EUROPEAN COUNCIL ON FOREIGN RELATIONS
ecfr.eu

POLICY BRIEF

THE POWER OF CONTROL: HOW THE EU CAN SHAPE THE NEW ERA OF STRATEGIC EXPORT RESTRICTIONS

Tobias Gehrke, Julian Ringhof

May 2023

SUMMARY

- Technology is increasingly a battleground in the strategic competition between the US and China.
- Western technology contributes to China's military modernisation as well as the development of Russian weapon systems.
- The US is restricting trade in key technologies with China and pushing EU member states to follow its lead.
- To better defend its interests, the EU needs to develop clearer policies on China and security, including pursuing the 'de-risking' of its relations with Beijing.
- The EU must develop a new strategic technology doctrine and upgrade its export control policy.
- This more coherent stance will enable the EU both to act where necessary but also to defend itself and its member states from future pressure from China – and the US.

In January 2023, the United States and two of its closest allies, the Netherlands and Japan, concluded a ground-breaking agreement – but took pains not to draw attention to it, or even to call it an agreement. They held no press conference and released no joint statement. Yet the subject of their deal goes to the heart of the growing strategic competition between the US and China. And it encapsulates some of the critical challenges facing the European Union at the intersection of international security, the world economy, the technological revolution, and strategic competition.

The agreed non-agreement between the three states pertains to some of the most complex machinery and most miniscule components humankind has ever produced. With their accord, the countries effectively restricted the export to China of the most advanced microchips and the tools to produce them. These items have become a focal point in international power politics because of their use in developing artificial intelligence and their centrality to many of the 21st century's most important technologies.

As news on the matter emerged, the Dutch prime minister confined his remarks to saying: "Those talks have been going on for a long time and we're not saying anything about it." The reason for reticence was clear; in response to their decision, China threatened retaliation against the Netherlands and Japan.

The move followed on from measures unilaterally implemented by the US in October 2022 to restrict the trade of advanced semiconductor technologies with China for reasons of international security. And it now appears that the Dutch national measures could soon be followed by a decision by the German government to restrict the export to China of chemicals needed for chip production.

As these sorts of incidents mount amid the escalating US-China strategic technology competition, the EU and its member states will find themselves increasingly caught in the crossfire. Washington will maintain pressure on its allies to align with its China policy. China's military build-up will continue to change the balance of power. And Beijing's willingness and ability to weaponise trade will likely continue to grow – it will no longer be possible for the EU to keep its pursuit of free trade separate from these powerful currents. If a rules-based order is to remain, the rules will need to change to take account of the ways in which economic security forms part of this wider competition.

To steer a course according to its own interests in this new era of strategic trade controls, the EU must urgently develop its own strategy and upgrade its tools to deliver on it. If it is to promote and defend its own sovereignty, it must start to draw its own red lines in technology engagement with China and upgrade its export control policy.

Strategic technology controls: A new era

Despite its threats of retaliation, Beijing's response to the Netherlands' export controls on advanced chip manufacturing equipment has so far been largely cautious. This is in contrast to the Chinese reaction to the United States' October 2022 decision to begin restricting trade in advanced semiconductor technologies with China. In response, China brought a case against the US at the WTO; it also targeted a number of American companies, sought to divide the US from allies, and pressured its own companies to eliminate foreign suppliers.

Advanced semiconductors are primarily needed for commercial applications, including supercomputers, to develop artificial intelligence for climate modelling, medical research, advanced manufacturing, and self-driving cars. Preventing China from importing and developing advanced semiconductors will likely slow the country's economic and technological development across a variety of commercial sectors dependent on supercomputers and artificial intelligence.

But semiconductors are inherently dual-use, meaning they are not only needed for many commercial applications but are also integral to modern weapon systems, as Russia's war of aggression against Ukraine is showing. Russian weapons, such as Kh-101 cruise missiles, are heavily reliant on Western semiconductors.

There is no doubt that advanced semiconductors from Western companies have been contributing to China's military build-up. Given Beijing's increasing political and military assertiveness, especially with regard to Taiwan, the US deemed restricting the flow of these technologies to China a legitimate security measure. Nevertheless, with this move, the economic realm is now firmly in scope for the wider US-China strategic competition.

EU member states are able to adopt measures similar to those of the US under the EU dual-use export control regulation. The bloc updated and upgraded this regulation in 2021 after five years of difficult negotiations. Nevertheless, the EU framework is much more confined and less coherent than that of the US. Crucially, the EU lacks a firm policy underpinning on China and on economic security to inform the use of export controls.

Yet, as the US-led move to restrict China's access to advanced semiconductors shows, this is

likely to be the first among many such examples, as China and the US each enhances its approach to technology on the broader strategic battlefield. The EU is likely soon to need new policy options to be able to act in this new era.

