areas where multiple jurisdictions are triggered (section 9).

1 Constituting elements of acquisition- and ownership-related policies to manage risks for essential security interests

31. Policies to manage security risks associated with the acquisition or ownership of sensitive assets have a long history and exhibit very different features. This diversity has so far inhibited a common understanding of the contours and defining features. Recent trends in policy design and entirely new types of policies have further eroded the already vague outer limits of traditional “investment policies related to national security”.

32. Informed dialogue about policy design requires a shared understanding of concepts. In this area, a certain focus of attention on review mechanisms has excluded a large group of functionally equivalent policies, such as legislated ownership caps and more mundane authorisation requirements for certain acquisitions. These policies share many commonalities with review mechanisms, and different policy mechanisms are often combined in country practice. Some of these policies focus on acquisitions, others condition or limit ownership. Some policies are commonly identified as “investment policies related to national security”, a traditional and widely accepted notion that refers to acquisitions, but which tends to ignore policies that relate to ownership or forms of control that are not conveyed by ownership.

33. Further notional diversity stems from the legislative context and authorities that are involved in implementation: Some countries manage national security risks as part of competition reviews under “public-interest” tests. Such embedded reviews – while functionally equivalent to investment reviews – are not uniformly classified: The United Kingdom’s mechanism is widely considered – and has been notified to the OECD – as an investment policy related to national security, while other countries’ public interest test in competition-focused

merger reviews are not recognised in the same category.⁷ Similarly, the Federal Antimonopoly Service (FAS) of the Russian Federation, the country's competition authority, is in charge of implementing the country's rules on control of foreign ownership.

34. Some countries apply controls over acquisition and ownership of certain sensitive assets regardless of the nationality of the acquirer. For this reason, they are sometimes seen as an expression of general police powers of States and conceal their similarity to the more frequently observed acquisition controls that focus exclusively on foreign acquirers. Despite the difference in covered acquirers, these policies serve the same purpose as policies that focus solely on foreigners.

35. A further group – policies to manage risk associated with certain asset types that are inherently sensitive – has just emerged. These policies do not operate at entry but, like acquisition-based policies, seek to manage the risk to essential security interests that is specifically associated with ownership through mitigation measures and, in some cases, ownership controls.

36. Some policies have been observed that regulate transactions involving a government entity as the seller – e.g. rules on possible acquirers in privatisation of publicly owned property. Although these cases are technically acquisition-related policies to manage national security risks, the government can manage these potential risks through its choice of acquirer rather than through an intervention in a transaction between private parties. These policies are not currently the focus of government interest and are hence not included in the scope of this report.

37. Furthermore, rules have been observed in which certain operations – which may require a license – are closely tied to acquisitions, including through greenfield investments.⁸ Where the acquisition or establishment of an asset are tightly related to its operation for which a license is required, and no other use of the asset is reasonably possible beyond the use that requires a license, the government is in a position to manage the acquisition through the licensing procedure without resort to an acquisition-related policy. These policies that manage the acquisition-establishment-operation nexus through a licensing procedure are likewise not the focus of current debate and are thus also excluded from the scope of the present study.

38. The choice to exclude these two areas from the understanding used for the present study does not suggest that the excluded operations are irrelevant for safeguarding essential security interests now or in the future.⁹ The choice exclusively seeks to focus the analysis of this report on a group of policies that are currently of interest to many governments.

39. As a result of these considerations, this report adopts a broad conception of acquisition- and ownership related policies to manage risks to essential security interests. It encompasses all policies

- whose primary *purpose* is to address risks to essential security interests, and

⁷ Analysis and country examples of public-interest tests in competition reviews is available at <http://www.oecd.org/daf/competition/public-interest-considerations-in-merger-control.htm>, and in particular in Despina PACHNOU (2016), “*Public interest considerations in merger control – Background Paper by the Secretariat*”, OECD, [DAF/COMP/WP3\(2016\)3](#).

⁸ Examples include the establishment of a media enterprise, the construction of a nuclear power plant, or the operation of a mine.

⁹ The framing used here does not correspond entirely to the categories established for the purpose of notifications recorded in the [List of Measures Reported for Transparency](#) under the National Treatment instrument.

- where the risk and risk-management are associated with the *acquisition or ownership of an asset*, but
- excludes transactions where a government entity is itself involved in the transaction as the seller or where the ownership is very tightly related to the operation of the asset which requires a licence or concession.¹⁰

40. A review of policies that meet these criteria of acquisition- and ownership-related policies to manage essential security risks reveal at least three groups of such policies:

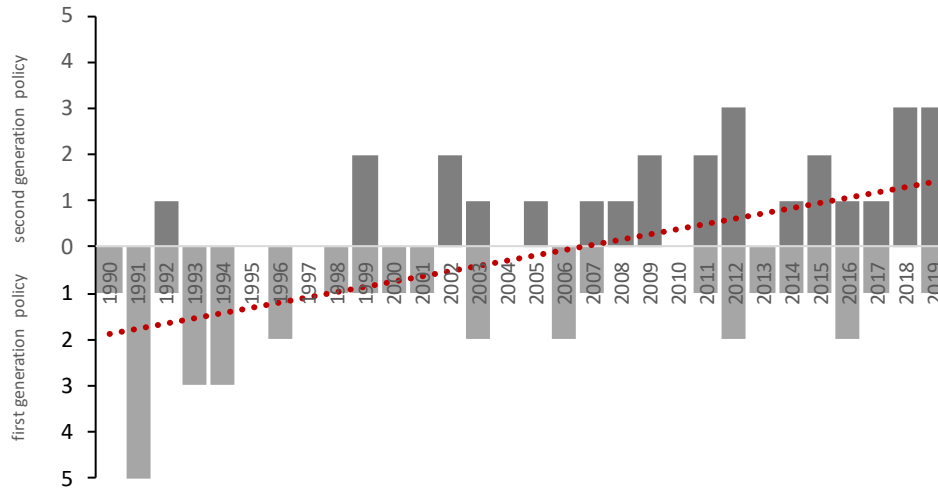
- Almost all countries in the sample are found to have one or more policies that impose ownership caps; require a government authorisation prior to an acquisition of specific assets or assets in a specified sector; or establish government-held *golden shares* in individual companies. In some countries, constitutional laws allow restrictions on certain transactions in principle while no lower-ranking law establishes actual rules on how this authority is to be exercised. Where such rules exist, they are relatively rudimentary, mechanical or contain little guidance to the applying authorities. Many of these policies are rarely activated, if at all. For convenience, this report refers to these policies as *first generation* policies.
- *Second generation* policies, as this report will call them, cover a broader range of sectors or apply across all industry sectors by using abstract concepts such as “national security” or the like to set out their scope of application. Their design is much more elaborate, at times composed by multiple legal documents and set out in dozens if not hundreds of pages of legislation, regulations and rules.
- A third group of policies is just emerging with just a few examples in the sample so far. These policies do not develop further on acquisition-related policies that dominate until now but establish control over owned assets post establishment, or control the outflow of certain assets from the jurisdiction that is implementing the policy.

41. The classification of policies into first- and second-generation policies does not imply any judgement on the merits of their use or design. Also, the designation does not suggest that they are necessarily old, as some countries are designing such policies at present. At times, that qualification of a policy as first or second generation policies may not be obvious, and as policies evolve over time, reforms may change defining elements to the point where individual policies change the features that suggest their classification. Also, many countries operate first and second generation policies in parallel, and sometimes they share some procedural features.

42. In the sample of 62 jurisdictions, 87 distinct acquisition- and ownership related policies to manage risks to essential security interest have so far been identified, with at most four distinct policies in a single jurisdiction; the final tally may still be higher. When these policies are classified as first or second generation, the evolution over time shows a clear trend towards preponderance of second generation policies since the mid-00s; second-generation policies were rare at the beginning of the 1990s. New first-generation policies still come into effect, but are less frequently used in more recent years (Figure 0.1).

