Dealing with China on high-tech issues

Views from the US, EU and like-minded countries in a changing geopolitical landscape

Clingendael Report

Brigitte Dekker &
Maaike Okano-Heijmans (eds.)

Clingendael
Netherlands Institute of International Relations

Clingendael

Netherlands Institute of International Relations

Dealing with China on high-tech issues

Views from the US, EU and like-minded countries in a changing geopolitical landscape

Brigitte Dekker & Maaike Okano-Heijmans (eds.)

Clingendael Report
December 2020

This Clingendael report includes country case studies by the following authors:

United States – James Andrew Lewis – Center for Strategic and International Studies (CSIS)
United States – Martijn Rasser – Center for a New American Security (CNAS)
United States – William Alan Reinsch – Center for Strategic and International Studies (CSIS)
Australia – Bart Hoogeveen – Australian Strategic Policy Institute (ASPI)
India – Rudra Chaudhuri – Carnegie India
France – John Seaman, Marc Julienne and Françoise Nicolas – Institut Français des Relations Internationales (IFRI)
Germany – Bernhard Bartsch and Anika Sina Laudien – Bertelsmann Stiftung
Japan – Kazuto Suzuki – Tokyo University

All contributions reflect solely the authors' views.

December 2020

Cover photo: Inserting connector into a socket with flag of the EU. Translation or online connection concept, 3d rendering. © Shutterstock

About the authors

Brigitte Dekker is a Junior Research Fellow at the Netherlands Institute of International Relations 'Clingendael' in The Hague. Her research focuses on various dimensions of EU–Asia relations, with a specific interest in South-East Asia and China.

Maaike Okano-Heijmans is a Senior Research Fellow at the Netherlands Institute of International Relations 'Clingendael' in The Hague and a visiting lecturer at the University of Leiden. Her main research interests are in connectivity, economic diplomacy and international relations in EU-Asia relations, with a special focus on China and Japan.

Table of contents

Introduction

Brigitte Dekker and Maaike Okano-Heijmans (editors) –
Clingendael Institute, The Hague

Under the administration of President Donald Trump, the United States' (US) decided to retreat from the international order that it had helped build over the past seven decades. This marked a significant turning point in international affairs. Combined with the challenges imposed by an increasingly powerful, confident and capable China, this put the European Union (EU) and its member states on a track to reposition themselves in a world defined by great power rivalry and without a guaranteed, strong transatlantic partnership.

As President-Elect Joe Biden enters the White House, opportunities for EU–US cooperation are set to grow, both bilaterally and in the multilateral context. The newly established EU–US China Dialogue (October 2020) and the EU's paper titled 'EU–US agenda for global change' (November 2020) show that both sides are ready to re-engage on key issues. China and high-tech feature prominently. This is important, as China's growing dominance in the digital domain challenges not only the existing balance of power, but also – and more profoundly, perhaps – reshapes the rules of the game of that very system and the standards and norms underpinning it. The US is strongly resisting both developments, not afraid of direct confrontation. Even though the EU shares the US concerns about the geopolitical alterations, it does not wish to curb China's rise as a technological power.

Renewed transatlantic cooperation?

Despite the optimistic tone of the European Commission's paper, transatlantic consensus on key topics such as reforming and strengthening the World Trade Organisation (WTO) and jointly shaping the digital regulatory environment will be challenging. There is 'no way back' to the pre-Trump era for the transatlantic partnership, which in recent years suffered severe setbacks.

Both the EU and the US stand to benefit from a 'grand bargain' with like-minded countries that encompasses a variety of issues in the tech and data domains. This would entail different parts of the high-tech and digital ecosystem, and allow all sides to address jointly any concerns related to China, as well as to update policies and regulations to contend with the rapid technological change that is impacting our

societies. Clearly, such a comprehensive agreement requires change and concessions on both sides of the Atlantic. As stated in the Commission's paper:

> *As open democratic societies and market economies, the EU and the US agree on the strategic challenge presented by China's growing international assertiveness, even if we do not always agree on the best way to address this.*

For its part, the US needs to acknowledge that its 'unipolar moment' is over and that it, too, needs to make concessions – if not to China, then at least to its allies. In the coming years, its goal should go beyond deterring 'great-power war' to also including 'great-power peace and cooperation in advancing shared interests'.

Separately, a grand bargain requires that European countries be clear about where they stand – that is, not equidistant from the US and China, but with closer and deeper links to the US. This position, as visualised in figure 1 below, is implied in the Commission's paper, which represents Europe's efforts to chart its own course and emphasise what the EU can bring to the table in the economic, political and (hard) security fields.

Figure 1   No equidistance: the transatlantic relationship and the EU/US views on China in trade–tech issues reflected in a scalene triangle
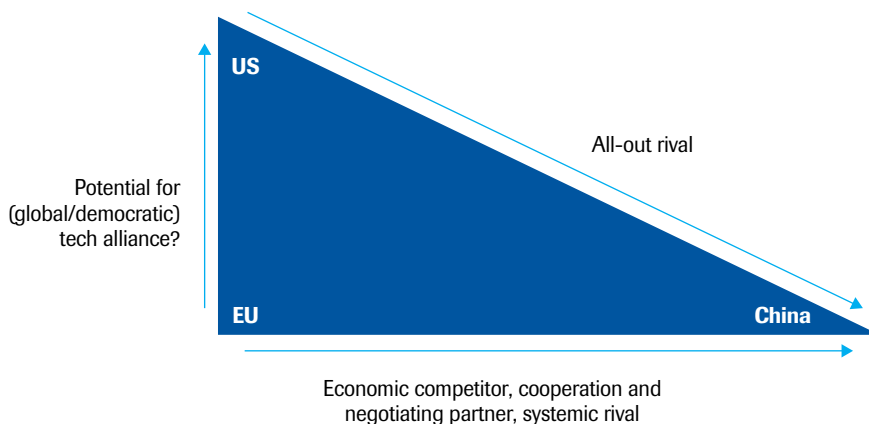
After years during which the growing power of China – also as a norms and standards-setter in international politics – became more evident and the US sometimes looked at its European allies with contempt, the EU has started to chart its own course. The EU's response to China's Belt and Road Initiative came only in September 2018, with the launch of its Connectivity Strategy, and the engagement of European countries and the EU with like-minded partners in the Indo–Pacific region is only now taking off.

The EU and its member states have also taken various defensive measures in recent years – including on investment screening and a 5G Toolbox – and discussion on 'strategic autonomy' more broadly is now firmly on the agenda. With the COVID-19 pandemic, this concept has been widened from issues of defence and security, to new subjects of an economic and technological nature. EU High Representative and European Commission Vice-President Josep Borrell refers to this as 'the Sinatra doctrine': calling on the EU to deal with the US and China in its own way – that is, 'from its own point of view, defending its values and interests, and using the instruments of power available to it'.

A more autonomous EU may not in all ways be to the United States' liking. The US, specifically under the Trump administration, has raised concerns that strategic autonomy may signal a more independent EU that does not naturally follow the US lead. Examples include, among others, efforts by the EU and its member states to uphold the Iran Nuclear Deal after the US withdrawal from the agreement, and their resistance to US pressure to ban Chinese telecommunications firm Huawei's 5G infrastructure equipment.

For their part, the EU and its member states have emphasised that increased strategic autonomy for the EU would mean they would be more capable and better equipped to act internationally as an equal partner to the US. The EU's push towards strategic autonomy should thus not be mistaken for a protectionist or inward-looking EU. To quote Borrell once more: 'Only a more capable, and thus more autonomous Europe, can meaningfully work with Joe Biden's administration, to make multilateralism great again'.

Going forwards, it is clear that the EU and its member states' aim for continued engagement with the US and deepened and renewed engagement with other partners and stakeholders. Together, they need to deliver on broadening multilateralism to new areas and, in certain cases, new approaches.

This Clingendael Report aims to contribute to a reorientation of the EU in the trade, high-tech, and digital domains, in the transatlantic context and with Australia, India and Japan. The policies of European governments and businesses in this domain are undergoing profound changes: stakeholders are starting to act on the awareness that some geopolitical challenges, in particular concerning China, cannot be solved within the liberal–democratic mindset alone. Still, however, they do want to uphold and update the basic principles of the rules-based system.

An 'outside–in' approach: views from key partners

In discussing the many economic security challenges, this report adopts an 'outside–in approach': presenting views and forward-looking suggestions by key experts from

the US and significant European and Asian countries, rather than from a specifically Dutch or EU perspective (or 'inside–out').[1] Hence, eight chapters present views from six countries: three from the US; and one each from Australia, India, France, Germany and Japan.[2] The inclusion of three US contributions reflects the starting point of the project: dealing with China in the transatlantic context. For their part, France and Germany were chosen for their key roles in EU politics and economics, and their strong track records in pushing the debate on China forward in the EU-context. These chapters not only discuss the domestic context in these two European countries, but also reflect on transatlantic cooperation between the US and the EU as a whole. Finally, Australia, India and Japan stand out as three partners with whom deepened cooperation seems particularly promising in this particular field.

All of the experts were asked to reflect on the same leading question:

> *What opportunities and challenges exist for cooperation, coordination and synergies between the US and the EU, and with like-minded partners in Asia, to address the shared challenge of a stronger and more assertive China?*

Taking this question as a starting point, all of the experts were asked to reflect on their government's approach to issues spanning defensive measures such as 5G, investment screening, export controls and foreign influencing, as well as offensive and regulatory issues including platform regulation and data protection, and the upholding of standards in the field of digital human rights. In addition, they offer reflections on developments in Europe and opportunities for future cooperation with Europe, the US and like-minded partners, including in multilateral settings.

The chapters can be read as stand-alone sections, but are most valuable when read together. As a whole, the eight chapters offer valuable insights into the convergences and divergences that exist among the transatlantic partners, and Australia, India and Japan. These convergences and divergences are shaped by countries' political philosophies and economic systems, and extend to the problems that countries experience, concerns that are prioritised and their preferred approaches to dealing with the perceived challenges.

Finally, in the concluding chapter the editors will highlight the key trends that emerge from the preceding chapters, as well as a few key insights that stand out as opportunities and obstacles for further dialogue and joint action.

---

1   For this reason, a stand-alone chapter on the Netherlands is not included in this report. The conclusion does include reference also to the EU, based on analysis presented in various chapters of this report as well as earlier work by the editors. (see also footnote 16)

2   The contributions reflect solely the authors' views and not those of their institutions. The experts were selected based on their proven track record on the topics under discussion.

EU and US policies towards China

William Alan Reinsch – Center for Strategic and International Studies (CSIS), Washington D.C.

The Trump administration prioritised restructuring its relationship with China. Originally described as an attempt to rebalance the trading relationship and reduce the bilateral trade deficit, the administration subsequently changed its focus to concentrate on security issues and the threat that Chinese actions pose to US national security. There are three reasons for this change:

1) Increased awareness of the threat to US telecommunications networks using Chinese hardware and software, along with growing concern about the threat of cybersecurity incursions.
2) Growing realisation that the security threat also encompasses China's goal of supplanting US technology leadership globally, and that one of China's tools to accomplish this is acquiring US technology legally or illegally to accelerate China's own development.
3) President Trump's pique at his inability to achieve his economic goals with China and at China's handling of the COVID-19 pandemic.

The emphasis on security has also accelerated a significant decline in public support for China in the US and has consolidated opinion among leaders of both the main US political parties behind the president's analysis, if not his tactics, which remain the subject of controversy.

Trade

President Donald Trump favoured trade tools, primarily tariffs, that are intended to bully the target into acceptable behaviour. To that end, he imposed tariffs on approximately 65 per cent of Chinese imports, which had the effect of raising the average tariff rate on Chinese goods from approximately 3 per cent – the Most-Favoured Nation (MFN) rate – to 19 per cent. This resulted in an agreement, characterised as 'phase one', implying that there is a phase two to come, which consists largely of Chinese commitments to purchase increased quantities of US goods and to make a variety of regulatory changes that will permit greater access to Chinese markets and increase the ease of doing business there. The important issues in the negotiations – Chinese subsidisation,

forced technology transfer and favoured treatment for state-owned enterprises, among others – were reserved for phase two, which may not take place. The Chinese have met many of their phase one regulatory commitments, but are well behind in their purchase commitments. Since their obligations are based on the calendar year, it is too soon to conclude that they will not meet them, but there is widespread scepticism in the policy community whether they will do so.

Defensive and offensive security measures

With respect to security issues, the Trump administration has acted both offensively and defensively. Defensively, it has sought to maintain the integrity of US telecommunication systems by requiring the removal of Chinese equipment and prohibiting additional imports. The administration also took a variety of non-public actions to prevent cybersecurity breaches and deter hacker attacks, many of which appear to originate in China. In addition, the administration has implemented new legislation that expands government reviews of inbound foreign investment. While the law applies universally, its effect has been increased rejections of proposed Chinese investments, which, coupled with Chinese policies discouraging outbound investment, has led to a record low amount of Chinese foreign direct investment (FDI).

Offensively, the Trump administration has sought to dissuade other countries from installing Chinese telecommunications equipment, with mixed results so far. It has also attempted to slow down China's technological progress by denying it critical technologies. Huawei and its subsidiaries have been placed on the US Commerce Department's Entity List, which means a licence is required for any exports to them. In addition, reacting to China's policy of blurring the distinction between military and civilian production, the administration has expanded export controls on dual-use items to cover end-users previously considered civilian but now reclassified as military because of their relationship with China's armed forces, the People's Liberation Army (PLA). The primary impact of that measure has fallen on the semiconductor industry. Finally, the administration has used the extraterritorial aspects of US law to prevent third-country producers of critical dual-use items that either contain US content or are manufactured using US equipment from exporting them to China.

There are rumours that the US administration will broaden the reach of these restrictions. At the same time, outrage over the Chinese government's repression of its Uyghur minority and its actions in Hong Kong have led to economic sanctions on individuals and companies complicit in those actions. While not strictly related to security, they have become part of a larger policy effort aimed at demonstrating the unacceptability of Chinese behaviour and US determination not to condone or facilitate it.

At the same time, the administration has begun to increase research and development (R&D) in selected areas, such as quantum computing and artificial intelligence,

although the scale of expected government support still lies far behind China's. A Biden administration will likely do more in this area.

Diverging transatlantic views

It appears that while many EU member states may be moving in the same direction as the US, they remain considerably behind in their conception of the seriousness of the 'China problem' and in prioritising dealing with it. That appears to be changing, impelled in part by the same human rights issues that have contributed to China's downward spiral in American public opinion. At the same time, European governments do not appear eager to disrupt existing economic relationships with China. American companies are largely not eager to 'decouple' either, but the US administration's pressure to do so, combined with its tariff and export control policies, has created a different set of economic calculations in the US than in the EU. Were the European Commission or the larger EU member states to adopt policies similar to those of the US, European companies would likely respond in the same way American companies are responding.

One area where European attitudes are changing more rapidly is with respect to both 'technological sovereignty' and 'strategic autonomy'. This is the consequence of growing concern in Europe that EU countries are falling behind in sectors key to future economic growth and job creation, and that the EU should carve out its own path rather than follow those of the US or China. In the short run, much of the anxiety is focused on climate and the digital economy and the significant role that large US companies play in the latter sector in Europe, particularly the so-called GAFA companies (Google, Apple, Facebook and Amazon). A similar level of concern has yet to be expressed about Chinese companies such as Alibaba, ByteDance and WeChat, no doubt because their presence in the EU marketplace is much smaller. Regardless of the source of concern, however, EU actions to accelerate Europe's own technological development in these sectors will impact both the US and China. The US argument will continue to be that EU policies should be focused on China as the greater threat, but it does not at present seem clear whether that view is universally shared in the EU. The hostile actions of the current Trump administration towards Europe and resulting low opinions of the United States within Europe are making the US argument more difficult.

It is too soon to say how this issue will evolve in the EU. There appears to be a debate about the merits of industrial policy generally, which is similar to the debate in the US. The US experience has been, however, that consensus on industrial policy (or innovation policy, as it is increasingly being called) is easier to achieve if the rationale is national security-based rather than competitiveness-based. That also explains why the US has mixed feelings about its development in the EU: welcoming it as a counterweight to China, which is a national security rationale; but objecting to it if it is seen as disadvantaging US companies, which is a competitiveness concern.