¹⁰ An example are mining concessions, rules on cabotage by foreign-owned operators, and licenses to operate or build nuclear-power stations or railway infrastructure.

Figure 0.1. Introduction of first- and second-generation policies over time – number of new policies per year and trend in the repartition among types



Note: The linear trendline indicates repartition of 1st and 2nd generation policies among new policies introduced between 1990 and 2019 (excluding projections of new policies expected to come into effect in 2019).

Source: OECD.

2 Whether and which policies to manage risks associated with acquisition or ownership are warranted remains controversial

43. While most countries have had broader policies to manage risks associated with acquisition or ownership of certain assets for many decades and continue to experience vigorous debates about their scope and design, some advanced and emerging economies covered by this report did not have broader acquisition- or ownership-related policies that go beyond narrow sector-specific ownership caps or rare authorisation requirements in early 2019.

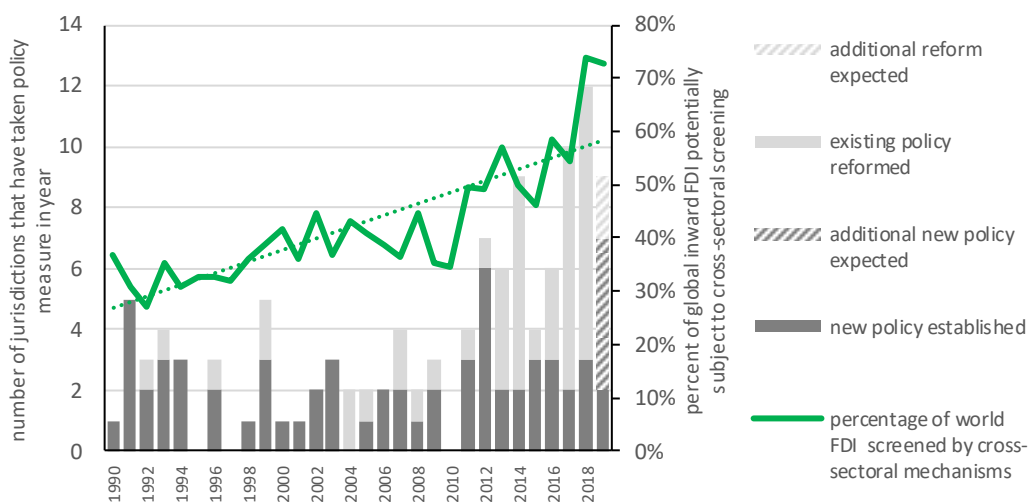
44. Among the 62 jurisdictions covered by this report, 87% had at least some policy to manage acquisition- or ownership-related risk to essential security interests in place at the beginning of 2019. Only 10% of jurisdictions however had established a 2nd generation-policy at that time, while the remainder of the jurisdictions in the sample were content with authorisation requirements, ownership caps or “golden share” arrangements in a limited number of sectors.

45. As a result of this policymaking, over 70% of global FDI in 2018 flew into countries that apply cross-sectoral review processes – almost twice the share of global FDI inflows that prevailed for most of the 1990.¹¹ Projections for 2019 point towards a possible uptick in the number of countries that introduce 2nd generation policies for the first time, especially as a

¹¹ The share of total flows that are subject to acquisition- and ownership-related policies to safeguard essential security risks cannot be determined given the absence of sufficiently fine-grained data on individual sectors.

number of countries in Europe are considering or have just introduced new policies in this area.¹² The number of countries that were introducing such policies for the first time remained small until around mid-2018, and most policy activity was concentrated in a few countries that already had comprehensive policies (Figure 0.2).

Figure 0.2 Evolution of acquisition-related policies to manage essential security interest since 1990



Note: Based on the currently 62 economies that are invited to OECD-hosted dialogue on international investment policies.

Source: OECD. Some data for 2018 and 2019 are based on estimates and projections.

46. Despite the swift increase in the number of countries that establish second generation policies to manage risk to their essential security interests, there are strong regional differences. This observation suggests some degree of polarisation between countries that seek to address risks stemming from acquisition or ownership of certain assets through dedicated and ever more refined policies on one end of the spectrum and countries that do not consider such policies appropriate or needed on the other end and that continue to rely at most on narrow, first-generation policies.

47. Other than regional particularities, there is no obvious explanation for these observations. Neither size of the economy, level of development, ratio of FDI to GDP, FDI in total foreign assets, or imitation effects offer a stringent explanation for why countries make such different assessments of whether acquisition- or ownership-related policies are warranted to manage essential security risks.

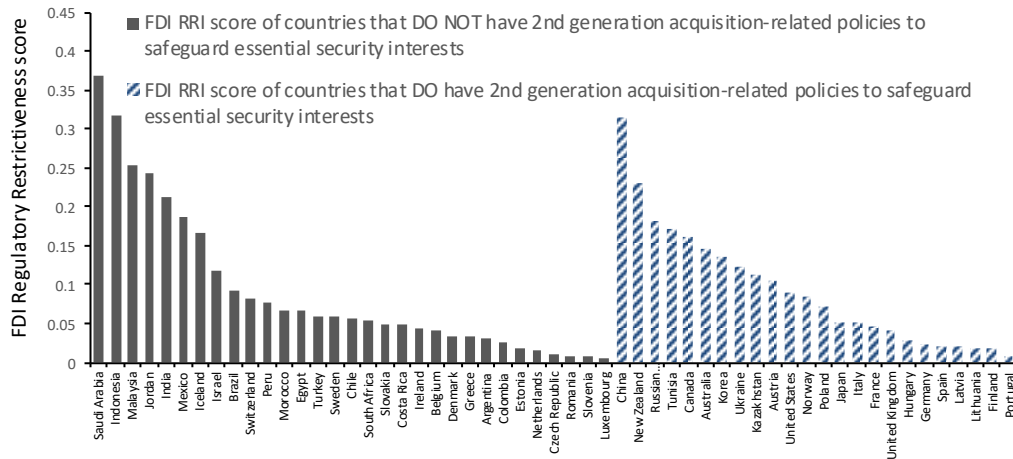
48. There is also no discernible correlation between the degree of openness to FDI and the presence of a mechanism to manage acquisition- or ownership-related risk: Open economies do not seem to perceive a greater need for a mechanism of last-resort to protect their essential security interests. Figure 0.3 shows the restrictiveness to FDI – as measured by the OECD’s FDI Regulatory Restrictiveness Index¹³ – for the 55 economies covered by this report for which the

¹² New policies came into effect on 1 January 2019 in Hungary (see Hungary’s notification in [DAF/INV/RD\(2019\)2](#)) and Norway.

¹³ Information about the FDI-RRI, its methodology and scores for individual countries and sectors is available at www.oecd.org/investment/fdiindex.htm. Mechanism that are operated to safeguard essential security interests are not considered for the purpose of calculating the FDI RRI.

FDI RRI has been assessed and whether or not the country operates a second-generation mechanisms to manage risk associated with acquisition or ownership of certain assets.¹⁴

Figure 0.3. Regulatory Restrictiveness for FDI and presence of a second generation acquisition-related policies to safeguard essential security interests



Note: No FDI RRI scores are yet available for Bulgaria, Paraguay, Singapore, Thailand and the European Union.
Source: OECD.

49. Two factors – idiosyncrasy and the desire to signal openness in particular economic situations – can likely contribute to explaining some countries’ policy choices. Some countries have introduced policies in the context of identified trigger-events;¹⁵ others introduced such policies when they had to abolish traditional mechanisms such as golden-share arrangements that may fulfil similar functions;¹⁶ and still others are likely to have been motivated by a specific geographical, demographic or political exposure. Fiscal stress or the desire to signal openness to foreign capital is held to motivate reticence to the introduction of such policies in some countries.

3 Policies continue to show little convergence towards common criteria and procedural designs

50. Among the many countries that have established dedicated policies to manage security risks resulting from acquisitions and ownership of specific assets, there is little homogeneity or

¹⁴ Jurisdictions for which no FDI-RRI score is currently available but that are covered by the present report are: Bulgaria, Paraguay, Singapore, Thailand, and the European Union. Policies that consist of narrow sectoral equity caps are omitted from the assessment.

¹⁵ A smaller European country may serve as example where the government sought to halt the takeover of an enterprise by an organised-crime related entity but found to have no legal means to do so. A different country, the Netherlands, were considering, in 2018, a policy related to the telecommunications sector after a takeover bid for Dutch company *KPN* by a Mexican enterprise.

¹⁶ Italy for instance introduced policies in 2012 after the Court of Justice of the European Union had found Italy’s “golden shares” arrangements in certain companies to be in contravention to European Union law ([CJEU judgement of 26 March 2009, Case C-326/07, Commission v. Italy](#)).

convergence in approaches and designs. This diversity is observed notably in criteria laid down for risk profiling of transactions, detail and coverage of rules that establish the mechanisms, design of procedures, and resources allocated to policy implementation, among others. Outcomes, to the extent they can be assessed and compared, also vary widely.

51. A particularly wide spectrum is observed with respect to risk identification. Some countries are content with narrow, asset- or sector-specific restrictions, while others have designed multiple and often broad cross-sectoral review mechanisms. The criteria that the legislators have laid down in individual countries shows different perceptions on where and under which conditions risk is concentrated. Each country currently combines a different set of risk-enhancing factors from a total pool of 16 parameters; almost a dozen individual sectors have been identified collectively as areas of risk, but each country has chosen a different subset of these sectors.

52. The level of regulatory detail also varies widely. While the volume of text is not a solid proxy of regulatory detail, it is notable that some countries' mechanisms are laid out in rare brevity – a single article in a law in one case –, while other countries need over a hundred pages to lay down, conditions, procedures, responsibilities, sanctions, scope for mitigation measures, costs and fees, transparency and reporting requirements and so forth.

53. Strong variance is also observed with regard to the resources that different countries dedicate to the implementation of their acquisition- and ownership-related policies: Some countries require almost no resources to administer the policy, especially where self-executing equity caps for foreign investments are used or where narrow, sector specific authorisation requirements are rarely triggered. On the other end of the spectrum, some countries have heavily resourced institutional arrangements that involve the intelligence community, rely on international cooperation, and have multi-million USD annual budgets. To the extent that budgets, even when adjusted for the size of the corresponding economy, are an indicator or proxy for procedural efforts, they indicate the broad variance of implementation efforts for governments and entities to which the policies apply.

54. The differences indicated by the budget allocations are by and large confirmed by the caseload per country. Among the countries for which the number of cases that were subject to a review are known, there is broad spectrum: some countries review hundreds of transactions per year, while others have never used their review mechanisms, as few or no transactions have ever met their trigger conditions for the rules to apply.

55. This diversity in policy design is somewhat surprising given that investment policies related to national security have enjoyed recognition for decades in international law¹⁷ and policy practice, ample opportunities for multilateral exchange on the subject,¹⁸ availability of information,¹⁹ and the young age and rather frequent reform of policies in several countries.

¹⁷ The [OECD Codes of Liberalisation](#), adopted in 1961, contain a self-judging exception for national security in relation to cross-border capital flows in their Articles 3. Many investment treaties likewise contain such carve-outs.

¹⁸ The OECD launched its [Freedom of Investment Roundtables](#), initially exclusively dedicated to this policy area, in June 2006.

¹⁹ Notifications of new policies are discussed at the Freedom of Investment Roundtables – and [publicly available in reports on the discussions at the Roundtables](#), are available on a [dedicated website](#), and are set out in the [List of Measures Reported for Transparency](#) under the National Treatment instrument.

56. The diversity in approaches has an important upside for policy design: it offers an opportunity to compare, assess or estimate their likely effectiveness as well as side-effects and cost, and allows countries that wish to introduce new policies or reform existing ones to learn from a great wealth of experience.

4 Perceptions evolve further of which assets are sensitive and how threats may materialise

57. Perceptions of which assets are sensitive for essential security interest evolve over time and depend on the specific situations of individual countries. Despite individual differences, some common trends and appreciations can be observed in specific periods of time. Similarly, the mechanisms through which threats are transmitted or amplified evolve over time.

Changes in the perceptions of sensitive assets

58. Initially, countries were mainly concerned about foreign ownership of defense manufacturing and occasionally sensitive areas of land, e.g. in border areas. A few decades ago, critical infrastructure – electricity generation and distribution, railroads or water supply, for instance – joined the list of sensitive assets in many advanced economies, once the companies operating these assets had been privatised and hence become available to investors. Risk perceptions evolved further, even those expanded categories of assets were considered obsolete and sector-specific lists that enumerated individual asset categories gradually gave way more recently to cross-sectoral review mechanism of enterprises in any sector.

59. New trends continue to emerge again now. Several countries' policy changes emphasise the sensitivity of two groups of assets that hitherto had not been captured specifically or at least not been included explicitly in the scope of acquisition- or ownership-related policies even though they may have been captured by cross-sectoral mechanisms:

- Advanced, dual use and network technology;²⁰ and
- Personal data and enterprises that control such data.²¹

The explicit reference to some of these groups of assets was foreshadowed by implementation practice in some countries, where they were often at least implicitly covered by cross-sectoral

²⁰ These areas are explicitly singled out in countries including (year indicates first explicit coverage): Germany (2017), France (2018), Italy (2018), United Kingdom – in a proposal for a future policy, “[National Security and Investment – Draft Statutory Statement of Policy Intent](#)” of July 2018), the United States (2018), and the European Union (2019), [Framework for screening of foreign direct investments into the European Union](#).

²¹ These areas are explicitly singled out in countries including (year indicates first explicit coverage): Germany (2017), France (2018), the United Kingdom (2018), the United States (2018), and the European Union (2018). In Australia, these types of assets have likewise been identified explicitly in a [speech delivered on 14 August 2018](#) by the Chair of the Australian Foreign Investment Review Board (FIRB); given the design of the Australian review mechanism under FIRB, no explicit reforms of legislation or rules is required to implement such an adjustment.

review mechanisms. Their inclusion in legislation has either served as a further clarification,²² added them in sector-lists as new items,²³ or modulated policy.²⁴ Unlike the more traditional national-security relevant assets, which are associated with large, often listed companies, companies that produce advanced technology may be small,²⁵ non-listed, sometimes young and little known, and produce items whose national security relevance appeared less obvious until recently.

60. A further notable change is the coverage of certain real estate assets in a greater number of jurisdictions. Real estate in border areas has been a traditional item in some countries' acquisition- and ownership-related policies related to the protection of essential security interests and is found in sector-lists in these countries. Now, some countries include real estate that is located near certain facilities, beyond border areas.²⁶

61. The inclusion of certain asset categories in individual countries' policies is somewhat asynchronous, and countries' policies appear rooted in different decades in how they frame what bears risk – an observation that is reminiscent of the broader disagreement on whether specific policies are needed to manage security risks associated with acquisitions or ownership of certain assets at all.

62. A further example of such asynchronous policy-changes are recent policies that itemise assets for the application of the review mechanisms. Such policies have been introduced in Poland in 2015²⁷ and Lithuania in 2017²⁸, and, albeit in a different setting, in Australia in 2018.²⁹ These approaches stand in some contrast to many countries' cross-sectoral approaches that use high levels of abstraction to define the scope of the policies' application.

²² Germany's reform in 2017 ([Neunte Verordnung zur Änderung der Außenwirtschaftsverordnung](#)) contained – in regard to sectors – a mere clarification rather than a broadening of the cross-sectoral review mechanism.

²³ Italy made this modification through Article 14 of the [Decree-law 16 October 2017, n.148](#), as confirmed, without modification, by the [law of 4 December 2017](#), notified to the OECD as [DAF/INV/RD\(2018\)5](#).