The multilateral context: the WTO and China

The Trump administration has not been very interested in the multilateral system. President Trump believes in the unilateral exercise of American power, and he has withdrawn from, ignored or fought with multilateral institutions. The US 'contribution' to the system, therefore, has been primarily negative, with one exception. The Trump administration has been successful in drawing multilateral attention to difficult issues that have long gone unaddressed. A good example is its ongoing effort to point out the shortcomings of the World Trade Organisation (WTO). A frequent statement in the US about the president's policies has been 'right diagnosis, wrong prescription'.

The EU claims to be more supportive of a multilateral approach to problem-solving, although there is a strong view in the US that there is a substantial element of hypocrisy in EU public statements. President-Elect Biden is a committed multilateralist, and once he takes office, US policy with respect to multilateral institutions will change.

Consistent with its multilateral approach, EU thinking has been 'inside the box', in that it believes that actions taken concerning China should be consistent with multilateral rules. The Trump administration has argued that China does not fit inside the box – that it is too big and complex, and existing institutions and rules are not equipped to cope with it. In contrast, the incoming Biden administration will attempt to develop a common policy with the EU, but its goals will not differ significantly from Trump's.

With respect to the US private sector, the American public is not deeply engaged with multilateral rules or institutions. Companies that are in China, however, do not share the Trump administration's preference for tariffs and prefer an approach more focused on diplomacy and multilateral persuasion. However, there has been a noticeable erosion in the business community's willingness to press for 'constructive engagement' policies publicly. Over the past five to ten years, as China's policies have moved in the direction of more state control and as the Chinese regime has become more repressive, the US business community has found itself in a dilemma: China is simultaneously their best customer and their biggest threat. They see the enormous competitive challenge they face from companies backed by huge Chinese-government subsidies, but they are reluctant to endorse policies that might ultimately force them to abandon China and the profits they are making there. The result is that many US companies are paralysed, unsure of what to do. The result has been that the public policy debate field has largely been ceded to the China 'hawks', who advocate a more confrontational policy. There are recent signs that the business community is slowly moving towards accepting the possibility of decoupling. Consumer-facing businesses face the growing risk of consumer backlash if they are seen to be doing business with Chinese companies involved in China's policies of repression, and others are simply finding it increasingly difficult to do business in China because of the government's discriminatory policies. Decisions about leaving China, however, will primarily be based on a company's

business model. Those that are in China to serve the Chinese domestic market will stay. Those that are manufacturing in China and shipping back to the US will be under growing pressure to leave. Those that do leave will not necessarily return to the US, but will more likely go elsewhere in South-East Asia or to Mexico.

The future of the transatlantic relationship

The EU appears to be moving slowly in the same direction as the US, but remains considerably behind in its willingness to confront China directly. Even where a plan is being debated, as with the technological sovereignty issue, the goal seems to be ensuring European companies are better able to compete with American companies in Europe. Achieving consensus on a plan of action among the EU member states will also be difficult, although it does appear that China may be squandering any goodwill that resulted from its Belt and Road Initiative, which will make it easier for countries that have benefited from Chinese investment to support strong measures, nevertheless.

Under a Biden administration, prospects for active coordination between the US and Europe will improve significantly. His administration will be more interested in a common approach that is consistent with multilateral rules. Its analysis of the problem, however, and its determination to address it will not be appreciably different than that of the Trump administration, except in two respects. First, a Biden administration will place greater emphasis on human rights and will expect its partners to do the same. That will make progress with China more difficult, but it will be a political imperative in the US. Second, a Biden administration will look at the relationship holistically rather than transactionally. That means there will be an overall strategy that would look for areas of cooperation, such as climate change, as well as identify areas of conflict.

Despite a more strategic approach, American public opinion has shifted sharply against China, and Biden will be under considerable Congressional pressure to take a strong stand. If possible partners, whether in Europe or elsewhere, take a more nuanced approach, it may be difficult to agree on a joint plan of action. While the EU may be an obvious place to discuss cooperation, it is not the only place, and a Biden administration will reach out to Asia in order to restore the American presence in the Pacific. Many Asian nations have hundreds of years of experience dealing with China and will prefer to walk a line between the two contending powers. To the extent Chinese policies become more aggressive, coalition-building will be easier.

Mitigating Chinese influence begins with understanding US limits. The current leadership in China has made statist economic policies an integral part of their overall strategy for controlling the country. They resist Western demands for market reforms not because the demands are bad economics, but because, for them, they are bad politics. This is not likely to change. While it is appropriate to press China on its failure to meet

international obligations or on actions that break multilateral rules, we should be realistic about what that can accomplish. What we can better control are our own economies. Successfully pushing back against China will require three things:

1) Pursue domestic economic policies that promote innovation and job creation.
2) Recapture the international standards-setting process so its products do not favour Chinese standards.
3) Build international economic structures based on rule-of-law and market principles.

Those actions will produce a stronger, market-oriented global community that will constitute the most effective counterweight to China.

A renewed transatlantic partnership

James Andrew Lewis – Center for Strategic and International Studies (CSIS), Washington D.C.

The shared values of transatlantic market democracies provide the foundation for a renewed partnership to defend, once again, fundamental rights and the rule of law, since these are again under threat from powerful authoritarian regimes. This renewed threat requires that we strengthen existing vehicles for collaboration and build new ones when necessary. Greater transatlantic cooperation is necessary to reduce the flow of advanced technology to China, counter China's predatory commercial practices and agree on policies to defend fundamental rights and strengthen transatlantic growth. Addressing these problems requires agreement between Europe and the US on some difficult issues, something that we should not assume will occur automatically or in its old forms.

The foundation for renewed cooperation between Europe and the US is the transatlantic community's shared values. These values are now under threat from powerful and ambitious authoritarian regimes in China and Russia. While a growing concern over China's behaviour is shared by European nations, the US and Asian democracies, this shared concern does not translate automatically into a common approach, and there is considerable risk of a transatlantic divergence. That said, European ambivalence about China appears to be ending. China is not a security threat in the traditional sense, as the People's Liberation Army (PLA) is unlikely to invade Europe, but it is an economic and political threat, as China's economic policies and its disregard for fundamental rights and the rule of law harm European democracy. Under the current leadership in Beijing, this is unlikely to change. The Chinese believe that the United States and the West are in decline and that China is in the ascendant. The possibilities for agreement are shaped by this Chinese expectation of a gain in relative power for its one-party state. Both Europe and the US would be better served if they met this challenge jointly.

We should not have to make the case for why a unified transatlantic response to China is necessary. Under President Xi, China's ambitions have grown and its use of illicit and predatory practices to achieve those ambitions has also grown. This poses not only a security risk, but a risk to economies around the world where industries could find themselves competing with Chinese firms that benefit from both state capitalism and state-supported technological espionage. More importantly, China's leaders do not

respect the rule of law or fundamental human rights, something that China has shown in Hong Kong and within its own borders against minorities such as Uyghurs or Tibetans, as well as, frankly, against its own people. There are profound ethical issues raised by relations with a country that possesses immense re-education camps where the grounds for incarceration are simply a different religion or culture.

It will be difficult to thwart China's ambitions and will take years of sustained action to get it to change its behaviour, but in the past the Chinese have been willing to make concessions when unified demands came from the US, Germany, United Kingdom, European Union, Japan, Canada and other Western countries. Yet while US allies are suspicious of China and are considering their own measures to reduce economic risks, the US has not cultivated the potential alliances that allies' distrust could afford. The Chinese fear that we will forge alliances, which is a good indicator of its usefulness.

What will not change after the US elections?

Biden's win in the 2020 US presidential elections signals an end to chaotic policy-making and over-excited nationalism. However, there are trends that will not be affected by the outcome. The first is that the direction of American policy to counter China will not change, although its implementation is certain to be different and the ultimate goal may no longer be a hard 'decoupling'. This is not yet a new Cold War (at least not yet). Nor will this be a new 'containment'. China does not have the universalist goals of the Soviets, although it is no friend to democracy or law. The business connections between China and the rest of the world are too great for easy decoupling. The goal should not be to isolate China or bifurcate the world, but instead to compel China to change its behaviour. Managing China requires a common approach by the US and Europe. On a political level, the elements of this are already there: a shared concern for democracy and human rights and a shared interest in the rule of law. These provide the framework upon which a partnership can be built, but serious issues must be addressed for this to move forward.

Obstacles to transatlantic cooperation

There are significant obstacles to transatlantic cooperation, chief among them Europe's desire for technological sovereignty, its reasonable concerns about American tech giants over competition and taxation, and the gulf between the US and EU over deep and legitimate European concerns about privacy. These issues cannot be dismissed. A Biden administration is likely to be more sympathetic to some issues, but less willing to compromise on others when they affect business interests. Each issue, however, presents opportunities to build a stronger relationship, based on shared political values. 2021 is a year of opportunity. In the US, it is likely to be the year when the US finally

reconsiders its patchwork of privacy protections. This will entail a long debate, with change stubbornly resisted by technology giants, and the outcome will not be a decision by the US to adhere slavishly to the EU's General Data Protection Regulation (GDPR) – the argument that since EU members have made up their mind, it cannot be changed, simply does not hold in international negotiation. If there is flexibility on both sides, the possibility for agreement on how to govern technology can increase.

Anti-trust, taxation and regulation are also major issues between the US and the EU, reflecting real disagreement about how best to manage the commercial consequences of technological change. This goes beyond commerce and involves managing hate speech, protecting fundamental rights, governing data flows and developing ethical guidelines for new technologies like artificial intelligence (AI). The essential questions are whether we need multilateral agreement on rules and perhaps institutions for tech governance, and how the US and EU can work together to build such new rules and understandings. Much will depend on whether we emphasise our differences, such as attitudes towards risk and entrepreneurship, or our political similarities.

Areas of cooperation

If progress can be made on these issues, some measures can be put in place to protect transatlantic economies and accelerate their growth. One area for cooperation is the screening of potential foreign investments. Foreign investment screening has become a key issue for the European Union, which is in the process of implementing a new screening mechanism to facilitate dialogue and mandatory information-sharing between member states and the European Commission regarding incoming foreign investment and acquisitions across Europe. The new regulations allow both states and the European Commission to present enquiries about investments in other states, although each member state will maintain national competency over, and final adjudication of, investments within its borders.

European Union member states have increased their scrutiny of Chinese investment in the technology and critical infrastructure sectors. Each EU state maintains its own national assessment of the dangers of inviting and accepting ownership by both public and private Chinese entities (although governments increasingly acknowledge that this distinction may not necessarily exist for Chinese investment) within industries deemed essential to national security and economic competitiveness. The new EU-wide rules on foreign investment that are set to take effect in national regulation in the next few months are a recognition of risk and an opportunity for transatlantic cooperation.

In the screening of Chinese investment, transatlantic collaboration would be valuable, first in the sharing of information about potential acquisitions, since one thing we have seen in the past is that when Chinese investment is denied in one country, it will go to

another to seek approval. The same is true for technology transfer. The second area for collaboration is the sharing of information on potential Chinese acquirers. This can be difficult for every nation, given the opacity of the Chinese government's involvement and intent, but working together, the intelligence resources of the United States, combined with those of European nations, could allow for improved screening of potentially dangerous transactions.

Another area of cooperation is a common approach to technology transfer. Both the US and EU nations are members of the Wassenaar Arrangement, the principle regime for export control. Yet the Wassenaar Arrangement needs to be modernised and does not fully capture the 'emerging technologies' that have caught the attention of pundits and policy-makers. The Wassenaar controls need to be updated to better capture these emerging technologies and address the difficulties created by attempting to regulate the integrated supply chain built with China over recent decades.

A third area for collaboration is ensuring the integrity of the standards-setting process. The standards-setting process is complicated, making it easy to exaggerate China's success, but there should be no doubt about its intent. Anecdotal reports from attendees at international standards meetings tell of greatly expanded Chinese participation. A standards process dominated by China could be manipulated to put both American and European companies at a disadvantage. At a minimum, common advocacy for standards processes that are country-neutral and depend on the selection of the best technology – and not political preferences – would advance transatlantic interests. It might be easiest to start with those areas where transatlantic agreement faces fewer obstacles. The more difficult issues, such as anti-trust and anti-competitiveness, will take longer to reach accord.

A shared agenda for growth

There are policies that the US can pursue cooperatively with European partners to help build a strong transatlantic innovation base. The US can support a drive for 'technological parity' by Europe rather than the pursuit of technological sovereignty – which is unlikely to end well because innovation is now transnational, connecting Europe, Asia and the US in a web of commercial and research ties that cannot be undone without cost to innovation.

This issue of innovation is linked to the privacy debate, since it is likely that European privacy regulations have had a chilling effect on its tech innovation. Europe missed the first technology boom. There are many reasons for this. Overregulation is one, as it discourages entrepreneurship and innovation. China's predatory policies are another. While European and American companies compete, the same is not true for nations. It is in the US interest to see a vibrant and innovative Europe.

A key issue for the United States is how to strengthen Europe's ability to innovate and create new technologies. This is, of course, a goal that the Europeans seek as well. It is accurate to say that Europe is more likely to achieve its technological goals if it works in partnership with the United States, but there are fundamental issues regarding the treatment of companies that offer services transnationally. These include taxation, competitiveness and privacy. All of these are serious issues that must be addressed if the US and Europe are to build a transatlantic technology partnership.

Some have called for greater R&D cooperation between the US and Europe. R&D cooperation is easier if it is confined to fundamental research, where the eventual ownership of any intellectual property created is not an issue. In some technologies, there are already strong transatlantic interconnections at both commercial and academic levels, such as in artificial intelligence. On 5G, there is an emerging transatlantic consensus (along with Japan and Australia) on the need to look beyond cost when making decisions on trustworthy infrastructure. The interesting question now for 5G is not how we build the 5G infrastructure, but how we use it to accelerate innovation and commerce, and this is where Europe has some advantages in the industrial internet that 5G will expand when we think of automotive technology or leading examples like Swedish digital streaming service Spotify. Europe has a great opportunity to innovate in this industrial internet that 5G will enable, but all would benefit from working together with Japan and others in making it even stronger.

There are dynamics on each side of the Atlantic that move both Europe and the US in the direction of stronger partnership. On the US side, there is a growing understanding of the benefits of potential government support for technology: this could fall under the rubric of industrial policy. The new Biden administration will embrace this. Of course, Europe has long used industrial policy as a tool, and there is an opportunity to find common ground that balances the European preference for a more directive industrial policy with the American preference for a more market-based approach. There is a middle ground that, if found, would make economies on both sides of the Atlantic stronger.

Rebuilding the post-1945 institutions

One dilemma for this discussion is that existing mechanisms for cooperation are inadequate either because of their membership, which in many cases is too broad, or inadequate because they are not specifically focused on the China problem. For example, the Wassenaar Arrangement does not have a membership that is likely to support a more assertive posture against China.

Some countries have proposed new arrangements, perhaps informal, focused on specific technologies and limited to those countries that actually make them.

Semiconductor-manufacturing equipment, for example, is largely dependent on four countries: the US; Japan; the Netherlands; and Germany. These might be all the countries (possibly with the addition of South Korea) that are needed to form the basis of some kind of new multilateral arrangement. If we were to look at a broader group of countries, it could include many members of the European Union, Japan, Australia, Canada and perhaps a few others. This kind of new multilateralism will have to be part of a response to China if it is to make progress.

The weakness in existing institutions goes beyond the Wassenaar Arrangement. The international order developed after 1945 no long fits global political realities and in some instances, such as the WTO, the post-1945 institutions have failed to deal with the central issue of our time: China's rise. China simply ignored its commitments and the institutions' failures to respond have been damaging. Technology helps to drive this erosion. Technology giants wield political power, dominate commerce and collect massive amounts of data on their users, but the trans-border nature of their commerce has rendered them immune to oversight and regulation. The outlines of new, informal coalitions are emerging, but they are at an early stage and the democracies will need to develop a shared vision and common strategy to rebuild or replace the global institutions inherited since 1945, starting with membership that is limited to market democracies. One example can be found in the joint statement signed by 27 countries at the UN General Assembly in 2019, agreeing to work together on a voluntary basis to hold states accountable for their behaviour in cyberspace. This agreement, which does not represent traditional alliance structures, is the 'precursor' of a new democratic multilateralism.