²⁴ The 2018 reform in the United States ([FIRRMA, Section 1703](#)) introduces specific rules for investments that is related to “critical technologies” or “maintains or collects sensitive personal data of United States citizens”.

²⁵ The acquisition of assets by *Huawei of 3Leaf Systems* in 2010 and divested in 2011, was valued at USD 2 million. Japan included SMEs and non-listed entities into the assets whose acquisition by foreigners may be assessed for essential security risks in 2017.

²⁶ The United States have explicitly included certain purchases or leases of real estate in close proximity to military installations or certain other government property in the scope of the CFIUS review in 2018 ([FIRRMA, Section 1703](#)). Finland had a bill ([Bill HE 253/2018](#)) in parliament in early 2019 that seeks to introduce measures in relation to the acquisition of real estate by foreigners.

²⁷ *Act of 24th July 2015 on Control of Certain Investments*, notified to the OECD as [DAF/INV/RD\(2016\)1](#).

²⁸ *Law on the Protection of Objects of Importance to Ensuring National Security of the Republic of Lithuania*, notified to the OECD as [DAF/INV/RD\(2018\)4](#).

²⁹ The Australian policy, described in greater detail in [DAF/INV/RD\(2018\)6](#), covers ownership of sensitive assets, rather than acquisitions; an acquisition-focused policy with a more abstract description of its scope operates in parallel.

Additional transmission channels for threats emerge

63. Just as perceptions evolve over which assets are sensitive for essential security interests, so do views change over the transmission channels of these risks. As in this policy area more generally, concerns did and do not develop contemporaneously across countries; some countries had certain concerns earlier before others began to share them.

64. The evolving sector coverage of policies offers a retrospective approximation of how threat scenarios were perceived in time: Traditional concerns focused primarily on *sabotage* and *espionage* – especially when defense assets and strategically located real estate were the main assets of concern. Later, with the possibility for foreigners to acquire critical infrastructure assets, the possibility that infrastructure’s availability could be *disrupted* or *withheld* became apparent as a further risk. As the set of assets that are considered sensitive continues to evolve to now include sensitive knowledge and personal data, some countries consider *leakage* of information, know-how, or sensitive personal data or the *malicious manipulation and alteration* as additional sources of risk to their essential security interests.

65. Finally, as monopoly positions for certain critical technologies (e.g. software or certain hardware components) or raw materials such as rare earths emerge or become more important or apparent, *dependencies on sole suppliers* receive greater attention as a further transmission channel of risk to essential security interests.³⁰ Mergers and acquisitions may consolidate or further expand such sole-supplier positions and may trigger policies with a view to avoid such developments. In some countries, concerns about sole suppliers and monopoly positions have existed for some time but were mainly based on undesirable dependence on foreign products or services, loss of “national champions” and pioneering industries and associated economic opportunities; additional implications for essentially security are only now becoming more prominent in many countries.

5 Four traditional features fade

66. Until recently, acquisition- and ownership-related policies to protect essential security interests almost universally featured four defining characteristics: policies were activated by an *acquisition*; they concerned acquisitions by *foreigners*; applied predominantly to the acquisition of *controlling stakes*; and only related to *inward* investment. These features circumscribed the core of concerns and implied assumptions on the sources of risks. Recent policy changes suggest that all four traditionally defining features begin to fade.

³⁰ Theodore MORAN (2013), “[FDI and national security: Separating legitimate threats from implausible apprehensions](#)”, In: *Foreign Direct Investment in the United States: Benefits, Suspensions, and Risks with Special Attention to FDI from China*, Peterson Institute for International Economics, p.56 points out that the United States government was concerned as early as 1988 that the United States’ access to supply of semiconductors might be brindled if foreigners – a Japanese company in this case – would acquire an individual supplier. Very similar concerns are voiced three decades later in U.S. Department of Defense (2018), “[Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States](#)”. The Netherlands’ National Coordinator for Anti-terrorism and Security also cites concerns over single-supplier risk in 2018 (“[Nationale veiligheid bij overnames en investeringen of inkoop en aanbesteding](#)”).

Acquisition and ownership

67. For decades, policy instruments to manage risks associated with ownership of specific assets were almost exclusively limited to acquisition-control. Acquisition-triggered policies are based on the assumption that a change of ownership of an asset can entail a change of associated security risk. Other types of changes that may impact the security relevance of ownership of assets are not addressed by these policies – intentionally or unintentionally. Risks developing from greenfield investment, even in enterprises in sensitive sectors; changing business orientation of an acquired enterprise; or changing security relevance of an asset, for instance an acquired company or its products, did not typically trigger policies.³¹

68. Other traditional instruments – sectoral ownership caps, regulatory oversight and expropriation – may not always offer satisfying solutions: Ownership caps are fairly inflexible, regulatory oversight does not always capture ownership-related risk, and the right to expropriate property in the public interest offers little flexibility, is potentially costly if investment treaty protections apply, and leaves the government with an asset that it may not have any interest to own.

69. Amidst the heightened awareness of risk in some jurisdictions and a legacy of past practice and resulting ownership positions that now raise concern, some countries have begun to diversify their risk-management instruments and put in place dedicated, more detailed and more flexible policies. Australia for example has established new policies that address such risks stemming from ownership of telecoms and other critical infrastructure assets, outside the context of an acquisition, making it one of the first countries to explicitly put in place developed policies to manage ownership-related security risks for specific assets post-establishment.³²

71. The availability of such mechanisms may have repercussions on the use of acquisition-related policies at entry. Policies that operate post-establishment may for instance substitute the application of acquisition-triggered policies and reduce the frequency of denials and mitigations under these policies. The availability of means to intervene if and when a risk emerges from a specific ownership position may give governments comfort to allow acquisitions that they would otherwise have prohibited for fear that the ownership could become problematic later. Rather than an accumulation, the existence of risk management tools post-establishment could appear as complementary which ultimately leads to fewer or lesser restrictions on acquisitions.

Foreign and domestic acquirers

72. Until recently, most acquisition- and ownership-related policies only applied to acquisitions by foreigners – implicitly suggesting that foreigners presented a greater security risk than nationals.³³ As the relevance of nationality tends to fade with greater individual

³¹ See Frédéric WEHRLÉ/Joachim POHL (2016), “[Investment Policies Related to National Security: A Survey of Country Practices](#)”, *OECD Working Papers on International Investment*, No. 2016/02. On 1 January 2019, Hungary has brought into force legislation that covers greenfield investment alongside acquisitions of existing enterprises (see Hungary’s notification to the OECD in [DAF/INV/RD\(2019\)2](#)).

³² The policies are established by the [Security of Critical Infrastructure Act 2018](#), in force since 11 July 2018, and the [Telecommunications and Other Legislation Amendment Act 2017](#), which is in force since 18 September 2018. Other countries may have similar regulatory elements at hand, but are not known to have embedded them in a context of responses to essential security interests.

³³ A policy proposal in the United Kingdom, “[National Security and Investment – Draft Statutory Statement of Policy Intent](#)” of July 2018 items 4.20-4.21 explicitly states that the U.K. “Government

mobility and easier and more widely available acquisition of additional nationalities by natural persons,³⁴ and as nationality of legal persons for this purpose had limited plausibility for long, some countries have done away with the focus on foreigners and concentrate instead on the nature of the concerned assets. Such policy design is now observed for parts of the policies of Australia, Lithuania, Norway and Poland.

Controlling stakes vs any interest

73. The third feature that characterises many traditional policies to manage risks for essential security interests is their application to controlling stakes, especially of listed, hence typically large enterprises – a plausible approach at a time when espionage and sabotage dominated the risk scenarios. This limitation also reduced the number of reviewable transactions, and reporting requirements under securities legislation made detection of reviewable transactions easy.