Shared transatlantic concerns – over China's predatory economics and the rise of authoritarianism – offer the possibility to build something new, but shared concerns do not guarantee an alliance, especially on technology issues. We will first need engagement to find common understandings on privacy, competitiveness and digital sovereignty to reach any agreement. Some kind of grouping, whether it is a revision of an existing group or a new one, is essential, as the 1945 structures do not work for resisting China.

A 'tech alliance' (whether formal or informal) must begin with core principles for accord among nations, the most important being that there must first be political agreement among the members if a group is to have meaningful effect. This kind of agreement has been frayed since 2016, but it can be rebuilt. Organising principles cannot be a dislike of China or a fascination with new technology, but would need to be based on agreement among members to endorse the rule of law and fundamental rights, and to decide how these principles should guide the governance of technology.

The opportunities for potential cooperation are great, but there are significant obstacles that must be overcome and common approaches to privacy, competitiveness and

innovation will need to be developed. Technology is at the core of these issues, and technological change places immense strain on the old transatlantic relationship. However, we should not underestimate the strength provided by shared principles for democratic governance, rule of law and respect for human rights. These provide the basis to rebuild the transatlantic relationship in ways that promote growth on both sides of the Atlantic and the ability to counter the risks created by the rise of an authoritarian China.

Opportunities for technology policy collaboration between the EU, US and beyond

Martijn Rasser – Center for a New American Security (CNAS), Washington D.C.

Rebuilding trust in American foreign policy among European leaders will be a top priority for the incoming Biden administration. A hallmark of President Trump's China policy was heavy-handed unilateralism, such as the actions against Chinese firms TikTok and the Semiconductor Manufacturing International Corporation (SMIC). Trump's term in office was also often marked by erratic and sometimes contradictory policy pronouncements. A case in point was the varied messaging on the risks posed by Chinese telecommunications equipment manufacturer Huawei and the reason for banning it from US networks. President Trump then stated that Huawei could be part of a trade deal agreement with China, thereby hindering his own officials' efforts to drive home the grave security risks that Huawei poses.

President Trump's rhetoric notwithstanding, a strain of multilateralism had taken root during the latter half of Trump's term in office, in part out of a begrudging realisation that there are few areas where the United States can effectively go it alone. Particularly on matters of technology policy, Trump administration officials had softened prior stances and were engaging more effectively with allies and partners.

American officials reached out to counterparts in Europe and Asia to discuss the viability of 5G open radio access networks – which offer a mostly software-based alternative to proprietary hardware – as a technological alternative to current telecommunications network equipment. The United States joined the Global Partnership for AI, an OECD-hosted initiative spearheaded by Canada and France, after months of protestation. American diplomats proposed a multi-nation Economic Prosperity Network to kickstart supply-chain restructuring and were stitching together a 'Clean Network' coalition of countries pledging to exclude information technologies from untrusted vendors from their national infrastructure. The Trump administration even appeared open to creating new international groupings: in early October 2020, for example, US Secretary of State Pompeo announced his desire to institutionalise the Quadrilateral Security Dialogue, an informal grouping comprising Australia, India, Japan and the United States.

These efforts create a foundation for much-expanded cooperative multilateral efforts on technology policy matters. The ideas that underpin them remain relevant and will continue to influence overall US policy, even though their scope and execution will change under a Biden administration.

Technology policy during the Biden presidency

There is no question that a Biden administration will be very different from its predecessor in tone and style. It is likely to open up new avenues for cooperation, particularly in green technologies. For example, the appointment of John Kerry as climate envoy and the prominence of climate change as a policy priority are clear signs that Biden considers the issue of green technology a national priority and intends the United States to take a leading role in the global response to climate change.

A Biden administration is also likely to take a more strategic and coherent approach to technology policy. In particular, the statements and writings of Biden and key advisors indicate that multilateral collaboration will be front and centre of the administration's foreign policy and technology policy. Biden called for a 'united front of friends and partners' to counteract China's rampant theft of technologies and intellectual property. Tony Blinken, Biden's chief foreign policy advisor and nominee for Secretary of State, spoke of the need for the United States to lead, coordinate and work with leading techno-democracies to counter techno-autocracies like China. Creating new 'trusted communities' of like-minded allies and partners will be an important pillar of this approach.

A Biden presidency will also mean renewed US engagement with and leadership in existing international organisations. Top concerns will be the United Nations and the World Health Organisation (WHO), the G7 and the G20. The United States is likely to focus on shoring up multilateral institutions to counter unwanted Chinese influence and can be expected to engage closely with the European Union and individual European countries as it does so, part of a broader effort to rebuild transatlantic ties.

Europe should expect considerable continuity on US policy goals towards China generally, and on matters of technology policy specifically. Concerns over the China challenge are one of the few areas of bipartisan agreement in Washington. There is broad consensus that the United States – along with like-minded countries around the world – is in a strategic competition with China and that a new approach is in order. Senior Biden advisors Kurt Campbell and Ely Ratner wrote about the need for such a rethink and included the assumptions that underpinned US policy on China for decades. We can expect these, and related writings, to form the intellectual framework for how the United States will deal with China once Joe Biden is president.

While EU leaders should anticipate substantial shifts in US tech policy, the specific contours will take shape over time. The degree of international technology-related policy change under a Biden administration has not yet crystallised for two key reasons. One is a dearth of public information and the fact that the make-up of the administration is still being determined. For example, the Biden campaign did not address its position on issues such as the leadership dispute at the World Trade Organisation or how a Biden administration would engage with the Organisation for Economic Cooperation and Development on digital taxes. Most importantly, the identities of relevant incoming administration officials – the clearest indication of policy direction – are not yet known.

The second determining factor is the balance of power in the US Senate, the legislative body with the most influence over foreign and technology policy and whose members confirm the administration's appointees. Control of the Senate will not be determined until two special run-off elections are held in the US state of Georgia on 5 January 2021. The Democratic Party would reach a 50–50 split in the Senate if it wins both races (with incoming Vice-President Harris able to cast the tie-breaking vote). The more likely outcome, however, is that the Republican Party retains control of the Senate, thereby providing a check on the Biden administration's room for manoeuvre. Influential Republican senators such as John Cornyn, Josh Hawley, Tom Cotton and Marco Rubio will be important voices on US policy towards China, the EU and technology matters. Despite this uncertainty, there remain a wide range of areas for the European Union and the United States to build up a common front.

A common code for collaborative technology policy

The European Union and the United States, as well as other like-minded partners, share major interests that form a solid foundation for multilateral cooperation on technology policy. A group of researchers, of which I was one, from the Mercator Institute for China Studies, the Asia–Pacific Initiative and the Center for a New American Security identified five such areas as part of a comprehensive multi-stakeholder effort to create the blueprint for an alliance framework for technology policy. Several of these areas are complex and expensive; all require multilateral cooperation to be achievable and effective. They are a mix of proactive, affirmative initiatives and necessary protective efforts. The five areas ripe for transatlantic cooperation on technology policy are:

– **Securing and diversifying supply chains.** Efforts to contain the COVID-19 pandemic exposed the brittleness of a range of critical supply chains, while Beijing's attempts at economic coercion underscored the risk of deep interdependencies. 5G rollouts showed the constraints of limited vendor choice. The EU and the US, together with countries such as Australia, Canada, India, Japan, South Korea and the United Kingdom, should join forces to reshape key supply chains. This includes identifying the supply chains where known vulnerabilities pose excessive risks to

a country's well-being; auditing and mapping these supply chains in cooperation with industry stakeholders; and crafting and executing a sensible strategic plan to disentangle and diversify these supply chains.

– **Protecting critical technologies.** Countering the theft and misuse of technologies and associated know-how is a cornerstone of economic and national security. Such actions by China alone cost the EU and US economies many billions of euros each year. Two lines of effort are in order: first, the EU and US should strengthen information-sharing on Chinese technology transfer activities and counterintelligence best practices to build better defences against these acquisition pathways; and the second is preventing the use of technology in illiberal ways. This could include export controls on surveillance technology in China – used to oppress millions in Xinjiang and Hong Kong, for example – and establishing research integrity standards so that know-how imparted by Western academics and researchers is not used for activities that do not comport with liberal democratic values.

– **Creating new investment mechanisms.** An important proactive and affirmative undertaking would be setting up new ways to promote secure digital infrastructure, underpinned by fair and sustainable investment mechanisms. This would provide a much-needed comprehensive alternative to Belt and Road Initiative projects and could be readily applied close by in Eastern Europe and further afield in Africa and the Indo–Pacific. Such an initiative would also help to create a fair and competitive landscape for companies from Europe, the United States and their partner countries.

– **Reclaiming the integrity of international standards–setting.** China is pursuing a strategy to place technologies of Chinese origin at the core of platforms used around the world and to limit reliance on foreign intellectual property. It is doing so in a manner at odds with the intent and spirit of international standards-setting. China's efforts pose a long-term threat to the competitiveness of European and American technology companies and would prevent the EU from achieving any semblance of digital sovereignty. The EU and the United States should work together to safeguard the integrity of global standards-setting by helping to ensure their companies are fully represented, and should call for much-needed reforms to prevent activities such as bloc-voting.

– **Codifying norms and values for technology use.** EU member states and the United States, in cooperation and coordination with their respective private sectors and civil societies, should delineate and promote the norms and principles for how technology should and should not be used. Illiberal use of technology by authoritarian states and the increasing proliferation of these techniques to other countries are direct threats to liberal democracy.

Turning vision into action: a technology alliance

Effective transatlantic collaboration on technology policy will require creative thinking, fresh approaches and initiative. The China challenge is too large and too complex for any one country to tackle. Even the EU does not have the necessary scale or leverage to do so effectively. Instead, tech-leading democracies in Europe, Asia and North America should set up a mechanism to coordinate and collaborate on matters of technology policy.

There is growing interest in and momentum behind such a concept. Proposals include expanding the scope and membership of the Five Eyes partnership, a 'Democracy 10' to tackle 5G and other technology issues, and the proposals from numerous former US government officials for a 'Tech 10' or other alliance frameworks to focus on a wide range of technology policies.

Remarkably, particularly given the hand-wringing over issues such as digital sovereignty, data rights and economic entanglement with China, none of these ideas were being generated in the EU until recently. In late November 2020, however, the *Financial Times* reported that the EU will call on the US to create a new global alliance to meet the strategic challenge posed by China. The draft plan purportedly focuses strongly on the need to bridge divides over tech policy and to collaborate on areas such as 5G.

It is no exaggeration to call this a 'once-in-a-generation' opportunity. This is a critically important development and one that will assuredly be welcomed by the Biden administration and by many members of the incoming US Congress. While crafting such an alliance will be difficult, the potential benefits are great. A new grouping is needed to maximise the economic competitiveness of the European Union and the United States and to ensure the empowerment and security of their citizens.

The German perspective

Bernhard Bartsch and Anika Sina Laudien – Bertelsmann Stiftung, Berlin

Mounting evidence that China is not converging with liberal market economies has led the EU to rethink its relationship with China. Long-term developments have shown that the Chinese leadership is not pursuing the path of deeper engagement and integration based on liberal market-economy principles, it is not implementing promised reforms, and it is neither keeping its WTO promises nor moving towards more openness.

This long-term assessment has been amplified by the COVID-19 crisis, which demonstrated the negative effects of economic overdependence on one single source. The experience of the pandemic has also shown that risks associated with relying on supply chains based in China are not limited to specific crises or supply shocks. China is in a position to disrupt trade and economic interactions for political and strategic reasons.

Reducing these risks is not easy and comes at a price. Globalisation in general and interaction with China, in particular, has brought huge welfare gains and it seems neither possible nor desirable to drastically reduce or eliminate economic ties. Although unpacking Europe's exposure to China is very complex, discussions of this nature are taking place at the EU level and they have already triggered a range of policy responses.

This chapter gives an overview of the state of the debate in Germany as of late 2020. For many years, export-oriented Germany has relied on its so-called 'special relationship' with China, profiting immensely from China's economic rise and its demand for German products. However, in the wake of rising political and economic tensions and considering China's declared technological and industrial ambitions, a wide consensus has emerged that Germany needs to reposition itself *vis-à-vis* China. Getting there, however, is a complicated and often frustrating process. Within the EU, Germany has not always been the driving force or supporter behind more robust policies towards China. This reluctance reflects a domestic debate that has long been dominated by the perception of high economic dependence on China. Lately, this narrative has been increasingly challenged. An assessment by the Federation of German Industries (BDI) highlights the following: although individual German companies and sectors are indeed heavily dependent on China (in particular the automotive industry), the German economy as a whole is not. 900,000 jobs in Germany are conditional on exports to China, which is less than 2 per cent of Germany's entire workforce. While this is a lot of jobs, it is hardly a number that would make Germany dependent. Significantly,

Germany's recalculation of the costs and benefits of the Sino–German relationship was not only triggered by political tensions, but mainly by the growing frustration of German companies and their fatigue over promises regarding a level playing field with China. This frustration led to the now-famous BDI China paper in January 2019, which introduced the concept of seeing China as a 'partner and systemic competitor'.

The BDI paper fundamentally changed the German discussion about China and resonated throughout Europe. In March 2019, the EU Commission expanded this narrative with the triad 'partner, competitor and systemic rival', which has become the standard vocabulary throughout Europe, including in Germany. While German Chancellor Angela Merkel has so far shied away from using the 'rival' description, many other German politicians have adopted the new vocabulary.

Key developments at the EU or national German level in recent years with regard to China include the following:

Investment protection

One reason behind Germany's awakening to the China challenge was the takeover of German robotics manufacturer Kuka by China's Midea in 2016, causing a massive media outcry in Germany. The Chinese shopping spree of European high-tech firms resulted in the EU Investment Screening Regulation of March 2019.[3] In accordance with this regulation, Germany upgraded its investment-screening framework in its Foreign Trade and Payments Act (*Aussenwirtschaftsgesetz*, AWG) and the related ordinance (*Aussenwirtschaftsverordnung*, AWV) was fully applied into German law in October 2020. Beyond this, the German government has announced its next review, which will identify critical technologies of particular (security) relevance, which are now mandatory to filing obligations and scrutiny.

Reforming competition policies

The attempted merger of the railway businesses of Germany's Siemens and France's Alstom, which was ultimately prohibited by the European Commission in 2019, shows some of the European companies' struggle. At home, they are subject to strict competition scrutiny for valid reasons, but they struggle to compete with China's heavily subsidised state-owned enterprises (SOEs) both inside and outside Europe. The German and French governments had strongly advocated for the railway merger and showed

---

3   In the meantime, the framework became fully operational as of 11 October 2020.

their disappointment after the Commission's decision. Germany's Federal Economics Minister Peter Altmaier argued that the EU needs 'European champions' in industry to be able to compete with China and the US.

Unlike the prohibition of the Siemens–Alstom merger, the EU Commission's White Paper on levelling the playing field with regard to foreign subsidies from June 2020 met with great approval in Germany. The White Paper aims to propose new solutions and tools to address subsidies granted by non-EU governments to companies active in the EU, since they appear to have an increasing impact on the European Single Market. The White Paper can be seen as a response to the call from Germany and France in early 2020 for new instruments in competition policy to cope with growing competitive pressure, in particular from China.

Security of 5G networks

Regarding telecommunications infrastructure and the security of 5G networks, the German government has so far resisted pressure to opt for a political exclusion of China's Huawei. Instead of taking a decision early in the debate, which mainly came to Europe because of US pressure, the controversy dragged on for years and even led to turmoil within Angela Merkel's party, the Christian Democratic Union (CDU). As of October 2020, the German government seems to have finally reached an agreement: the draft of the new IT Security Law 2.0 severely restricts use of Huawei components and envisages a two-stage procedure combining technical testing of individual components with a political assessment of the trustworthiness of manufacturers. This is expected to lead to the de facto exclusion of Huawei from any significant involvement in Germany's 5G infrastructure.

Industrial policy

In November 2019, Germany published its 'National Industry Strategy 2030', which aims to preserve Europe's technological sovereignty by improving the economic policy framework conditions for companies and providing greater support for the development of new technologies. The strategy calls for the creation of new instruments to protect the European model of open markets and free trade from distortions of competition by third countries.

2020 should have become a milestone for a German-led EU China policy, as Germany took over the EU Council Presidency in July 2020. The agenda for Germany's EU Council Presidency includes:
– pushing for progress with the Comprehensive Agreement on Investment;
– getting China to do more with regard to climate change and emissions reduction.