74. Now, as countries perceive that protecting their essential security interests may require withholding access to sensitive data or technology, countries like the United Kingdom³⁵ or Germany³⁶ have lowered the trigger thresholds or have introduced alternative criteria for certain transactions that do not meet the ordinary trigger conditions, such as the United States;³⁷ all three countries introduced the changes in the course of 2018. In a similar vein, Japan has brought unlisted companies under the scope of their acquisition-related policies.³⁸

Inward investment vs any trans-border asset transfer

75. Almost all traditional acquisition-based policies apply to transactions that are associated with the *territory* of the country applying the policy. They are triggered by the acquisition of an enterprise or asset that is *located* in the country that implements the policy, regardless of the ownership of that asset. As further testimony of the territorial focus of traditional acquisition- and ownership-related policies, they are not normally triggered by

considers that foreign nationality could prove to be a national security risk factor” and that foreign national “therefore are comparatively more likely to pose a risk than UK-based or British acquirers.”

³⁴ For an overview of available schemes see XIN Xu/Ahmed EL-ASHRAM /Judith GOLD, (2015) “Too Much of a Good Thing? Prudent Management of Inflows under Economic Citizenship Programs”, IMF Working Paper 15/93.

³⁵ See the United Kingdom’s notification of the policy change in 2018 in [DAF/INV/RD\(2018\)7](#).

³⁶ [Zwölfte Verordnung zur Änderung der Außenwirtschaftsverordnung](#), 19 December 2018.

³⁷ “Determination and Temporary Provisions Pertaining to a Pilot Program To Review Certain Transactions Involving Foreign Persons and Critical Technologies”, Department of the Treasury, Office of Investment Security, 31 CFR Part 801, FDR Vol 83, No 197, 11 October 2018, in particular § 801.302.

³⁸ A rationale for these changes at least for the United States is postulated by Michael BROWN/Pavneet SINGH (2017), “China’s Technology Transfer Strategy: How Chinese Investment in Emerging Technology Enable a Strategic Competitor to Access the Crown Jewels of U.S. Innovation”, Defense Innovation Unit Experimental.

transactions concerning assets owned or controlled by their nationals if these assets are located abroad.³⁹

76. Given their territorial focus, policies do also not normally cover the creation of new enterprises through joint ventures, the divestment of parts of an enterprise, or the sale of certain assets: none of these transaction-types grant control, influence or participation in the parent enterprise to the joint venture partner or acquirer of the divested asset.

77. The shift of concern over threats to essential security interest has focused some countries' attention on the implications of these types of transactions, given that joint ventures or acquisitions of assets or technology may offer an avenue through which other parties may gain access to certain information, know-how or sensitive technology in a similar way as an acquisition of an enterprise located in their territory would.⁴⁰

78. To address such situations, some countries have begun introducing or trialling policies that subject some of these transaction-types to reviews to safeguard their essential security interest. China has established, in early 2018, a policy trial that seeks to address the concerns that international transactions lead to an undesirable transfer of intellectual property that may threaten the country's essential security interests.⁴¹ In the United States, a reform in mid-2018 has included joint ventures in the scope of transactions that may confer "control of a US business";⁴² the same legislation has authorised strengthened export controls to address the sale or transfer of certain emerging and foundational technologies.⁴³

79. Both policy initiatives document sensitivities over transactions that involve the transfer of technology or intellectual property but are not captured by traditional investment reviews.

³⁹ Legal doctrine distinguishes extraterritorial *application* and extraterritorial *effect*. Where it is at times claimed that acquisition- and ownership-related policies are applied in an "extraterritorial" manner, the cases mentioned in support of the claim typically refer to elements of extraterritorial *effect*.

⁴⁰ United States legislation passed in 2018 explicitly recognise this link as it states in Section 1752 (10) of [NDAA 2018](#) that "Export controls complement and are a critical element of the national security policies underlying the laws and regulations governing foreign direct investment in the United States, including controlling the transfer of critical technologies to certain foreign persons."

⁴¹ [State Council Measures for the Overseas Transfers of Intellectual Property Rights \(trial\)](#), State Council release No.19 (2018) of 18 March 2018 and in effect since 29 March 2018. The *Measures* set out review procedures for the transfer of intellectual property from China abroad for implications for national security and China's innovation and development capabilities.

⁴² [Section 1703 of FIRRMA](#), amending Section 721(a) of the Defense Production Act of 1950 (50 U.S.C. 4565(a)), includes among the "covered transactions" any "merger, acquisition, or takeover that is proposed or pending after August 23, 1988, by or with any foreign person that could result in foreign control of any United States business, including such a *merger, acquisition, or takeover carried out through a joint venture*" (emphasis *not* in the original).

⁴³ In the United States, the Export Control Reform Act (2018), which was passed in the [same package](#) as the FIRRMA and is laid down in Sections 1741 and following of the [NDAA 2018](#), authorizes the U.S. Commerce Department's Bureau of Industry and Security to identify "emerging" and "foundational" technologies that are essential to U.S. national security and warrant control under export control mechanisms (Section 1758 of [NDAA 2018](#)).

6 Risks to essential security interest originating in non-ownership transactions come to the fore

80. Traditional investment policies related to national security address risks that stem from acquisition or ownership of certain assets. Certain non-ownership transactions may however lead to similar vulnerabilities and risks for essential security interests, and have hence drawn attention in three contexts recently:

- Lease of infrastructure used for sensitive government operations to or from certain owners or procurement of goods or services by governments such as refurbishment of critical infrastructure assets;
- Use of telecom, video-surveillance and similar equipment from certain suppliers in privately- or publicly-owned sensitive infrastructure; and
- Joint research activities and inward and outward exchange of research personnel.

Leases, concessions and public procurement

81. Implications for leases of infrastructure to and from foreigners have recently attracted public attention in Australia and the United States in particular, as they grant access to sensitive assets or data associated with such assets in a similar way as an acquisition would. The constellations were different in the two countries: In Australia, a foreigner leases an asset for 99 years;⁴⁴ in the United States, the government was leasing assets from foreigners in one case and from a specific owner in a particular case.⁴⁵ While the transactions appear reversed, the risks that they potentially imply are similar: each may grant access to sensitive information about security-related operations and could enable the government's business partner to disrupt or withhold functions of the asset – concerns that are very similar to those that acquisition- and ownership-centred policies seek to address.

82. Similar concerns may arise in the context of government procurement more generally, especially with regards to building or refurbishing sensitive publicly-owned infrastructure assets or procurement in sensitive sectors such as defence.⁴⁶ Recently, concerns have been expressed about foreign ownership of election infrastructure and data services companies.⁴⁷ Non-

⁴⁴ The lease of the Australian port of Darwin for a 99-year term contributed to policy changes in Australia, including the establishment of a [Critical Infrastructure Centre](#) and, among others. The United States have now, through [NDAA \(2018\)](#) Section 1703, identified the lease of an asset to a foreigner as a “covered transaction”.

⁴⁵ In January 2017, the United States Government Accountability Office (GAO) recommended that the United States Federal Government “determine whether the beneficial owner of high-security leased space is a foreign entity and, if so, share that information with the tenant agencies for any needed security mitigation.” GAO (2017), “[Federal Real Property – GSA Should Inform Tenant Agencies when Leasing High-Security Space from Foreign Owners](#)”, January 2017.

⁴⁶ The Dutch Minister of Justice and Security [reportedly](#) noted, in a letter to the Parliament dated 22 May 2018, national security risks in tendering and hiring in sensitive sectors.

⁴⁷ In mid-2018, [it became known](#) that the company that handles Maryland's voter registration database and candidate management operations, *ByteGrid LLC*, had been acquired by a company owned by a wealthy Russian individual, prompting calls for a review of foreign ownership of United States election infrastructure and the [introduction of a bill for a “Protect Election Systems from Foreign Control Act” in the U.S Congress on 19 July 2018.](#)

discriminatory procurement rules for such contracts in many countries typically enable foreign or foreign-controlled firms to bid for such contracts; here, the knowledge of the assets' design, weaknesses, and the risk of sabotage, espionage or manipulation may raise issues that are again similar to those of ownership. To be sure, domestic malicious actors could likewise pose similar risks.