The scheduled meeting, originally planned as a bilateral–multilateral summit between Germany and China plus all the other EU member states' leaders in Leipzig (on 14 September 2020) was cancelled because of the pandemic, and a video summit in a reduced version was held instead. The talks did not produce concrete results.

Projects and initiatives by the German government with a strong China reference can also be found in other policy areas. With regard to infrastructure, Germany supports the EU Connectivity Strategy. Launching an 'answer to the Belt and Road Initiative' is part of the German government's coalition agreement of 2018. Besides creating infrastructure for the Global South, the relevance of innovation at home is repeatedly stressed by the German government. Technological competitiveness is seen as the major factor within the systemic rivalry. Germany sees itself as a driving force behind the EU's Horizon 2020, the widest EU research and innovation programme with total funds nearing €80 billion. Germany and France, together with other European partners, initiated GAIA-X: cloud and data infrastructure for Europe. Regarding electromobility, the German Federal Ministry for Economic Affairs started to push for the establishment of battery cell production in Germany and Europe in 2019. To date, the ministry is pursuing two major projects for battery cell production and innovation with the European Commission and other EU member states. The projects are being implemented as so-called 'Important Projects of Common European Interest' (IPCEI), where German companies play an important role. Germany launched a 'National Hydrogen Strategy' in June 2020, but is still far from being a leader in the field and could easily fall behind. Reacting to concerns about academic freedom in China, the German Rectors' Conference in September 2020 released guiding principles on university cooperation with the People's Republic of China, addressing opportunities and risks for academic cooperation with China.

To seek partnerships with so-called 'like-minded' countries, the German cabinet approved policy guidelines for the Indo–Pacific region in September 2020, which aim to deepen cooperation with a wider range of partners in Asia. One declared aim is 'to diversify its relations both geographically and in substance – with a view to avoiding unilateral dependencies', especially in trade relations. At the same time, the new guidelines call for 'closing ranks with democracies and partners with shared values in the region'. The document is carefully worded in order to avoid the impression of being a policy to hedge against China's influence, but it is widely read in this context.

In general, Germany intends to rebalance its economic relationship with China by diversifying its economic ties, pushing for more resilient supply chains and concluding further free-trade agreements. The aim of this endeavour is to become less economically dependent on China. However, it is not easy to reduce dependence on China, or the perception thereof.[4]

Transatlantic China policy

Analysing the above-mentioned policy areas and objectives for commonalities and differences with the United States' China approach, we can state that Germany sees its view on China to be compatible with the American analysis and believes that a transatlantic response to the China challenge is both desirable and feasible. Nevertheless, Americans view US–China relations much more through a geostrategic lens, while Germans primarily adopt an economic competitiveness lens. Yet since there is a shared opinion, specific policy areas should be examined for more transatlantic cooperation and alignment towards China.

When it comes to economic dependence on China, the Trump administration opts for a 'decoupling' from Chinese supply chains. German policy-makers prefer the approach of supply chain 'diversification', seeing a real decoupling as harmful and not desirable at all. They are also of the opinion that global problems, such as climate change, cannot be solved without Chinese cooperation. Here, Europe and the US could coordinate much better concerning a selected decoupling of supply chains from China, based upon a common understanding of future global connectivity structures. The potential for institutionalised mechanisms among ministries and the private sector could be exploited to a larger extent.

As part of China's technology challenge, the US and the EU intend to keep and protect their competitive edge with regard to certain sectors. Also, both see the relevance of setting norms and standards for the use of future technology. However, both players see themselves as competitors and especially the US is perceived by the EU as mainly seeking to protect its own advantage.

Furthermore, both Germans and Americans show concern about Chinese surveillance and technologies for social repression. While the US does not particularly regulate technology, the EU has much more far-reaching and stronger rules that protect personal data (such as the General Data Protection Regulation, GDPR, from 2018) and seeks

---

4   One suggestion is to disentangle systematically the complex relationship with a focus on security risks: see *Exploring a 'green list' for EU–China economic relations* (a study by Bertelsmann Stiftung and Rhodium Group, September 2020).

to shape the ethical development of AI. Chinese techno-authoritarianism could be addressed more effectively if Germany (as part of the EU) and the US passed laws that align regulatory environments for technology companies and technology use on both sides.

The EU has rolled out a new investment-screening regime, but it is up to every individual EU member state to enforce it. In comparison, the US has strengthened its investment-screening mechanism much more significantly. Export controls for the EU and each individual EU member state also diverge considerably from the American export controls regime. This could lead to a transatlantic divergence in various spheres, such as supply chains, technology standards and research collaborations, etc. Efforts could be made to regularise and institutionalise EU and member state screening mechanisms and to consult with the US and other European states on how to unify screening mechanisms as much as possible.

Looking at China's prestige connectivity project, the Belt and Road Initiative (BRI), the US and Germany – as well as the EU – view it with increasing concern. This shared view could strengthen the capacities of their own development initiatives to compete with China's ambitions. Europe has launched the European Connectivity Strategy and the US boasts programmes such as the Blue Dot Initiative. Cooperation could start by identifying ways for jointly financing development projects and expanding development initiatives in order to compete with Chinese offerings such as the BRI.

To find solutions for more common action on China, more transatlantic dialogue and policy coordination are needed. Inter-governmental and non-governmental dialogues concerning China could be institutionalised. At the Track 1.5 and Track 2 levels, there could be more transatlantic exchanges. At the governmental level, this has gained new traction with the announcement of a new EU–US Dialogue on China by EU Foreign Minister Josep Borrell and US Secretary of State Mike Pompeo.

Putting these policy areas and objectives into the wider framework of the multilateral system, Germany's approach differs greatly from the United States' tactic. Germany, for example, together with France, launched the Alliance for Multilateralism as an informal network of states seeking to stabilise a rule-based international order in 2019. Within this framework, Germany tries to find like-minded partners and allies beyond the US. It is looking for partners that share its concerns and are willing to improve the existing order. This Alliance for Multilateralism could become a building block, if it shows real substance and its heads of states push it further, which is not an easy task since the Trump administration has led an American retreat from multilateralism. Since 2016, the US has left the Trans-Pacific Partnership (TPP) and the Paris Climate Accord and withdrawn from several major UN bodies, including the WHO. German and European officials continue to rely on multilateral approaches, reflecting their larger dependence on global multilateral systems.

Germany hopes that the new American administration will re-engage with international allies, partners and institutions to forge broad-based coalitions to deal with the challenges that China poses to all. It hopes that the US will return to its traditional role in multilateral organisations, work closely with Europe to strengthen them and jointly launch new multilateral initiatives that address issues related to China. Furthermore, it currently looks as if discussions on China will be broadened beyond the transatlantic partners to other like-minded liberal democracies, to share assessments and to take common steps.

France's search for greater (European) autonomy in the digital age

John Seaman, Marc Julienne and Françoise Nicolas – Institut Français des Relations Internationales (IFRI), Paris

While France is clearly aligned strategically with the US and is likely to remain so, divergences in managing the digital economy are emerging. At the same time, despite fundamental differences with Beijing, France can ill afford to cast China aside. Ultimately, the concepts of strategic autonomy and digital sovereignty are at the heart of the strategies and policies that France has been developing and promoting for responding to the complex challenges of an ever-more geopolitically charged digital age.

The China challenge and transatlantic friction on the high-tech and digital agendas

When faced with the wide-ranging challenges posed by China, France sees a convergence of views with Washington on the broad political, economic and strategic challenges that China and its growing technological power presents, but divergences over how to go about addressing them. In its confrontation with China, the US has unilaterally moved too hard, too fast and far too broadly for France on areas from trade to investment to sanctions. Paris has also at times questioned whether the motives for such US actions are motivated by Washington's search for a better 'deal' and more privileged access to China's market at the expense of other partners. At the same time, in parallel to the challenges that China presents, rapid technological change has opened rifts across the Atlantic on how to manage digital technologies and their impacts on society, and has highlighted Europe's and France's dependence on the US in the digital high-tech sphere. Three points of friction – on data management, taxation and broader digital governance – are worth noting.

On data management, Europe has entered into structural dependence on the US, wherein 80 per cent of European data are stored or flow through American servers. Rules for data privacy have emerged as a clear point of divergence, wherein France has long sought to establish more robust rules, based on the premise that data privacy is a right, rather than a privilege. This notion has so far materialised in the form of

the General Data Protection Regulation (GDPR), but has failed to catch on across the Atlantic, although signs of possible common ground are emerging from local state-level initiatives such as the California Consumer Protection Act (CCPA), which was inspired by the GDPR.

Another point of friction that has arisen specifically in relations between Paris and Washington is the question of a digital services tax, sometimes referred to in France as the GAFA tax (after the giant American technology companies Google, Apple, Facebook and Amazon). Following a failure of consensus at the European level, in April 2019 the French National Assembly voted in favour of a tax designed to correct what is considered to be a significant practice of tax avoidance on digital services by major US platforms – placing a tax on value where it exists, at the data creation point. Implementation of the law was suspended in early 2020, however, after Washington and Paris reached an agreement, and negotiations for an international accord on digital taxation were brought to the Organisation for Economic Cooperation and Development (OECD).

Finally, some broad concepts underlying digital governance have also proven to be sources of divergence between France and the United States. In general, there is broad agreement with Washington on the need for an open, global and interoperable internet that is respectful of the principles of human rights and democracy. This stands in stark contrast to the concept of internet sovereignty as championed by China, among others. Yet fundamental differences have emerged between France and the US on the interpretation of some of these core concepts. France has advanced the idea of 'digital commons', or the treatment of the internet as a 'common good', and been a staunch defender of 'net neutrality', a concept that all internet communications should be treated equally and in a non-discriminatory manner. ARCEP, the French regulator, has even argued that net neutrality should not only apply to internet service providers, but to mobile and other internet access devices and their manufacturers, including digital assistants. The practice of net neutrality, meanwhile, was struck down by the Federal Communications Commission (FCC) in the United States in December 2017, leaving internet service and access providers to allow for privileged, 'fast-lane' access for certain content through commercial exchanges, undermining the principle of a common good as France would have it. The treatment of internet access as a right and a common good also implies an important role for the state in ensuring such a right, and that internet governance would therefore fall increasingly into classical multilateral governance structures, wherein the role of the state is reinforced. The US (like China, although for different reasons) is staunchly opposed to such a shift. So far, internet governance has fallen back on technical management and has not risen into the domain of high politics, but such conceptual divergences are unlikely to be resolved easily.

Building greater strategic autonomy and digital sovereignty for Europe

Despite the divergences and points of friction, France and Europe are generally well integrated into the US-led technology sphere and widely converge on many of its underwriting principles. At the same time, while French President Macron and French officials have underscored the need for a 'less naïve' approach to China, one based on a more informed reading of Beijing's predatory industrial strategy, increasingly authoritarian political values and the emergence of Chinese 'hegemony' both regionally and globally, France has also sought to remain engaged and even in some areas to strengthen cooperation with China in the field of science and technology. In the face of a deepening rift between the US and China, France seeks to position the European Union and EU member states more independently between an American-led technological universe and other techno-political models, such as China's. In other words, Paris wants to avoid being trapped in a tightening vice between technological dependency on Washington and rising technologically enhanced authoritarianism from Beijing. To do so, France has been actively pushing the concepts of 'strategic autonomy' and 'digital sovereignty'.

5G and Chinese infrastructure providers

France's management of 5G licensing is illustrative of this more ambiguous, less confrontational approach, which also seeks to ensure security and to support European industrial development and competitiveness. France is necessarily cautious towards China, but also seeks to avoid falling into Washington's zero-sum approach. Formally, the French government has not issued a clear stance on Chinese 5G infrastructure providers, and insists on not targeting any company or country. Yet, Guillaume Poupard, head of the French National Agency for the Security of Information Systems (ANSSI), in charge of assessing security risks and delivering authorisation to telecommunications operators, has clearly stated that: 'the risk is not the same with European suppliers like Nokia and Ericsson as with non-Europeans'. Similarly, the French regulator ARCEP also advocated for a strict policy regarding access to the French market for 5G infrastructure providers. As a result, the French government took indirect measures in order to limit Huawei's involvement in the French market. In particular, operators that were already using European solutions for 3G and 4G are not allowed to purchase Chinese technology for 5G. This is the case for the leading French telecommunications company Orange (in which the French state is the majority stakeholder with over 64 per cent), as well as for the smaller operator Free. Operators that were already using Huawei equipment (such as SFR and Bouygues Telecom) are authorised to pursue cooperation with the Shenzhen-based company, but only for durations that vary between three and eight years, without any guarantee of renewal.

Investment screening

The screening of foreign (non-European) investment into strategic sectors has long been a feature of France's efforts to ensure its national security, a definition that also includes economic security. Paris has regularly stepped up its efforts over the last decade through successive reforms aimed at broadening the scope and improving the efficiency of its screening process, the latest of which entered into effect in April 2020.[5] Among a range of sectors now being scrutinised, from the media sector to natural resources, 'strategic sectors' are specifically named as cybersecurity, artificial intelligence, robotics, additive manufacturing, semiconductors, quantum technologies, dual-use technologies, big data storage and energy storage.

While China looms large, American investment pressure has not been absent from the debate on investment screening in France either. For instance, the 2014 investment by General Electric into a branch of Alstom triggered a new round of screening reform. At the European level, Paris had long been pushing for a common European investment-screening mechanism to resemble that of the American CFIUS, since at least 2011. Following a consensus with Germany and Italy in February 2017, France was a key initiator of the process that ultimately led to an EU-wide screening mechanism that, even if only partial, became operational in October 2020. For the time being, there is no 'one-stop shop' in the EU for screening FDI (as exists for merger control), but simply coordination and information mechanisms between EU member states and the Commission.

French national cloud solution

Cloud computing, including data storage, is another area where France has sought to develop a higher degree of autonomy. In France, the first initiative to build a French-based, French-made cloud was in 2012 with the Project Andromède. It gathered several national industry stakeholders, including Dassault Systèmes, Thales and Orange, but the project was then split in two, and eventually ended in failure in 2015.

It was not before 2018 that the 'sovereign cloud' made a comeback in France. So far, the main goal is to develop an economic competitor in the European market to US giants Google, Amazon and Microsoft, as well as the rising Chinese firm Alibaba. Since 2018, the understanding of 'sovereign cloud' has been much more focused on data security. In November 2020, the French government published guidelines aimed at all ministries to implement a cloud solution. This is today supervised by the Inter-ministerial Digital Directorate, under the office of the French prime minister. It is worth noting

---

5   Following the COVID-19 outbreak, the French government added biotechnologies to the list of strategic industries.

that the French Ministry of the Armed Forces is a major actor and driving force in the development of a national cloud solution, since it has particular sensitivity regarding data sovereignty.[6]

Cloud computing is based on a three-layer architecture: the hardware (data centre); the software; and the off the shelf services. France has several stakeholders that it tries to capitalise on to build up a national (or European) cloud solution. For instance, OVHcloud is the European leader and a pure player in the field of cloud hardware, with over two decades of experience. Outscale, a Dassault Systèmes' subsidiary, also provides hardware solutions. In the fields of software and off the shelf services, Atos, Soprasteria and Capgemini are important stakeholders. Thales and Orange, meanwhile, offer global solutions, although it is not their core expertise.[7]

In June 2020, Germany and France together launched an initiative to build a European cloud solution, the GAIA-X Project. It encourages French and German companies to develop solutions according to the driving criteria of transparency, security, interoperability and data portability, with the overall objective of digital sovereignty. In September 2020, France's OVHcloud and Germany's T-Systems (a subsidiary of Deutsche Telekom) accordingly announced they would provide a solution in early 2021.

Redrawing EU competition policy

In the wake of the Alstom–Siemens merger ban, France and Germany tabled a joint 'Manifesto for a European industrial policy fit for the 21st century' that rests on three pillars: pooling resources for 'massive' investment in innovation; adopting defensive measures (such as a European foreign investment-screening framework and a reciprocity mechanism for public procurement with third countries); and making changes to the European competition framework. On the latter point, the objective is to take into account competition at the global level rather than stick to a competition policy that was designed exclusively for the EU's internal market.

In other words, the EU's competition framework should be both more flexible and forward-looking so as to protect strategic interests and address the long-term implications of geopolitical threats such as those coming from China. In the digital field in particular, where Europe lacks home-grown options, it is important to revise competition policy to allow for the emergence of European champions. In France, competition policy is considered as a complement to industrial policy, incorporating a dimension of state intervention as a means to enhance the competitiveness of certain

---

6   Clotilde Bômont, 'Maîtriser le cloud computing pour assurer sa souveraineté', in Stéphane Taillat, Amaël Cattaruzza and Didier Danet (eds.), *La Cyberdéfense: politique de l espace numérique* (Armand Colin, 2018).

7   Interview with Clotilde Bômont.

industries and industrial actors. This is a clear source of divergence with the United States that is increasingly likely to emerge in the future. Indeed, while France has signalled loud and clear its ambition to improve its strategic autonomy and that of Europe in the digital arena, as elsewhere, much will depend on the willingness of the United States to accept a more autonomous Europe and the policies needed to be put in place to get there.

Improving multilateral cooperation with like-minded countries

In parallel with reinforcing resilience and improving digital sovereignty and competitiveness, a major pillar of France's international digital strategy is oriented towards developing open, multi-stakeholder, multilateral cooperation in order to orient the development and governance of digital technologies in a way that better reflects French and European values and interests. This includes reforming internet governance structures with a view to making them more democratic, representative and inclusive, guarding on one hand against the over-dominance of the United States and, on the other, increasing fragmentation of the internet through the emergence of sovereign, national internets (including China's).

France has also sought to develop multilateral initiatives on emerging 'disruptive' technologies, particularly with like-minded partners. One such initiative is the Global Partnership on Artificial Intelligence (GPAI), a joint Franco–Canadian effort born out of the 2018 Montreal Declaration and the successive G7 presidencies of Canada and France in 2018–2019, which seeks to channel a human-centred development of AI. The initiative now includes 15 states and organisations, including the United States.[8] With a secretariat based at the OECD and two centres of excellence in Montreal and Paris, the initiative aims to drive multi-party, multi-stakeholder interactions among industry, civil society, academia and governments in order to guide the responsible development and use of AI and develop work related to data governance, the future of work, and the innovation and commercialisation of AI-related technologies. Ultimately, it is only through such multilateral cooperation among like-minded states and actors, with strong transatlantic cooperation and a central role for the European Union, that digital technologies can develop and be used responsibly, respecting human rights and democratic values.

---

8   Australia, the European Union, Germany, India, Italy, Japan, South Korea, Mexico, New Zealand, Singapore, Slovenia, the United Kingdom and the United States, in addition to France and Canada.

Dealing with China: a Japanese perspective on high-tech and data cooperation

Kazuto Suzuki – Tokyo University, Tokyo

A number of measures have been taken in Japan in the context of China as an emerging threat to Japan's economic security. The Japanese government set up a sub-committee on trade and security in the Industrial Structural Council, one of Japan's powerful expert panels on trade and industrial policies. This sub-committee published a report in 2019 with policy recommendations, calling for comprehensive reform on export control and foreign direct investment control. This was strongly inspired by the new US initiatives such as the Export Control Reform Act (ECRA) and the Foreign Investment Risk Review Modernisation Act (FIRRMA).

The Japanese government takes the issue of economic security seriously and is revitalising its discussions with technical and policy experts. The establishment of an economic security group in the National Security Secretariat (the headquarters for strategic planning for national security policy) in April 2020 (preparatory office was set up in the summer of 2019) was not only a symbolic gesture, but also a demonstration of Japan's seriousness about taking economic security into account. Alongside the National Security Secretariat, Japan's Ministry of Foreign Affairs has also established the New Economic Security Office under the Foreign Policy Bureau.

Offensive and defensive measures

On the offensive, digital transformation was made a top priority on the agenda of new Prime Minister Suga's administration. Suga promised to establish a Digital Agency, which would transform the processes of the national administration and various civic activities, such as licensing or the authorisation of administrative processes, including defence contracts, to be more digitalised. In this process, data security is of paramount importance. The government will establish a special task force within the Digital Agency for cyber and digital security. The establishment of the Directorate on cyber and digital security would focus more rigorously on foreign intrusions on administrative processes. There are a number of reports that Chinese hackers reportedly penetrated the network of Mitsubishi Electric Corporation (MELCO), one of Japan's largest defence contractors,

not only once but twice in 2020, although whether they were state-affiliated or not is not yet clear. The Digital Agency will provide much stronger cyber defence measures to protect these defence contractors and their sensitive technologies. The means of protection are not yet clear, but this sort of cyber protection is one of the highest priorities for the new Digital Agency.

On the question of the diversification of supply and the value chain, the Japanese government has launched a policy to encourage Japanese companies operating in China to come back to Japan. The government will provide financial and logistical assistance for those companies wishing to return. In July 2020, Japan's Ministry of Economy, Industry and Trade (METI) launched a project to provide subsidies to any Japanese companies that want to move their production sites from China. The first batch (linked to Japanese webpage) of subsidies went to 87 companies, with 57 of them returning to Japan and 30 of them moving their production sites to other South-East Asian countries. The second batch of subsidies is granted to 146 companies with strategically important industry, such as semiconductors and advanced materials, from more than 1,600 applications for this subsidy project. Some companies producing household appliances and commodities, pharmaceuticals, optical lenses, and other small and medium-sized companies are granted the subsidies. They may not be strategically important, but some of them produce sensitive products. Applications for this project are open to any companies, resulting in a variety of types and sizes of industry, but the project has so far been a success in facilitating companies with concerns about the potential risk of continuing to produce goods in China.

Regarding defensive policies the Japanese government has amended the Foreign Exchange and Foreign Trade Law (Japan's central piece for export control and economic security) to improve the screening process of foreign investment in sensitive industries. Some news outlets reported that this amendment designates some non-sensitive companies such as a golf course management company, but it was undertaken to prevent the large shareholders of sensitive companies from being acquired by foreign entities. The new regulation requires companies to report to Japan's Ministry of Finance if the foreign share-holding is more than 1 per cent and the ministry may intervene if it has concerns about such an acquisition. The criteria for the designation of companies, which is listed by the ministry, is not clear. There are three groups of companies: (1) 518 companies in 12 core industries (that is, security-sensitive industries); (2) 1,584 companies in 155 semi-core industries (that is, those that may influence security-sensitive industries); and (3) 1,698 companies in non-core industries (although the industry may relate to a security-sensitive industry). The ministry has not announced the reasons for these designations. The Japanese government is also planning to strengthen regulations for land purchases around security-related locations such as military bases, in order to prevent land grabs by foreign entities.

As for export control, the Japanese government is in discussions with experts in emerging technologies such as synthetic biology, quantum computing and encryption, and 3D printing, etc,. about their applications regarding weapon systems or security-related activities. Furthermore, the government has taken steps to improve control over the admission of foreign nationals to Japanese universities, particularly in sensitive research areas. Traditionally, there were guidelines for the admission of foreign students for technologies related to weapons of mass destruction such as nuclear, biology, chemistry and aeronautics, but these guidelines have now been extended to emerging technologies. The METI and Japan's Ministry of Education, Culture, Sports, Science and Technology (MEXT), two rival ministries in many domains, teamed up to form a task force to ensure implementation of the controls over university admission, and they invite the presidents of major universities for further outreach on this regulation.

For data regulation, the Japanese government has launched the idea of 'Data Free Flow with Trust' (DFFT) as the central strategy for Japan's data policy. This concept was proposed by Prime Minister Abe at the World Economic Forum in 2019, followed by his statement at the G20 Summit in Osaka. This concept aims, on the one hand, to enhance cooperation among like-minded countries to share their data for building up 'Society 5.0', while rejecting untrustworthy providers and vendors from this network of data-sharing. It aims to build a multi-dimensional framework for cooperation among states, businesses, academia and specialists to utilise data for the improvement of society and the economy. Under this concept, the Japanese government launched a new initiative to improve data authorisation processes and data security. There is no consensus yet about how to protect personal data, but there are discussions with regard to developing a European GDPR-like protection regulation. Japan has already implemented the Law on Protecting Personal Information, and amendment of this law would be a central issue, but there are growing concerns among the commercial online industry about such an amendment.

The Japanese–American relationship

The goals and approaches of the Japanese government are widely shared with the US. Japan's recent amendment of the Foreign Exchange and Foreign Trade Law was clearly aiming at setting a similar tone to the United States' FIRRMA. Also, recent discussions with regard to strengthening the screening process for foreign students are clearly following the discussions in the United States. The Japanese government is increasingly aware of the Chinese threat to economic security, and the establishment of economic security directorates in Japan's National Security Secretariat, Ministry of Foreign Affairs and the Ministry of Defence is a reflection of such concerns. These new administrative changes also aim at establishing counterparts for the US government.

On the other hand, there are some differences between Japanese and US policies. One difference is concern over vulnerabilities in the supply chain. As noted above, the Japanese government has launched an initiative to encourage Japanese companies to return their production sites to Japan in order to secure the supply chain. Although there was a thought about bringing US industry back to its domestic market under the Trump administration, this was done more by renegotiation of the North American Free-Trade Agreement (NAFTA) or by imposing additional tariff measures. The Trump administration's main ideas on trade do not focus on securing the supply chain, but on employment. On the other hand, the Japanese government provided financial incentives for Japanese companies to return to Japan in order to reduce Japan's dependence on China. These are similar actions, but they have different purposes and objectives.

There is a lot of room for cooperation by Japan, the US and Europe, but in most of the cases, Japan will follow US leadership in the domain of economic security *vis-à-vis* China. However, one area where Japan does try to take the lead is the data-sharing protocol. The idea of DFFT is the flagship initiative of the Japanese government to mend fences between the United States and Europe, where the philosophy of data protection is different. From the Japanese point of view, the US market-oriented approach and the EU's GDPR are not easily reconciled, and Japan therefore wants to provide a third way. It is the Japanese government's belief that DFFT would provide an underlining principle to set the minimum foundation for data cooperation as a countermeasure to China's state-oriented data policy.

The EU–Japan relationship

Japan had an enduring understanding that Europe did not feel the same threat from China and that the EU would have a strong interest in trading with China. However, the recent changes in regulations *vis-à-vis* Chinese products in sensitive domains have changed Japanese perceptions of the EU. The Japanese government began to think that an opportunity exists to collaborate with European states in establishing international norms and rules. Now, since the election in the United States of incoming President-Elect Joe Biden, who is expected to have a stronger preference for international cooperation than his predecessor, Japan considers this an opportunity to establish international norms and rules, instead of bilateral or unilateral regulations, to set standards for protecting domestic industry from China's economic statecraft, for protecting data channelling through 5G network, and for protecting supply and value chains for international production.

The multilateral system

The most important contribution by the Japanese government to the multilateral system regarding high-tech issues is the proposal of DFFT. There is a clear intent that Japan will take the lead in the formation of a data-sharing scheme to counterbalance China's aggressive use of data to develop emerging technologies such as face recognition, artificial intelligence and smart cities. Japan, with the aim of taking the lead in 'Society 5.0', considers big data to be the key for the next generation of industry, and yet with regard to collecting big data, the Japanese population is considerably smaller than that of China. Thus, an alliance with the US, which consists of 350 million people, and the EU, with a population of 550 million, would make it possible to counterbalance China's 1.4 billion citizens, which may have a huge divergence between urban and rural data.

The other area where Japan can contribute to building up European efforts to reshape its policy towards China is the mitigation of vulnerabilities in its supply/value chain. Japan has experienced China exercising its economic statecraft on territorial issues. There was an incident with regard to the territorial dispute between Japan and China in 2010, and China demanded the return of an arrested captain of a fishing boat that was illegally operating in Japan's Exclusive Economic Zone (EEZ) in the East China Sea. China unilaterally halted the export of rare earths, which contain minerals that are critical for manufacturing hybrid cars. The Japanese automobile industry was hit hard by such Chinese measures and Japan recognised the vulnerability of its industrial structure. Since then, Japan has tried to diversify the supply of those critical items from China. In addition, METI launched a new initiative to find further vulnerabilities in the Japanese industry by investigating supply chain cybersecurity. This initiative found that several industries are heavily dependent on supplies solely from China, which may create weakness in cyber protection. This vulnerability-mitigation exercise may contribute to a strategic reorientation of like-minded countries in Europe that are now devising their own policies in this field.

Digital human rights, export control and economic security

The current agenda that the Japanese government is focusing upon is how to bring human rights into the field of export control and economic security. What is happening in China *vis-à-vis* Hong Kong and Xinjiang province is alarming, especially after the arrest of Japanese researchers without a proper explanation. In the last two years, several Japanese researchers and Japanese nationals, as well as Chinese nationals residing in Japan, have been captured by Chinese authorities on the grounds of espionage and other anti-government activities, without properly demonstrating the reasons for their actions. The Japanese government is considering bringing human rights clauses to the exercise of export control, but there is a little experience in this domain. This may require international cooperation with like-minded partners such as

the EU, together with international organisations such as the Human Rights Council of the United Nations.

Another domain requiring change is the restructuring of the export control regime. Traditional regimes such as the Nuclear Suppliers Group (NSG) and the Wassenaar Arrangement take a long time to finalise updating their lists, and often they are not suitable for controlling emerging technology items. For example, 5G telecommunication networks or 3D printing are commonly available on the civilian market, and it is extremely difficult to distinguish them from the military use of these items by using the technical specification. Furthermore, these new technologies are subject to rapid changes, so the traditional methodology of building consensus in the regime is no longer a suitable system for effective control. One solution for these problems is to create a new, small, multilateral gathering of like-minded countries and to establish standards for controlling these emerging technologies.

An Indian perspective

Rudra Chaudhuri – Carnegie Endowment for International Peace
India, New Delhi

India is undergoing a transformation in its relations with China. This process is driven by two interlinked factors: first, the need to reduce India's economic dependency on China, which has been a key objective of Indian foreign policy for over a decade. It has recently been given added impetus because of the United States' 'decoupling' strategy with China. The second factor is China's naked aggression on and across the Line of Actual Control (LAC), which separates Indian and Chinese-held territories along a 3,488km-long and contested border. It is a notional line that has not been delimited.

During summer 2020, the People's Liberation Army (PLA) of China crossed several points on the LAC. These actions led to physical altercations, with fatalities on both sides for the first time since 1967. That China was, and is, the provocateur is without doubt. As of 26 November 2020, Indian and Chinese officials are yet to negotiate a return to a status quo that is acceptable to both sides.

Offensive and defensive measures

These two factors – the need to reduce India's economic dependency on China, coupled with China's aggression on the LAC – have fundamentally altered India's approach to China since early 2020. There is no question of returning to business as usual.

In 2020, the government of India took significant steps towards reducing its economic dependency on China. In April 2020, it announced measures to filter foreign direct investments (FDI) from India's bordering neighbours. Seemingly, this policy was put into effect with an eye on Chinese investment. While this did not stop Chinese investment in India, it added a layer of scrutiny. The new policies prevent takeovers of Indian companies and assets. The Indian government's consolidated FDI policy – announced in October 2020 – forces countries that share a land border with India, such as China, to invest in India through the government route. Investments from China will therefore be examined on a case-by-case basis by government agencies.

The primary reason for gating Chinese investments has to do with the trade imbalance between India and China that overwhelmingly favours the latter. For the past 15 years, China has had every opportunity to invest in India, without any restrictions. China

has been a major investor in India's infrastructure sector, in telecommunications manufacturing and in India's vibrant start-up ecosystem. Tencent and Alibaba have invested in many major Indian start-ups. In turn, China has been unwilling to open its markets to Indian firms. It is this that finally led the Indian government to restrict Chinese investments. The PLA's aggression on the LAC in June 2020 cemented this line of thinking within India.

India banned 59 Chinese apps, including TikTok and WeChat, in July 2020. It banned a further 43 apps in November 2020. While the economic effect of these actions is unclear, what is clear is that for the Indian government, aggression on the border is inextricably linked to limiting China's economic interests in India.

India's relations with the United States

By the end of 2019, it became clear that the trade war between the United States and China was symptomatic of a deeper strategic competition. By early 2020, the wheels completely came off that relationship. As US Secretary of State Mike Pompeo spoke more about a free and open Indo–Pacific, it became clear that this was just a euphemism for the strategic logic underlying the containment of China.