83. In most countries, management of such risks is carried out under different rules that those used for acquisitions, if at all. In some cases, acquisition-based policies have allowed to anticipate the risk of later bids for contracts regarding sensitive assets.⁴⁸ In other cases, property transfer to foreigners may be allowed, but the acquired company is subsequently excluded from providing sensitive services; this approach moves the risk-mitigation behind the border.⁴⁹ Policies also exist in some countries that regulate, still closer to actual operations, access privileges to manage risks of suppliers and account of, among others, foreign ownership for the attribution of access.⁵⁰ One country is known to have institutionalised collaborative oversight over a telecom equipment manufacturer to manage risks associated with the use of its products.⁵¹

84. Most recently, first signs emerge in legislation of a more holistic approach to manage security risk stemming from a broader set of interactions between governments and businesses to identify potentially malicious actors; such policies may or may not include acquisition control as a component. Australia for instance has complemented its acquisition-based review mechanisms with rules that grant the government certain powers in relation to owners of specific sensitive assets. Norway has brought a comprehensive security into force in January 2019 that covers acquisition control, procurement, and many related areas in a comprehensive law.⁵² The Netherlands have adopted a comprehensive “economic security programme” that mentions acquisition-related risk does not contain a broader ownership or acquisition control component beyond planned legislation relating to the telecoms sector.⁵³

⁴⁸ Canada [prohibited, on 23 May 2018](#), the acquisition of construction company *Aecon Group Inc.* by a foreign company; *Aecon* refurbishes, among others, nuclear power plants, builds airports and other major infrastructure for private or public entities in Canada; the [public discourse](#) and potentially Canadian government's risk assessment have taken current and future contracts on sensitive assets into consideration.

⁴⁹ The Australian Defence Department announced in June 2017 that it would terminate its relationship with a data company, *Global Switch*, after a foreign company had acquired a large minority holding of *Global Switch's* parent.

⁵⁰ In the United States, for instance, security clearances for companies are granted under the rules of the *National Industrial Security Program* under the rules set out in the [National Industrial Security Program Operating Manual](#). The rules may prevent a company under foreign control to obtain certain clearances even though permission has been granted to a foreigner to acquire the company.

⁵¹ In the United Kingdom, a *Huawei Cyber Security Evaluation Centre* has been established in November 2010 mitigate any perceived risks arising from the involvement of *Huawei* in parts of the United Kingdom's critical national infrastructure. See for more details the [Fourth annual report for the National Security Adviser from the Huawei Cyber Security Evaluation Centre Oversight Board](#) (2018).

⁵² Norway has included provisions on the handling of security-rated procurement in its [Security Law](#) (2019), Chapter 9.

⁵³ The Dutch *National coordinator of Terrorism prevention and Security*, attached to the Ministry of Justice and Security, explicitly identifies take-overs of enterprises and public procurement as the two areas of risk for its economic security programme, “[Nationale veiligheid bij overnames en investeringen of inkoop en aanbesteding](#)”, June 2018.

Use of equipment in privately- or publicly owned sensitive infrastructure assets and supply chains

85. The use of certain products or services for sensitive operations or infrastructure – be they privately or publicly owned or operated – has recently emerged as a further concern with implications similar to those of foreign ownership.

86. A particularly visible example in this area are components of telecommunications network equipment, amid concerns that such equipment may give the manufacturer or other malicious actors access to sensitive information circulating in the network built from such components. In several countries, governments have prohibited, warned against or withdrawn financial support for the use of products of certain manufacturers in 5G mobile telecommunications networks for instance, even when these networks are privately owned.⁵⁴ Other products, including consumer products that are widely used, such as mobile phones, video-surveillance equipment and small camera-equipped unmanned aerial vehicles (UAVs, “drones”) have raised concerns recently for similar reasons, as they may also transmit or provide access to sensitive information to actors without the user’s knowledge or explicit consent.⁵⁵

87. While equipment for telecommunications network are a prominent example of risks involving products and services, they are not the only one. In Australia for example, outsourcing or maintenance by water or power companies has reportedly exposed vulnerabilities to espionage and sabotage.⁵⁶

⁵⁴ Australia’s [Telecommunications and Other Legislation Amendment Act 2017](#) for instance requires telecom service providers to notify even relatively minor changes to its supply chain, as indicated in [notes on notification examples](#); the Australian Government has also pointed out that telecom [carriers may not be able to fully manage risk when using equipment from vendors who are likely to be subject to extrajudicial directions from a foreign government](#). Some countries have expressed outright bans on or expressed advice against certain suppliers for some network components, including New Zealand (where [on 28 November 2018 the Government Communications Security Bureau has prohibited a telecom provider to choose equipment from a specific maker for the 5G network](#)), the United Kingdom (whose National Cyber Security Centre has [issued advice](#) in April 2016 to a limited number of United Kingdom telecommunications operators regarding the potential use of *ZTE* equipment and services in April 2016, stating that the “national security risks arising from the use of *ZTE* equipment or services within the context of the existing UK telecommunications infrastructure cannot be mitigated.”), and the United States (where [NDAA \(2018\)](#), Section 889 prohibits executive-branch agencies from procuring or contracting for certain telecommunications equipment or services from certain companies – and where the [Federal Communications Commission \(FCC\) has proposed in April 2018](#) that Universal Service Fund resources be not used for the purchase of equipment or services that may undermine United States national security. Arrangements in the United Kingdom have led to the establishment, in November 2010, of the *Huawei Cyber Security Evaluation Centre* to mitigate perceived risks arising from the use of the company’s equipment in the United Kingdom’s critical national infrastructure, as set out in the Centre’s [annual report 2018](#).

⁵⁵ Recent examples include the concerns over the [alleged use](#) of surveillance cameras produced by *Hikvision* in a military facility in Australia. The United States has, in 2018, banned by law ([NDAA 2018](#), Section 889) the government procurement of equipment or services offered by four individually named companies, *Hytera Communications Corporation*, *Hangzhou Hikvision Digital Technology Company*, and *Dahua Technology Company*.

⁵⁶ The Head of Australia’s Critical Infrastructure Centre was [quoted in September 2017](#) with statements made at the Australia National Security Summit 2017.

International research cooperation and global allocation of venture and human capital

88. In a few jurisdictions, foreign funding of research or joint research activity have recently raised concerns. On their face, these forms of collaboration across borders are fairly far removed from acquisitions of existing enterprises, but there are concerns that such collaboration could be a substitute to acquisitions in some sectors, especially advanced technology and other cutting-edge, research-intensive domains: Joint research work in universities or research institutions, financed by foreign governments or foreign enterprises, allows these funders to tap into knowledge, know-how and networks to acquire capabilities that are not available domestically. While exchange of information across borders and mutual learning are among the very objective of international research cooperation, it may in certain areas run counter some countries' endeavours to withhold certain capabilities from countries they believe may potentially threaten their security interest.⁵⁷ From some perspectives, the difference of foreign-funded research to acquisitions is in fact rather small: an acquisition provides the acquirer with access to the mature technology and know-how of the target, while research funding or academic exchanges opens access to technologies that are still in infant-stages.

89. Concerns about the national security implications of foreign-funded research and academic exchanges have entered public discussion only recently, and so far, concerns seem to be concentrated in a few countries.⁵⁸

90. Today's nascent concerns in these areas may broaden when and if the parallels of exposure are considered sufficiently pertinent to trigger a policy response. Ultimately, the acknowledgement that the capabilities lie within humans' capabilities would constitute the latest step on the current path of dematerialising the source of risk: From hardware in the past decades to intellectual property and data today to human capacity in the future. No tangible or intangible assets will then need to change ownership, with yet unforeseeable implications for policy design.