Yet, while India has embraced a close bilateral alignment with the United States, it will not sign into an alliance system against China. Few expect it to. There is, today, a clearer sense in India that cooperating actively in the Indo–Pacific provides a hedge against Chinese aggression. Apart from support from the United States – in the form of sharing intelligence and sensitive information – it is clear to Indian decision-makers that the troubles on the LAC are India's to deal with. Hence, the strategy as far as the United States is concerned appears to be three-fold:

First, India looks to work closely with the United States in the Indo–Pacific. India is committed to a free and inclusive Indo–Pacific. This entails enlarging the structure and meaning of the 'Quad' group of countries, which currently includes India, Australia, the United States and Japan. That India invited Australia to join the Malabar Naval Exercises in October 2020, along with other Quad navies, is significant. In the past, Australia had been excluded from those exercises.

Second, India looks to cooperate with partners such as Japan and the United States to limit the growth of strategic Chinese technologies, such as 5G, that compromise national security. India is likely to limit Chinese firms from auctioning 5G spectrum. Furthermore, India looks to re-scale Chinese investments into India.

Third, India intends to work with the United States and Japan to mitigate the risks of China's growing Belt and Road Initiative (BRI). India, the United States and Japan

reject outright the BRI; they remain in unison as far as not participating in BRI-financed projects.

The Quad countries are aligned on the need to strengthen defence and economic ties in order to unsettle Chinese ambitions. However, they are not in agreement about creating an abiding alliance structure squarely and clearly against China.

This is where India's vision for its relationship with China departs from that of the Trump White House. Once the current crisis along the LAC de-escalates (returning Indian and Chinese forces to the positions they occupied in March 2020), India may leave room for re-engaging with China. This does not mean that the contours of such engagement will return to those in force before 2019–2020, but it does mean that, in all likelihood, India will seek a form of engagement that rebalances a large trade deficit with China, limits but does not end Chinese financing into India, and at the same time redesigns deterrence strategies to deal with the PLA's increasingly aggressive postures along the LAC. When and if the immediate border crisis subsides, a degree of economic re-engagement can be expected. Yet given China's aggressive posture on the LAC, it will mean that a lot more kinetic activity can be expected on the border in the coming years. Fighting, trading and talking might just become the conceptual arch shaping India's new advance with China.

If this is the case, Joe Biden's US electoral victory might be very good news for India. From all accounts, there is growing bipartisan support within the United States to continue the deep competition with China. The Biden foreign policy team are very well acquainted with India and Indian leaders. Under Biden, economic and political engagement is likely to be a crucial part of a better and more effectively designed strategy to deal with Xi's China. This, it would appear, is in keeping with India's own self-designed approach to deal with China in the long-term: engage, but with many added layers of scrutiny and caution.

India's relationship with the European Union

The central problem with the EU's approach to China, from an Indian standpoint, is a structural one – the EU does not speak with one voice. This means that the EU will have an uneven view when it comes to dealing with China.

Many EU member states have woken up to the strategic challenge posed by China, especially since 2018, when Xi Jinping became 'president for life'. That European countries like France and Germany have limited or eliminated the potential of Chinese-built 5G technologies is significant. Investment screening is becoming more of a norm rather than an exception across the EU. Developing an Indo–Pacific strategy (such as

the one announced in 2020 by Germany) is increasingly a central aim of EU member states.

However, and at the same time, there are several EU states that have embraced the BRI. They remain compromised, in one way or the other, in their dealings with China. What the EU – as a collective – wants in its relations with China remains less clear. Furthermore, while EU member states consider articulating individual visions for the Indo–Pacific, it is still unclear whether or not the EU as a whole will be able to do so any time in the near future.

That said, there is enormous opportunity for cooperation. The EU and India can, and should, focus on three imperatives. These imperatives might be enablers that set out a clearer rationale and need for aligning the EU and India's advance in the future.

First, it is important to conclude a trade agreement that has been stuck on five or six key points of debate for many years. The EU Commission needs to overcome administrative hurdles, re-evaluate what is on the table and, for the sake of impetus, find common ground. Equally, India needs to meet the EU half-way. It can do so more easily by discovering a strategic logic that drives these hard-fought and often tiresome negotiations. The key strategic logic is simple: that better working relations between the EU and India ensure greater multilateralism in a multipolar world. Broken working relations do little more than further fragment the uneasy multilateralism that exists today.

Second, there is much that the EU and India can do to strengthen technology relations between their two jurisdictions. This would help start-ups and technology companies to co-invest in each other's futures. Both the EU and India could work more closely in dealing with sensitive and emerging technologies such as blockchain and AI. They could find common ground in designing standards that are compatible with each other's social and democratic make-up. For instance, they could consider common standards for facial recognition systems and the ethics of using machine-learning tools. None of this will be easy. The EU has what might be considered an unnecessarily burdensome General Data Protection Regulation (GDPR). The EU's standards for data-related agreements (also called data transfer agreements) are such that they are designed for Europe but not for partner states that are evolving their own unique standards. By 2021, there is a very good chance that India will have its own data protection law. There are bound to be areas of divergence between what the EU Commission expects from the Indian law and what the legislation will actually entail. Rather than data becoming yet another long-held area of dispute between the EU and India, such as trade, it is imperative to begin early negotiations to ensure cooperation. The EU and India must find common ground on their respective legal treatments of data. For the EU this will be crucial; after all, India is and will remain the largest open data market in the world.

Third, continuing cooperation with the EU and India on the future of the Indo–Pacific will be crucial to syncing efforts in Europe with those evolving strategies in India. To date, four EU countries have committed themselves to an Indo–Pacific vision or guideline. Potentially, in the next few years, more and more EU member states will look to articulate publicly their own positions. Yet EU member states have limited military capabilities to ensure a free and open Indo–Pacific. Hence, the actual terms of cooperation between India and the EU need to be clearer, setting the right expectations of what each side can actually deliver in the Indo–Pacific.

The multilateral dimension

In January 2021, India will become a non-permanent member of the United Nations Security Council. In 2022, it will chair the G20. In each of these forums, India will look to place its own impression on the future architecture of global politics. It is likely to do so in the following four ways. First, it will continue to support the Paris Agreement. It will embrace the United States' return to the treaty. Yet, and as much as climate change is a matter of theological proportions for President-Elect Biden, there will need to be a balance of expectations of what performers like India can and cannot do. As for the EU, the main concern has to do with the green deal. Setting unrealistic standards for manufacturers and suppliers in India who work with the EU will do little for either EU–India relations or the need for actionable climate change policies.

Second, at the G20, India can be expected to take a unique position on digital taxation and the free flow of data. India has refused to join the DFFT (Data Free Flow with Trust). Insiders in the Biden campaign zealously advocate for the free flow of data across borders. Trump supported the free movement of data for purely commercial reasons. The Biden administration is likely to do so for the ease of business, but also to set global norms on the movement of data. India will resist this. India has already commandeered payments companies to localise data within India's borders. While there is little likelihood of harmony among the EU, US and India, there is every potential to find minimum common denominators in the global management of data. Indeed, the process of finding these denominators might turn out to be much more rewarding than the actual end state.

Third, Biden is committed to abiding by general rules of the international trade game. He is expected to lower tariffs, end the trade battles with Europe, and work with and for allies such as Japan and South Korea. India, given its own need to recover from long-struggling economic woes, is unlikely to embrace free trade. India's decision in 2019 to stay clear of the Regional Comprehensive Economic Partnership (RCEP) is only indicative of its free-trade's advance. The state of the economy was certainly one reason for India's exit from RCEP. What is clear is that this is a wide-ranging area of

multilateralism, where challenge and contest are likely to dot the near future. Alignment will be difficult if not impossible.

Concluding remarks

There is a fundamental shift in India's approach to China. In the near future, and for the reasons illustrated above, India can be expected to rely a lot more on greater economic ties with the EU and the United States as it lowers its dependence on China. This means that India will look to the EU and US to find a greater set of convergences, with an added zeal and effort. In the case of the United States, the path to strategic convergence is almost pre-ordained. The two countries are closely tied on almost every bilateral aspect of the relationship. With the EU, there is much more that can be done to realise potential in a relationship that will, in time, serve as the levers that shape a reforming multilateral system.

Do not box us in! Australia and its approach to dealing with China in areas of technology

Bart Hoogeveen – ASPI, Canberra

In 2017, Australia's Foreign Policy White Paper predicted a decade of unprecedented change with globalisation, technological change and new forms of production, consumption and trade, wherein Australia should expect to see its values and ideas increasingly challenged.

Few anticipated, however, the state of Australia–China relations to deteriorate as rapidly as it did. A vicious circle of responses, counter-responses and over-responses since 2018 have led to a situation of Australian government ministers being denied direct access to their Chinese Communist Party (CCP) counterparts; a boycott of key export products and increased tariffs;[9] and the last accredited reporters of Australian media outlets having left China in fear for their personal safety.

Australia is seen as a testbed for the CCP's approach to dealing with liberal economies, and leaders in the US and Europe are carefully watching Australia's balancing act with Beijing.

Despite American attempts to force Australia's hand (it is a choice between 'freedom and democracy, against tyranny and authoritarian regime', said US Secretary of State Pompeo), Australia's Foreign Minister Marise Payne in July 2020 insisted at their bilateral US–Australia meeting in Washington DC that she did not want to injure relations with China unnecessarily. The recent EU–Australia Leaders meeting of November 2020, however, stands in sharp contrast, where both delegations discussed a wide range of regional issues, including those in which *also China plays a role*, with technology issues at the bottom of the agenda.

---

9   In May 2020: beef and barley; in November 2020 an informal announcement by China's President Xi to stop importing sugar, barley, red wine, timber, coal, lobster and copper from Australia, followed by a 'list of grievances' shared by the Chinese Embassy in Canberra.

This chapter looks at how Australia deals with China in technology affairs. Alternately in the shape of coalition, cooperation, competition and conflict, the chapter looks at defensive measures, technology issues and Australia's tech diplomacy, while comparing Australia's practices with those of the US and Europe.

Defensive measures

The Australian governments under Liberal Party Prime Ministers Turnbull (2015–2018) and Morrison (2018–present) introduced new initiatives addressing foreign interference and the protection of critical information infrastructure. In addition, the 2020 Defence Strategic Update includes a ten-year commitment of AUD 270 billion to augment Australia's autonomous defence capabilities, supplemented by a national cybersecurity strategy.

While these policies and legislation are technically country-agnostic, they are seen as a response to CCP-instigated actions against what Australia sees as its democratic values, prosperity and rightful place in the Indo–Pacific, and they mirror similar steps taken in the US, coordinated through the Australia–US Ministerial Consultation (AUSMIN) mechanism.

Two eye-catching government decisions – which touched nerves in Beijing – are the Espionage and Foreign Interference Act and the decision to ban Chinese vendors from competing in the development of 5G infrastructure in Australia, both from 2018.

Countering potential interference, espionage and coercion

The Espionage and Foreign Interference Act (EFI) provides an update to Australia's legal framework for conducting counter-espionage activities. Among other things, EFI introduced the Foreign Influence Transparency Scheme and added the crime of stealing trade secrets on behalf of a foreign government and causing damage to critical infrastructure where it could jeopardise national security, for instance by leaving a system vulnerable to future misuse or exploitation.

This regulatory push inspired a review of at-risk sectors. The Australian universities are such a sector, after they were found to be engaged in high-level forms of collaboration with researchers affiliated with the People's Liberation Army, in particular in areas covered by China's military–civil fusion strategy. Subsequently, Australian universities and the Australian government worked together to provide 'guidelines to counter foreign interference in the Australian university sector'.

Australia's decision to ban Chinese vendors from competing for 5G infrastructure kicked off reassessments of, in particular, the use of Huawei equipment in countries worldwide.

Huawei had previously been banned from competing for Australia's national broadband network for reasons of protecting the integrity of Australia's information infrastructure, but this time the Telecommunications Sector Security Reforms (TSSR) were invoked.

The security obligations included in the TSSR, which took effect in September 2018, must protect networks and facilities from unauthorised access and interference. Huawei and other China-based vendors are subject to the CCP's National Intelligence Law and therefore, according to the Australian government, constitute a risk that they 'are likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law'.

Similar considerations are currently brought up with respect to Chinese social media platforms. A platform such as TikTok asserts that Australian user data are stored on servers in the US and Singapore, while intelligence services reportedly assess TikTok's parent company ByteDance as at risk of being forced to hand over data to the Chinese authorities.

Strengthening the defence portfolio

The 2020 Defence Strategic Update signals additional measures of Australia putting up its technology fences against China's attempts at interference, espionage and coercion. It includes an uplift of AUD 1.4 billion for the Australian Signals Directorate, which is responsible for Australia's foreign signals intelligence, the national cybersecurity centre, and for providing offensive cyber capabilities to Australian law enforcement and armed forces.

The Defence Department is also responsible for the implementation of the 2012 Defence Trade Control Act and the Defence and Strategic Goods List (DSGL), which includes all goods and technologies that are controlled by export regulations. The 2012 update of the Act was initiated after the US Congress expressed reservations about 'intangible transfer and the brokering of controlled goods, technology and services' before it would ratify the 2007 Australia–US Defence Trade Cooperation Treaty.

With increased reporting about China's application of high-end technologies to suppress ethnic minorities, commit human rights violations and conduct foreign espionage, Australian authorities are showing growing apprehension about the use of artificial intelligence and surveillance technologies *inside* Australia too. The domestic use by governments of devices manufactured by Chinese companies like Hikvision and Dahua have has been reviewed after US Congress banned the use of products by these companies. In December, the Human Rights Sub-committee of the Australian Joint Standing Committee on Foreign Affairs, Defence and Trade issued a report (with contributions from Estonia, Lithuania, Netherlands, US and Canada) suggesting a

stand-alone law that would address human rights violations and corruption, similar to the United States' Magnitsky Act 2012.

Cohesion in Australia's multi-level system of governments

Australian states and territories hold a substantial degree of autonomy, and this has led to two situations where states have entered partnerships with China, notwithstanding federal policy.

In 2018, the Government of Victoria signed a memorandum of understanding with China on cooperation within the framework of the Belt and Road Initiative (BRI), with a focus on 'growth in knowledge-intensive industries and services'. Earlier, in 2015, the Government of the Northern Territories leased the port of Darwin for 99 years to Landbridge, a subsidiary of Shandong Landbridge Group. Although operating from another port, Darwin is a strategic location for the Australian Defence Force and allied militaries.

In response to these developments, the Australian parliament passed a new law that establishes a process whereby the (Commonwealth) minister of foreign affairs can override state or territory arrangements with foreign states if they assess the effect of these arrangements to be detrimental to Australia's foreign relations and a consistent foreign policy.

Examples abound of sub-national jurisdictions stepping out of line with the national or federal government. However, these do not tend to touch upon a sensitive issue like the bilateral relationship with China, and do not involve a foreign actor so apt at exploiting a seeming lack of internal cohesion.

Like the 5G debate, the 'State and Territory Arrangements Bill' may inspire entities like the EU to explore a similar course of action when aligning individual EU member states. In fact, internal solidarity has been the *leitmotif* of the Association of South-East Asian Nations (ASEAN) in its strategy to counter potential attempts by outside powers to play out differences.

Offensive measures and technology issues

At a time when technological development has become a matter of geopolitics, a posture of sheer technology-taker is no longer viable. However, the current state of Australia's technology ecosystem is characterised as fragile, which is not helped by the Australian government's siloed approaches in the national security, industry development, and education and R&D portfolios.

While Australia has shown an ability and willingness to take an autonomous approach to defensive measures, R&D, technology exports and natural resources critical to technology products are a different story. Here, Australia is competing with like-minded partners to gain access to China as a technology partner and investor.

Promoting education, research and development

Australia's higher education sector provides the third-largest source of export income. In 2019, Chinese students brought in approximately AUD 12 billion, which constitutes a revenue stream of over 20 per cent for some universities. This dependence on a single source of overseas students is higher than any academic institution in the US or Europe.

With public spending on R&D in decline between 2009 and 2018,[10] Australian science and technology institutions have been encouraged to engage in international partnerships, including through an instrument like the Australia–China Science and Research Fund (ACSRF).[11]

Australian researchers now have a comparable degree of collaboration with China as with the US. Europe, including the United Kingdom (UK), is still Australia's largest science and innovation partner. Collaboration with China concentrated on physical sciences (astronomy, chemistry, earth sciences, mathematics and nanotechnology), and with the US on life sciences. Defence technology is exclusive to the Five Eyes countries (Australia, the US, UK, New Zealand and Canada) and cooperation with the EU concentrates on climate change, disaster risk reduction and sustainable development, as well as space technologies.

While academic and research sectors have a large stake in collaboration with China-based partners, Australia's national research agenda has remained diverse and largely reciprocal in nature.

Growing a technology export market

In 2019, only 1.1 per cent of Australia's total exports were related to technology. Despite close university linkages with partners in both the technology powerhouses of the US and China, Australia remains predominantly a 'spectator rather than a participant in technological innovation'.

---

10   From 2.25% of GDP in 2009 to 1.79% in 2018 (note that the OECD average is 2.37%).

11   The ACSRF is jointly managed by the Australian Department of Industry, Science, Energy and Resources and China's Ministry of Science and Technology. Key work includes joint research centres, workshops, seminars and symposia, and the Australia–China Young Scientists Exchange Programme.

The last few years have seen several policy initiatives from Australia's Department of Industry, Science, Energy and Resources, including the AI Action Plan (2020), Australia's Tech Future (2018), the Global Innovation Strategy (2016) and the National Innovation and Science Agenda (2015). International partnerships are actively promoted, with an accompanying catalogue targeting 'foreign governments, businesses and researchers who are interested in finding partners and collaborators in Australia'.

Nonetheless, Australia is seen as lagging behind nations such as the US, UK, France, the Netherlands, Ireland, Singapore and South Korea in promoting local technology and innovation sectors. Unlike the US or the European Union, Australia lacks a homegrown market that creates sufficient 'demand' and economies of scale, and therefore relies on diversity in markets for the import and export of technology products.

Exploring critical minerals

A recent addition to Australia's perspective on technology is the market for critical rare-earth minerals.[12] China currently controls 80–90 per cent of the extraction and production processes of rare-earth elements. When President Trump decreed the US should be less dependent on China, market prospects loomed for Western and Northern Australia, two states that are rich with mineral resources.

Australia's subsequent Critical Minerals Strategy (2019) encouraged overseas partners to invest. Chinese parties are all but excluded, although their financial depth, processing and marketing expertise, as well as market demand would, in fact, help to solve the underdevelopment of Australia's current critical minerals' market. For the moment, however, Australia has formalised partnerships with India, the US, South Korea, Japan and Canada.

Australia's cyber and tech diplomacy

In 2017, Australia's Department of Foreign Affairs and Trade (DFAT) recognised the need for a coordinated conduit when it established an ambassadorial role for cyber affairs and later added critical technologies.[13] Australia remains one of the few countries with

---

12   Rare-earth elements are needed for many modern high-tech products, such as batteries, computers, smartphones, hard drives, lasers and other devices.

13   The position of Ambassador for Cyber Affairs was created in 2017, based on the example of the cyber coordinator at the US State Department. Since then, many countries have followed this example, in particular many European nations. In 2020, the ambassador's mandate was expanded to include 'critical technologies', partly inspired by the Danish Technology Ambassador, an envoy to the Silicon Valley-based tech sector in the US.

a central coordination point for international engagement on cyber and technology diplomacy.

Situated in the Indo–Pacific region, Australia engages in what could be described as three distinct spheres of diplomatic gravity. China's posture and technology play a pre-eminent role in each. This section now looks at these three spheres of external engagement.

Australia's global leadership

The first sphere includes other (highly) developed nations and, in particular, the Five Eyes partners, as well as South Korea, Singapore and Japan.

The Australia–US coalition runs very deep, irrespective of which administration occupies the White House. On issues of countering foreign interference, defence technology development and risk perception, Canberra and Washington see eye to eye. Related Australian laws, regulations and policies regularly refer to, or were inspired by, comparable US legislative initiatives.

Conversations with the other developed nations are dominated by the need to protect the rules-based international order, alongside democratic values and institutions. To manage the peaceful use of technologies, Australia and its partners advocate an approach based on 'norms of responsible behaviour of states', grounded in a recognition that international law applies. Australia also makes a point of being transparent about states' use and application of technological capabilities.

Australia's success in rallying support from European nations, the EU and NATO, as well as from Japan and South Korea, around the (political) attribution of malicious cyber incidents shows how Canberra is investing in building deeper levels of collaboration in intelligence-sharing, technology exchange and norm-setting with this group of partners.

Regional coalitions with ASEAN in the centre

The second sphere of gravity are countries in South and South-East Asia. As dynamic and emerging economies with strong governments, these are considered swing regions between a more liberal and a more authoritarian approach to the use of technologies, and Australia has managed to bolster relations with countries such as India, Indonesia, Japan and Vietnam. More than the US or EU, Australia is perceived by its Asian partners as being similarly on the receiving end of China's actions.

This regional and pragmatic approach reflects Australia's deeper reappraisal of global multilateralism. As with successive US administrations, there is a growing preference

for mini coalitions of able and willing partners when it comes to issues of high politics, despite South and South-East Asian nations remaining non-aligned states.

The Quadrilateral Security Dialogue (known as the Quad) with India, Japan and the US has especially grown in prominence. The few overseas trips by Australian (prime) ministers during the COVID-19 pandemic were in fact to Japan, the US and ASEAN states, and Australia and India in June 2020 signed agreements on cooperation in critical technology and on critical and strategic minerals.

Institutionally, ASEAN is central to Australia's regional security approach. In November 2020, Canberra pledged AUD 555 million to support the Mekong countries '[developing] critical technologies, including 5G networks'. This contribution to the Mekong region's post-COVID-19 economic recovery is also an attempt to prevent 'South-East Asian countries being pulled into Beijing's orbit through sheer force of economic gravity'.

In contrast, the US relationship with ASEAN has been less steadfast and described as 'transactional'. The European Union, albeit with a much lower profile, and individual EU member states like France, Germany and the Netherlands are similarly putting their eggs in the ASEAN basket. They regard ASEAN as the prime custodian of regional security, including on matters of information and communications technology (ICT) security and of regional digital infrastructure development.[14]

Maintaining a Pacific footprint

The South Pacific represents Australia's third sphere of diplomatic gravity. Australia is traditionally the dominant regional actor, but recent years have seen activities in trade, diplomacy, commerce and aid by the PRC increase gradually but significantly.

In the context of reaching the UN Sustainable Development Goals, Australia (and New Zealand) has been supporting connectivity and digital transformation projects on many South Pacific islands. China, instead, has been providing state bank loans to deliver (relatively) large infrastructure projects such as communications systems, data centres and other information infrastructure.

Australian and Chinese interests came to a head in 2018 when the Solomon Islands and Papua New Guinea were about to sign a deal with Huawei to lay a submarine fibre-optic cable. Not wanting such piece of geo-economic infrastructure in Chinese hands, Australia committed to financing the Coral Sea Cable System instead.

---

14   See the recent French, German and Dutch Indo-Pacific Strategies.

This created a precedent. In October 2020, Australia, the US and Japan announced financing for another cable, this time connecting Palau to the trans-Pacific link between Singapore and the US. And in May 2020, when China Mobile was suspected of taking over Digicel, a major telecommunications service in the Pacific, the Australian government signalled that it would consider stepping in too.

Conclusion

Australia and Europe have both attempted to keep innovation, trade and technology separate from security and defence issues in their relations with Beijing. It is unlikely, however, that this approach will be viable for much longer, as terms like rivalry, competition and coercive interference are entering the official discourse.

Australia's hedging strategy on the technology front may open up prospects for stronger Euro–Australian collaboration.[15] Renewed interest in the Indo–Pacific by France, Germany and the Netherlands has been welcomed by Canberra. Nonetheless, Australia is sceptical of global multilateralism and would expect Europe to follow up with tangible and meaningful deeds. Moreover, Brussels' digital sovereignty narrative suggests a risk to Australia's nascent tech economy if it goes beyond diversification of technology supply chains.

Australia is 'only' a middle power, but its strategic location, policy preferences and political weight position Australia as a norm-setter and strategic partner in the Indo–Pacific and around niche global policy areas. Technology affairs clearly represent such a niche area.

Europe and the US would benefit from keeping a close eye on developments in Australia and understanding the various pull-and-push factors in its relationship with China. Australia also houses one of the largest concentrations of China expertise and language skills. The US has recognised this, among others through a large diplomatic presence with a broad reach into Australian organisations, whereas the European effort remains unconvincingly coordinated and lopsided towards areas of 'low politics'.

---

15   'Is there a place for Europe in Australia's post-COVID outlook? A unified approach to China: opportunities for EU–Australia partnership', in: *After COVID-19, volume 2: Australia, the region and multilateralism* (ASPI, September 2020).

Reflections: towards a transatlantic approach to dealing with China?

Brigitte Dekker and Maaike Okano-Heijmans (editors) –
Clingendael Institute, The Hague

An oft-heard observation in Europe in recent years was that European capitals and Brussels share US concerns about China's growing technological prowess, but not its approach. At the same time, President Trump's policies have frequently been described in the US as 'right diagnosis, wrong prescription'. Taken together, this may give rise to the idea that the transatlantic woes on 'dealing with China' in the trade–tech–data sphere will naturally fade with the upcoming change in administration in Washington.

Unfortunately, the eight chapters bundled in this report suggest otherwise. The contributions from six countries – namely, the United States, Germany, France, Japan, India and Australia – reveal diverging views on China, as well as preferred responses. Taken together, the expert reflections suggest that opportunities and willingness for more transatlantic cooperation with like-minded partners in the trade, technology and digital domain certainly exist, but the eight chapters also caution against high expectations for quick fixes.

This concluding chapter reflects on the findings of the various expert contributions.[16] First, it details the varying trajectories of the six countries studied, concerning their 'diagnosis' of China's growing role and influence, as well as their 'prescription' for how best to deal with it. This clearly shows that while European perceptions have certainly evolved, they have not changed as fast as in the United States, which was several years 'ahead' of Europe in the first place. Also, they are not on the same page as Australia, India or Japan.

---

16 The various figures in this conclusion are based on the analysis presented in the preceding chapters, and have been verified by all contributing authors. Reference to the EU is based on analysis in various chapters as well as on earlier work by the authors of this conclusion on export control; industrial policy 2.0 and economic security (in Dutch); and EU/NL digital connectivity.

Aiming to identify fields where cooperation is more (and less) feasible, this chapter's second section then summarises the various countries' positions on (enhancing) defensive and offensive instruments for dealing with China. Defensive instruments include oft-discussed tools like 5G and FDI screening, but also stretch to the newer domains such as cybersecurity, the platform economy and data protection. Separately, offensive tools range from innovation and reorganisation of supply chains, to standard-setting and digital rights.

Finally, this chapter discusses two key obstacles to enhanced cooperation in the trade, technology and digital fields that emerge from the chapters: (perceived) protectionist tendencies; and the normative dimension that revolves around trade-offs concerning business interests, individuals' interests and state security in technology governance. It also summarises key recommendations emerging from the chapters for European capitals, as they search for new ways to deal with China together with key partners and in the international system. Addressing differences in the problem definition, approach and prioritisation; improving mutual understanding of the relevant institutional and political domestic context; and learning from partners will be key to enhancing much-needed synergies and cooperation.

Diagnosis and prescription

The chapters in this report provide valuable insights into the varying trajectories of the six countries under study, regarding each country's assessment of China's behaviour and their preferred responses to this. Until just a few years ago, France, Germany and the EU as a whole took a very positive approach towards China, with few limits to engagement. The economic opportunities outweighed possible national security threats, and this was amplified by the geographical distance and strong internal focus of the EU. Notably, all other countries included in this report start from a less open position – that is, a position of or close to conditional engagement – and have long assessed China's behaviour as assertive or even aggressive.

Figure 2   Diagnosis and prescription: assessment of China's behaviour and the preferred response of various governments
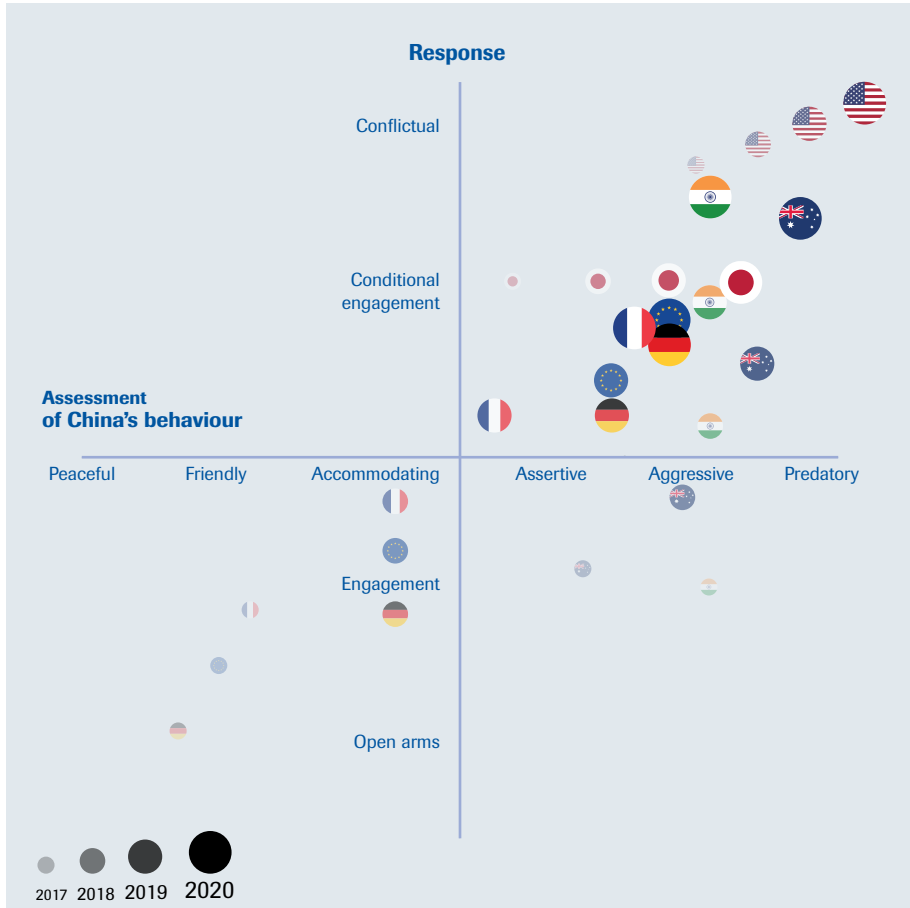
Today, there seems to be a strong consensus on conditional engagement with China, wherein cooperation is not ruled out but care is taken not to align one's own priorities with those of the Chinese government or the Communist Party. Also, all the countries in this study now consider China's behaviour as somewhat aggressive. However, as both the starting points and intensity of change differ, current stances obviously still vary. The US stands in lonely distance from the other countries, (publicly) assessing China's behaviour as predatory and taking an outright conflictual approach. As the next section shows, preferred responses vary between the countries.

Defensive measures

Defensive measures, as outlined in Table 1 below, are predominantly based on long-held political philosophies and practices. The systemic challenge that China now poses, however, is inducing more rapid change on countries than seen in previous decades. These changes may be assessed by way of a scale that shows where the introduction of specific instruments and regulation stands – ranging from absence, consideration, initiation, implementation or policies in place, to the improvement thereof. This assessment builds on existing regulations; in other words, change concerns a revision of existing regulations (as of 2020) to match new economic and national security threats, and does not suggest that no regulation had been in place earlier. For example, all of the countries in this study have long had export control systems in place, and our focus here is on the extent to which this is now being updated.

Table 1   Countries' positions on defensive measures

Defensive measures	Absent	Awareness	Considering	Initiating	Implementing	In place	Improving
5G		🇪🇺*	🇩🇪 🇫🇷			🇦🇺 🇮🇳 🇺🇸	
Cyber security		🇪🇺*	🇩🇪	🇫🇷	🇮🇳	🇦🇺 🇯🇵 🇺🇸	
Export control		🇬🇧 🇮🇳		🇩🇪 🇯🇵		🇺🇸	🇪🇺
FDI control		🇪🇺*			🇩🇪 🇫🇷	🇦🇺 🇺🇸	🇮🇳 🇯🇵
Platform economy	🇯🇵		🇦🇺 🇩🇪		🇺🇸	🇫🇷 🇮🇳	🇪🇺
Academic openness		🇪🇺*	🇫🇷	🇩🇪	🇺🇸	🇦🇺 🇯🇵	🇮🇳
Data protection			🇺🇸		🇮🇳	🇦🇺 🇩🇪 🇪🇺 🇯🇵	

* Note that the EU does not have competence to act in all fields.[17] Where it is nevertheless acting to push EU member states forward, the EU is here categorised under 'awareness'.