91. The effects of such further dematerialisation of the transmitters of threats may have secondary effects on the allocation of financial and human capital: In anticipation of difficulties to sell businesses or assets to a world-wide market of investors, firms may allocate research capacities in countries that have no relevant policies or are less risk-averse to avoid that the fruits

⁵⁷ On 11 October 2017, Chinese firm *Alibaba* announced a [global research programme for cutting edge technology development](#), which was to set up research labs in the United States, Russia, Israel and Singapore among others, to work on “foundational and disruptive technology research including data intelligence, Internet of Things (IoT), fintech, quantum computing and human-machine interaction”—all areas that are now explicitly or implicitly singled out for their national security relevance in some countries.

⁵⁸ For the United States, policy proposals on such restrictions can be traced back to at least [May 2016](#), and resurface in Michael BROWN/Pavneet SINGH (2017), “[China's Technology Transfer Strategy: How Chinese Investment in Emerging Technology Enable a Strategic Competitor to Access the Crown Jewels of U.S. Innovation](#)”, Defense Innovation Unit Experimental, p.5, who consider (p.24) whether Visas for Chinese foreign national students studying in the United States without developing any proposal. Further reports about United States government considerations on restricting foreign researchers' collaboration emerged in [April 2018](#). In Canada, collaboration between Canadian universities and *Huawei* over research on 5G wireless networks have raised concerns in some circles, “[How Canadian money and research are helping China become a global telecom superpower](#)”, the *Globe and Mail*, 26 May 2018. On 8 January 2019, Oxford University [reportedly](#) suspended new research grants and donations from *Huawei Technologies Co Ltd* or its related group companies, citing growing security concerns.

of research and development cannot be sold at market value or at all if there is no market participant that could obtain regulatory clearance.⁵⁹

92. These trends may have secondary effects on global capital and human resource allocation: As the likelihood of sales-restrictions can be expected to be related to the degree of innovation, restrictions may stifle the flow of venture capital in such technologies to certain countries more broadly or lead to incorporation in countries with relaxed or no restrictions on foreign acquisitions. Likewise, individual talent may move to countries where their ingenuity or knowledge fetches higher returns. A country that operates stricter rules on foreign acquisitions and technology transfer could inadvertently push the development of technology and innovation abroad and undermine the conditions for innovation in their country, hence undercutting the foundations on which its prosperity and security ultimately relies.⁶⁰

7 Interaction increases between acquisition- and ownership-related policies and other norms of domestic and international law

93. Design and implementation of acquisition- and ownership-related policies to manage risk experiences increasing interaction with adjacent areas of law, both international and domestic law. This interaction stems from rights and protections afforded to the involved economic actors or society at large.

94. In policy implementation, such interaction is conceivable, for instance, with market-access provisions or investment protection provisions of investment treaties. Further interaction

⁵⁹ Significant price depressions of assets that were considered sensitive by governments of the seller have been observed early. Theodore MORAN (2013), “[FDI and national security: Separating legitimate threats from implausible apprehensions](#)”, In: *Foreign Direct Investment in the United States: Benefits, Suspicions, and Risks with Special Attention to FDI from China*, Peterson Institute for International Economics, p.56 mentions that after the sale of *Fairchild Semiconductors* to *Fujitsu* was blocked in 1987, the acquisition by *National Semiconductor* came at a substantial discount. Similar discounts were observed in other transactions – e.g. *Philips’* sale of its 80.1% stake in *Lumileds* in December 2016 earned Philips only around [USD 1.6 billion](#), slightly over half of what had been agreed with a different prospective acquirer in March 2015 ([USD 2.9 billion](#)) but for whose acquisition [regulatory clearance national security grounds had not been granted](#) – and national security concerns have long been used by competitors as a pretext to lower valuations to ease their own take-over ambitions.

⁶⁰ The secondary effects of policies and implementation have received little attention so far, as focus appear to be concentrated on achieving primary objectives; [Section 1752 \(3\) of NDAA 2018](#) may be understood to allude to these secondary effects when it states that “The national security of the United States requires that the United States maintain its leadership in the science, technology, engineering, and manufacturing sectors, including foundational technology that is essential to innovation. Such leadership requires that United States persons are competitive in global markets. The impact of the implementation of this part on such leadership and competitiveness must be evaluated on an ongoing basis and applied in imposing controls under sections 1753 and 1754 [which contain among others rules on technology transfer and export of foundational technologies] to avoid negatively affecting such leadership.” A more direct description of the potentially conflicting interests is formulated by Robert WILLIAMS, “[The Innovation-Security Conundrum in U.S.-China Relations](#)”, *Lawfare*, 24 July 2018 and Robert WILLIAMS, “[In the Balance: The Future of America’s National Security and Innovation Ecosystem](#)”, *Lawfare*, 30 November 2018.

with treaty-based national treatment provisions may occur when treaty-covered companies seek to engage in security-sensitive business with governments or in security-sensitive infrastructure with other parties in a given country.⁶¹ Interaction is also possible with high-ranking domestic law, in particular constitutional law, for instance with respect to due-process rules or civil liberties.⁶²

95. In addition to interactions that may occur in policy implementation, the dense net of international obligations in the area of international investment, including those taken on in investment treaties or multilateral arrangements such as OECD investment instruments, notably the Codes of Liberalisation, may constrain policy design. As additional transaction-types are brought under the cover of acquisition- and ownership-related policies, additional international rules may come into play and increase the scope of potential tensions or influence.

96. Interactions between these areas of law are bidirectional: Treaties increasingly contain carve-outs and language that seeks to accommodate present or anticipated future needs for policy space to manage acquisition- and ownership-related risk.

97. So far, these interactions have been subject to limited study, and few cases are known where tensions between different obligations and bodies of law have become apparent. This is likely to change however, as claims based on investment treaties are used more frequently and more ingeniously, as pre-establishment provisions in investment treaties and post-establishment policies to manage risk become more widespread. These trends may increase the potential for frictions and the need to establish adequate safeguards in treaty design.

98. Interaction has also been observed with constitutional law protections in countries that implement investment policies related to national security, especially where these policies allow for divestment orders. Again here, little study has been devoted to the issue in general and to conclusions for policy design in particular.

8 Dilemma situations emerge from policy practice

99. As ever more countries collect experience with their policies' implementation, they encounter more complex scenarios and difficult decisions. The power to prohibit certain transactions may not always address the full scope of economic implications of certain situations:

- What needs to be done when debt-for-equity swaps in an insolvency scenario would bring in an acquirer deemed unsuitable? While rules may cover such scenarios, they do

⁶¹ In February 2019, it was reported that a manufacturer of equipment used in telecom-infrastructure was threatening a treaty-based claim – as well as claims under domestic law – against a government that had publicly warned about alleged security concerns in relation to the manufacturer's products.

⁶² A case that is often cited in this context is [United States Court of Appeals for the District of Columbia District, No. 13-5315 \(15 July 2014\), *Ralls Corporation vs. CFIUS et al.*](#); while the matter was ultimately settled, the Court of Appeals acknowledged that the acquirer's property interests benefited to some extent from a constitutional protection with respect to due process aspects. The judgement was rendered before the recent reforms of the framework under FIRRMA in 2018, so other considerations may apply now.

not necessarily decide who should own the sensitive assets – and at what price – if the beneficiary of the swap does not receive government consent to the acquisition?⁶³

- Can certain assets or companies – for instance those developing advanced dual-use technologies – become unsellable because all potential suitors are considered a risk for the home country’s essential security interests?
- What if the government wishes to review the acquisition of an asset, e.g. a pipeline, by the government of another country in which the largest part of the asset is located? How to resolve the conflict between the public interest of one country to buy an asset that is situated on its soil with the public interest of another country who feels its national security may be impaired by that acquisition? How would, in extremis, the expropriation of an asset by the host country be handled by the review mechanisms of the home government of the previous owner?