Several defensive measures have been high on Washington's agenda in recent years. From 2018, the United States' strong focus on tariffs was expanded to include also other defensive measures, such as export control and 5G. Although Australia was first to publicly cite the risk of having equipment of untrusted vendors on 5G networks and to ban Huawei, the US has been most vocal on this point – putting significant pressure on all its allies to ban Huawei from (core) 5G networks. France and Germany are still considering their desired proportional response towards China, while Japan and India, for their part, are phasing out Huawei infrastructure.

---

17   More on this in the concluding section 'Lessons for Europe'.

Two other defensive measures stand out in particular: push-back against the big-tech platform economy; and data protection. With regard to regulation of the platform economy, governments are taking defensive measures in various forms and to various extents. As the French chapter in particular shows, the EU tends to focus on the US big-tech companies – especially Google, Apple, Facebook, Twitter and Amazon. This shows the EU's rapidly changing attitude and diverging stance with respect to technological sovereignty and strategic autonomy *vis-à-vis* the US. As William Reinsch notes, a similar level of concern has yet to be expressed about Chinese companies such as Alibaba, ByteDance and WeChat.

With regard to data protection regulations, EU member states and businesses, both inside and outside European borders, processing data from European citizens have to adhere to the General Data Protection Regulations (GDPR), which are considered strict in comparison to all other data protection regulations globally. Japan and the EU aligned their positions in this respect, as illustrated by the Adequacy Decision of 2019. As James Lewis points out, privacy regulation may be an opportunity for transatlantic partners in 2021, as US regulators are catching up with Europe on privacy regulation. Like India, however, the US will not 'slavishly' adhere to the GDPR, and flexibility on both sides is still required for agreement on how to govern technology.

Cooperation with India could also be enhanced concerning data-sharing and finding common ground in designing standards compatible with each other's social and democratic make-up, as Rudra Chaudhuri points out. India, like other countries, considers the GDPR as an unnecessary burden and not compatible with its partners' own data protection mechanisms. In order to cooperate with India after the introduction of the 2021 Indian data protection regulations, Chaudhuri argues, '*It is imperative to begin early negotiations to ensure cooperation. The EU and India must find common ground on their respective legal treatments of data. For the EU this will be crucial; after all, India is and will remain the largest open data market in the world.*'

Offensive measures

As well as defensive measures, all of the countries have invested in offensive measures, which are set out proactively to push forward certain concepts, ideas or actions to enhance a country's status.

Table 2   Countries' positions on offensive measures

Offensive measures	Absent	Awareness	Considering	Initiating	Implementing	In place	Improving
Innovation					🇦🇺 🇮🇳		🇩🇪/🇪🇺 🇺🇸
Digital transformation					🇦🇺 🇨🇳 🇯🇵		🇩🇪/🇪🇺 🇺🇸
Supply chain diversification*	🇦🇺 🇫🇷	🇩🇪			🇮🇳	🇺🇸	🇯🇵
Data flows	🇺🇸	🇮🇳			🇦🇺 🇩🇪/🇪🇺 🇫🇷 🇯🇵		
Digital human rights*	🇺🇸		🇦🇺 🇩🇪 🇯🇵	🇮🇳			
Standard setting			🇦🇺	🇫🇷/🇪🇺 🇩🇪			🇪🇺 🇺🇸

* Note that the analysis presented in this report is insufficient to categorise the EU.

Between the EU and US, offensive measures reflect major issues and real disagreement between the two sides on how best to manage the commercial consequences of technological change, as outlined in James Lewis's chapter. Technological competitiveness is considered a major factor within current geopolitical tensions and systemic rivalry. To accelerate innovation, digitalisation and the so-called 'greenification' of the EU industry, the EU is strongly focusing on policies that support the commercialisation of innovation. The Franco–German 'Manifesto for a European industrial policy fit for the 21st century', cited in the chapter on France, emphasises the need for massive investment in innovation. Additionally, the manifesto mentions the need to broaden the EU's exclusive view on the internal EU market, and also to take competition and geopolitical tensions at the global level into account. While emphasising the high-tech side, rather than the digital domain as a whole, the German contribution adds to this the need for financial means to boost European innovation. GAIA-X stands out as a prime example of the proactive stance of France and Germany, but also so-called 'Important Projects of Common European Interest' contribute to the innovativeness of the EU member states.

As James Lewis notes, the issue of innovation is strongly linked to the privacy debate, norms and standards. In the eyes of the US, the EU overregulates its market, thereby discouraging entrepreneurship and innovation. Yet on the underlying norms and standards, in general the EU and US are still allies, or as Lewis aptly puts it: 'While European and American companies compete, the same is not true for nations. It is in the US interest to see a vibrant and innovative Europe'.

A normative coalition with Australia and Japan would be an obvious path to pursue for the EU and the US, especially on digital rights. European countries have been frontrunners in this field, and more recently Japan and Australia are starting to act on similar concerns. Japan is currently considering how to introduce human rights into the field of export control and economic security, and shows initiative with its Data Free

Flow with Trust on privacy and data regulation. Australia, for its part, is increasingly concerned about the use of surveillance technology inside and outside the country, after the domestic use of devices manufactured by Chinese companies has been reviewed, writes Bart Hoogeveen. It is now considering a stand-alone law that would address human rights violations and corruption.

India appears to be 'the odd one out', as it rejected the Regional Comprehensive Economic Partnership (RCEP) and refused to sign the Japanese-initiated DFFT. Nevertheless, Rudra Chaudhuri emphasises that India may provide opportunities to strengthen its technology relations with like-minded partners such as the EU, US, Japan and Australia in finding common ground to design standards that are compatible with each other's social and democratic make-up. Second, as Chaudhuri also points out, India could be a valuable partner to cooperate with on the future of the Indo–Pacific. France, Germany and the Netherlands have committed themselves to an Indo–Pacific vision or guidelines, and this renewed interest has been welcomed in New Delhi and Canberra.

The renewed focus on offensive measures in Europe coincides with the likely return of the US to multilateralism under a Biden administration. Yet as the German chapter states, while US allies hope that the new American administration will re-engage to forge broad-based coalitions to deal with the challenges that China poses to all, the transatlantic relationship has changed. In order to set new digital standards proactively and push back on China's increasing multilateral power, like-minded democracies have to share assessments and take common steps. This could be done if countries recognise that differences on digital and high-tech issues are transnational. To quote Martijn Rasser in his chapter: 'tech-leading democracies in Europe, Asia and North America should set up a mechanism to coordinate and collaborate on matters of technology policy'.

EU strategic autonomy versus US decoupling?

Moving from specific instruments to approaches, a key issue emerging from the chapters is the EU's 'strategic autonomy' or 'technological sovereignty' and US 'decoupling'. Just as Europe's turn to 'strategic autonomy' or 'technological sovereignty' is not uncontroversial within the European Union, this debate is met with diverging responses in the US and beyond. As one among many, the association representing US businesses in Europe, AmCham EU, urges the EU to define better the concept, expressing concerns 'about the potential adverse effect that resorting to a model of "open strategic autonomy" could have on trade and investment'.

The chapters in this report show that opinions differ, also among US experts. James Lewis, for example, speaks of the 'reasonable concerns' of Europe over competition and

taxation and 'legitimate concern' over privacy, while his CSIS colleague William Reinsch emphasises that the US has 'mixed feelings': 'welcoming [steps towards strategic autonomy] as a counterweight to China, which is a national security rationale, but objecting to it if it is seen as disadvantaging US companies, which is a competitiveness concern.' Clearly, there is a fine line between 'offensive action' and 'protectionism'.

As 'strategic autonomy' in recent years became the new buzzword in Europe, 'decoupling' was increasingly heard in the United States. Although the two concepts are hardly discussed in tandem, strategic autonomy and decoupling are arguably two sides of the same coin. After all, both constitute an attempt to regain control over Chinese state-steered economic actors that traditional market-capitalist instruments have allowed to go unchecked for many years. Also, both are said to be a function of how much China chooses to engage with Europe and to deliver on its promises. Finally, just as Europe's push for strategic autonomy is slowly being put into practice – by way of investment monitoring, a 5G toolkit and forthcoming competition policy regulation – decoupling is already happening.

These similarities notwithstanding, strategic autonomy and decoupling differ in important ways. While decoupling aims to disconnect the two largest economies, strategic autonomy assumes that this is not possible and instead sets out to increase Europe's geopolitical space in an interconnected world.

Another key difference is that Washington's steps towards decoupling also have an impact on companies' operations outside the US, while Europe's push towards strategic autonomy is 'EU-internal'. While decoupling – unlike strategic autonomy – is mostly not by design, the thinly veiled threats and real policy steps (for example in export control) of the Trump administration have forced the private sector to take (preparatory) steps. The effects of this strategically ambiguous policy are not just for American businesses to bear; the extraterritorial effects of US policies are forcing *all* global business players to respond. Seen in this context, US criticism and its worries regarding Europe's push for strategic autonomy seem somewhat hypocritical.

Clearly, both the EU and the US need to clarify their intentions and consider the effects of their actions under these controversial labels. The perceptions and real consequences of their actions for allies and like-minded partners need to be taken on board, at the risk of growing divergences that obstruct much-needed joint action.

A rights-based approach to tech governance?

A second challenge to enhanced cooperation lies in the normative dimension. Central to the debate and any policy decision in the digital domain are the trade-offs concerning privacy, business interests and national security. While all regulations are a combination

of these three, the different choices that the EU and US make – and the political philosophies underpinning those – are an indication of the hurdles to future transatlantic cooperation in this field.

Clearly, the US and EU share – with like-minded partners like Australia, India and Japan – concerns over China's authoritarian approach, which emphasises state security. Herein, Chinese businesses are supported and leveraged to pre-empt threats to the PRC and, more specifically, to the Chinese Communist Party. China's approach is evident from its strict data localisation requirements, which prevent any data from being stored outside its borders and a mandatory security assessment for cross-border transfers.

For Europe, however, there is more to the story. The EU approach to digital and tech domains emphasises individuals' privacy, equity and online privacy, thus putting a strong focus on ethics with a human-centred approach. In data protection regulations (like GDPR), this is evident from its strong focus on the ability of people to manage and control their data. This contrasts with the path that the US has taken, which prioritises the interests of businesses and (economic) efficiency, manifested, for example, in the strong focus on free data flows, both personal and non-personal, to strengthen companies' competitive advantage in collecting and using data to develop themselves. By contrast, EU law is much more open to equity decisions, even at the arguable cost to efficiency.

In this report, differences in approaches across the Atlantic are most evident, albeit implicitly, in the French chapter. Rather than starting from the challenge posed by China, the French chapter starts by discussing divergences between the US and France that are not directly related to China – reinforcing William Reinsch's point that some in the US wonder which challenge is considered to be bigger: the US or China? Clearly, the EU and US share more between them compared to what they share with China – namely, a rules-based and liberal–democratic approach (hence, the scalene triangle visualised in Figure 1 in the introductory chapter). Finding common ground on specific topics, such as digital human rights, the application of AI or data protection, could enable the EU and US to move forwards also on the normative dimension.

'Digital rights' will be on the EU's agenda more broadly in 2021 under the Portuguese EU Council presidency. The Portugal-proposed 'Charter for Digital Rights', which promotes fundamental values of democracy, sustainability and ethical behaviour in the digital domain. In previous years, the Netherlands and other EU member states have taken the lead on this, by including 'digital human rights' considerations' in their assessment of whether or not to grant export-control licenses. Also in like-minded countries, the momentum seems to be growing, as even Japan is now considering proceeding on this agenda, as Kazuto Suzuki states in this volume.

A key question for the future is whether individual digital rights can also be on the transatlantic agenda, and in the democratic space more broadly. As US President-Elect Biden sets out to embed climate policy throughout his government, a first opportunity seems to present itself in the link between digital technologies and climate and the UN's Sustainable Development Goals.

Conclusion: Lessons for Europe

Taken together, the various chapters in this report offer a range of lessons for the Netherlands and other EU member states as they seek to reposition themselves in the face of China's rapidly growing technological prowess.

As a developed Western-orientated country and a key like-minded partner in Asia, Australia's recent spat with China should be considered an important warning shot for the EU and European capitals. More than ten years ago, Australia's action on investment screening already provided incentive for Europe to act in this field – but the EU failed to do so. While protest from Beijing was much less likely then compared to now, the political climate and mood among businesspeople were at that time not yet ripe for measures that might upset China. Today, the situation is much the opposite.

What has not changed, however, is the fact that there is still much to learn for European countries from Australia's experience – in particular, on countering foreign influencing. As EU member states' alignment and cooperation on China have significantly improved in the last years, recent steps in Australia can help to solidify this trend by enhancing the EU's capability to align EU member states on this growing challenge. As Bart Hoogeveen points out, 'internal solidarity has been the *leitmotif* of the ASEAN in its strategy to counter potential attempts by outside powers to play out differences'. Australia's State and Territory Arrangements Bill, which attempts to align the country's states to the national government's policy, can serve as an inspiration to explore a similar course of action for individual EU member states.

Separately, another key point that emerges from the preceding chapters is that the EU and its member states need to explain better their respective competences in the trade–tech–digital fields, as well as the consequences they hold for the role that each can play. The complexity of the EU and EU member states' system is hard to understand, even for many Europeans, and seems to be obscure also to key partners that the EU now wishes to engage. This is evident from the point by Martijn Rasser that, until recently, the EU has not generated any ideas for a democratic technology alliance (or similar) between like-minded countries, even if Brussels has been pushing the boundaries on issues such as digital sovereignty, data rights and economic entanglement with China.

This observation seems to overlook the reality that the EU requires a mandate from its member states to act. After all, while trade policy falls under the EU's exclusive competence, meaning that the EU manages trade policy and trade negotiations on behalf of the Member States, the EU does not have this legal competence in several other fields – like 5G and cybersecurity. On yet other issues, including export control and foreign investment, this competence is shared between Brussels and European capitals, meaning that both member states and the EU have clearly defined competencies. The EU is thus constrained to act on the comprehensive agenda that is before us now. It has, however, employed an internal market rationale and increasingly incorporated security and fundamental rights' considerations to push forward important issues, including cybersecurity."

A fair assessment of the EU's contributions to the creation of new multilateral frameworks should consider both the EU and EU member states levels. To name a few such ideas and actions: the Global Partnership on Artificial Intelligence (launched in 2020 with an OECD-based secretariat, following a proposal by France and Canada in 2018); and the Alliance for Multilateralism, based on a proposal by Germany in 2018 and launched in 2019 at the United Nations General Assembly. Also, less well-known international initiatives have come from Europe, including the Global Forum on Cyber Expertise (GFCE), initiated by the Netherlands and established at the 2015 Global Conference on Cyberspace in The Hague; and the Next Generation Internet (NGI) initiative of the European Commission, which furthers its human-centred approach to the internet by actively supporting civil-society organisations and media pluralism in countries in and neighbouring Europe.

To be fair, these initiatives may be considered individual pieces of the puzzle, rather than a broad framework that enables all to see the big picture. In the transatlantic context, an obvious benefit of such a comprehensive approach is that it allows for a potential 'grand bargain'. Brussels-based scholar Andrea Renda has suggested steps for a transactional approach that encompasses different parts of the 'digital ecosystem'. He proposes, for example, that the US 'offers its European counterparts enhanced access to its domestic 5G market, in exchange for more cooperation, and perhaps regulatory convergence, on the side of platforms and AI'.[18]

European proposals have also attempted to shape a such comprehensive approach for a 'tech alliance'. The UK proposal for a D10 of 2020 is one suggestion, and perhaps the only one formally proposed by a government. There is no dearth of ideas, however: former Member of the European Parliament Marietje Schaake put forward specific suggestions for a global democratic alliance.

---

18   Andrea Renda, 'The digital revolution: scenarios for enhanced transatlantic cooperation', unpublished discussion paper (CEPS and European University Institute, November 2020).

Clearly, the need for new initiatives is urgent. The transatlantic allies, with like-minded partners, must jointly act upon China's strengthening techno-authoritarianism, the failure of multilateral institutions to incorporate the digital world, and confront the power of technologies to derail democratic societies and undermine fundamental individual rights.