100. Two factors are likely to lead to a growing frequency of such situations:

- The growing number of countries that operate review systems and the growing scope of their individual coverage; and
- The interlinkages of MNEs whose affiliates and operations span an ever greater number of jurisdictions, potentially triggering reviews in ever more jurisdictions.

101. The complexity is only just building up, and solutions are yet to be developed. In some recent cases, governments have acquired assets themselves through state-controlled funds to avoid their sale to suitors deemed undesirable or to overcome limitations of the rules in place. The German government suggested in February 2019 the establishment of a State-owned fund to acquire companies to prevent foreign takeovers in certain situations;⁶⁴ such funds have been in existence in other countries and have been used for such purposes in the past.⁶⁵ In others, the construction of infrastructure by the government itself has [allegedly](#) been considered to keep control over suppliers and manage risks. The Finnish Parliament began considering a bill in

⁶³ This issue was debated in the context of financial difficulties reported for *Petroleos de Venezuela* (PDVSA). PDVSA has given its significant ownership stake in Houston-based *Citgo* as collateral in exchange for a USD 1.5 billion loan from Russian company *Rosneft*. The United States [FIRRMA](#) (2018), Section 1703, explicitly clarifies that transactions pursuant to bankruptcy proceedings or other defaults on debt are covered by CFIUS reviews, but does not resolve the potential consequences.

⁶⁴ On 5 February 2019, Germany announced the prospect to establish a government fund to temporarily take over assets to avert undesirable takeovers (“[National Industry Strategy 2030](#)”, Federal Ministry of the Economy and Energy, 5 February 2019). In mid-2018 the State-owned German development bank *KfW* had acquired a 20% stake in a company, *50Hertz*, that owns an important electricity distribution grid and for which a Chinese company had bid; as the German screening policy at the time had set the trigger threshold for government intervention at 25%, the transaction was not under the scope of the review mechanism.

⁶⁵ In 2012, the French sovereign investment fund FSI – now known as *Banque Publique d’Investissement* (BPI) – acquired *Areva*’s stake in sensitive asset *Eramet* with this purpose (“[Agreement between AREVA and the Fonds Stratégique d’Investissement for the disposal of AREVA’s stake in Eramet](#)”, Areva press release, 16 March 2012); an allusion to the original statement by the then director general of the BPI is available in the [minutes of the Economic Affairs Commission of the French Parliament of 15 May 2013](#), and secondary documentation is available in the OECD policy monitoring report covering [measures taken 16 February to 15 September 2013](#) and the [Summary of Discussions at Freedom of Investment Roundtable 19](#)). In June 2018, the BPI and the Ministry of Defence created a further fund, [DefInvest](#) to support SMEs that are strategic for France’s defence sector.

November 2018 according to which the government would obtain a right of first refusal over the acquisition of certain areas of land to absorb assets that could be sensitive if in foreign hands.⁶⁶ These solutions are reminiscent of earlier decades when State-ownership of critical infrastructure was widespread even in advanced economies.

102. Not all governments may wish to acquire assets that have become too sensitive to be owned by any other bidder. Also, some sensitive assets may be too-big-to-buy, as some countries have experienced with financially distressed sensitive infrastructure assets such as ports.⁶⁷ In the past, golden-share arrangements have effectively allowed governments to control assets without putting up the equity required to command the equivalent power under regular rules; this model of the past may inspire governments again in the future.

103. The sole power to prohibit transactions or to order mitigating measures may not always offer sufficient flexibility to address security concerns and economic imperatives simultaneously; governments may increasingly orchestrate asset attribution or buy assets themselves to manage security implications of sensitive assets.

9 International cooperation – from harmonisation to mutual recognition – may become increasingly critical

104. With the number of countries that operate review mechanisms growing, and with supply chains and operations tending to involve more countries, individual transactions are likely to require clearance under acquisition-related policies in ever more jurisdictions. This development will likely increase uncertainty, delays and costs for transactions, and transactions involving multinational enterprises (MNEs) with operations in multiple jurisdictions may become less manageable.

105. That MNEs have to meet regulatory requirements in multiple jurisdictions is a standard occurrence in a globalised economy and not confined to such security-focused reviews. In many areas where countries seek to regulate aspects of a globalised economy, international cooperation has helped attenuate the effects of the accumulation of review requirements. These examples and practices could inspire solutions for reviews for essential security interests as well, while taking into account the specificities of the area.

106. International cooperation can take many forms, such as information-sharing, regulatory alignment and mutual recognition; several avenues of cooperation can be pursued in parallel. Cooperation may be delicate where essential security interests are concerned, given the confidentiality that dominates this area, different strategies, vulnerabilities and risk assessments in different countries, among others, and countries may not be willing to share their concerns and information as willingly as in other areas.

107. Even when considering these specificities, there is probably scope for cooperation: Some countries have established cooperation on national security issues that involve information-sharing,⁶⁸ have publicly emphasised the importance of “cooperation on investment

⁶⁶ [Bill HE 253/2018, tabled in the Finnish Parliament](#) on 29 November 2018.

⁶⁷ An example of this scenario is the acquisition of a 99-year lease of the port of Hambantota (Sri Lanka) and 69km² of land in 2017 by a foreign lender following difficulties to serve debts for its construction.

⁶⁸ E.g. intelligence co-operation under the [UKUSA Agreement](#) (“Five Eyes”).

reviews for national security purposes”,⁶⁹ and some new policies – e.g. in the United States⁷⁰ or the European Union⁷¹ – call explicitly for international cooperation, without always making the avenues and mechanisms explicit.

108. In addition to information sharing, regulatory alignment could be a promising avenue to reduce drag on transactions that results from the differences in criteria and procedures that individual countries apply on a same given transaction. These differences increase costs and time required to complete transactions – without necessarily producing commensurate benefits for governments and the societies they serve. Alignment of criteria and procedures, to the extent possible and practicable, could help lower the impact that the accumulation of review requirements in different jurisdictions is likely to have.

109. In other policy areas, concentration of a government response in one jurisdiction, combined with full or partial recognition of findings or decisions by other jurisdictions have proven useful and effective: Examples include the cooperation among competition authorities in merger reviews to lower the burden for businesses and government resources.⁷² Similarly, National Contact Points established under the OECD Guidelines for Multinational Enterprises to resolve specific instances of operations by MNEs cooperate and concentrate case-handling in the NCP that is closest to the issue.

110. International cooperation relies on understanding, shared information and trust. Only where information is readily available to peers, can regulatory alignment work, and the basis for mutual recognition be established. This survey of practices, along with OECD-hosted policy dialogue and transparency mechanisms contributes to informing governments about the policy choices their peers have made.

⁶⁹ E.g. “[Joint Statement of the Trilateral Meeting of the Trade Ministers of the European Union, Japan and the United States](#)”, 9 January 2019. On 25 September 2018, a [Joint Statement on Trilateral Meeting of the Trade Ministers of the United States, Japan, and the European Union](#) had stated that “The Ministers confirmed the importance of coordination among themselves to mitigate risks to their national security from trade and foreign investment, including the continued cooperation between appropriate authorities of the three partners to share best practices and exchange information on foreign investment review mechanisms.”

⁷⁰ [FIRRMA](#) (2018), Section 1713 allows CFIUS to establish: a formal process for the exchange of information with governments of countries that are allies or partners of the United States that facilitates the harmonization of action with respect to trends in investment and technology that could pose risks to the national security of the United States and countries that are allies or partners of the United States; provide for the sharing of information with respect to specific technologies and entities acquiring such technologies as appropriate to ensure national security; and include consultations and meetings with representatives of the governments of such countries on a recurring basis.

⁷¹ European Union (2019), [Framework for screening of foreign direct investments into the European Union](#), Article 13 states: “Members States and the Commission may cooperate with the responsible authorities of third countries on issues related to screening of foreign direct investment on grounds of security and public order”.

⁷² See on this effort to foster cooperation among competition authorities the OECD work on [International co-operation in competition](#), OECD webpage, undated.

www.oecd.org