The United States' approach to strategic export controls

The United States' October 2022 restrictions signify a strategic change in its post-cold war use of export control policy. For many decades, the use of export controls across the globe was largely confined to military and dual-use goods. Under the Trump administration, the US – somewhat erratically – introduced technology blockages against individual Chinese tech giants. The Biden administration has now begun to leverage export controls as a strategic tool to "maintain as large as a lead as possible" in key technologies over China.

Indeed, the US National Security Strategy, adopted in 2022, clearly states that keeping ahead of China in technology is a central pillar of American national security. In a pivotal speech last September, national security adviser Jake Sullivan set out how this new doctrinal thinking is reshaping US domestic policy – by promoting American industry and technology – and foreign policy – by capping China's access to critical US technologies, limiting US dependencies, and bringing allies along. This is grand strategy in the making.

To deliver this developing strategy, the US has been steadily expanding its toolbox to limit China's access to, and arrest its advancement in, technology industries that Washington considers foundational to American military and economic power. Over the last half-decade, and through over half a dozen legislative acts, the US has: beefed up controls on Chinese investments in America; ringfenced its telecoms sector from Chinese involvement in building and maintaining infrastructure; tightened visa restrictions on students from China; barred Chinese imports; and is removing Chinese ICT providers from its supply chains. More such legislation is in the pipeline.

Alongside these steps, the Biden administration has also created ways to actively retain American positions of leadership in various technology sectors – or seek to win these positions back. Both the CHIPS and Science Act and the Inflation Reduction Act (IRA) aim to re-wire strategic technology supply chains for semiconductors, electric vehicles, batteries, and renewable energy components – thereby limiting China's power of control over these technologies. The CHIPS Act, for example, makes subsidies for companies conditional on them limiting certain operations in China. Since the entry into force of the IRA and the CHIPS Act in August 2022, companies have committed over $200 billion in investment in these strategic sectors in America. This underlines Washington's power to shape global industries through its national security policies.

In these ways, the recent Western measures on semiconductors are set to advance the United States' objective of safeguarding its military and technology leadership. This act aims to freeze China's own progress towards developing advanced semiconductors domestically. It is thus delivering on a central objective of Biden's national security agenda.

The White House has stated that advanced semiconductor technologies not only have broad commercial applications but also act as "force multipliers" that contribute to military strength. It identifies a clear link between semiconductor technologies and China's development of weapons of mass destruction (WMD). For this reason, it wants to control the trade in these primarily commercial technologies with China, despite the risk of significant collateral damage for the US, China, and the world economy and the risk of an escalating trade conflict. The US commerce department justified its semiconductor restrictions by drawing connections between advanced semiconductor technologies and WMD development, China's military modernisation, and human rights abuses.

That being said, the restrictions on largely commoditised memory chips (where China had been gaining market share, but where no clear links between such chips and AI and modern weapon systems can be made) that were part of the October control package suggest that the measures are also intended to maintain or change market balances in favour of the US. Economic security considerations are also evidently at play.

Importantly, the October 2022 measures rested on a firm bipartisan consensus enshrined in the 2018 Export Control Reform Act (ECRA), which clearly defined the parameters of national security that allow for the broad use of export controls. Beyond long-established goals of preventing the proliferation of WMD and military and dual-use technologies, the ECRA established new powers to impose export controls with the explicit aims of preserving US military superiority, strengthening the US industrial base, maintaining US technological

leadership, and advancing US foreign policy objectives, including the protection of human rights and the promotion of democracy.

The ECRA was written with China and its challenges to economic security in mind. With the adoption of the ECRA, the Commerce Department is now tasked, on an essentially permanent basis, with identifying which additional "emerging and foundational technologies [that are] essential to the national security of the United States" ought to be controlled – particularly vis-à-vis China.

Relations with the EU

Maintaining leadership over China by cordoning off access to, and hampering the development of, advanced technology is as profound a strategy as it is disruptive to the global economy – and the EU's position therein. While national security is the leitmotif, it remains unclear where and on what basis Washington draws the red line for technology trade with China, as this area is constantly evolving. To what extent competing interests such as open trade, efficiency, and multilateralism can still play a role in this reassessment also remains unknown. While the Biden administration has invested significant diplomatic effort in explaining its security policy to European allies – and some European leaders have become more outspoken about their shared security concerns regarding China's economic and technology policies – wariness and distrust of US motives and interests remain strong in some parts of Europe. A Republican White House may be more willing to force closer European alignment by leveraging its security dominance.

Still, Washington is aware that it cannot single-handedly address the security challenge that the economic, military, and technological rise of China poses. It knows that unilateral controls lose their effectiveness and negatively affect US economic competitiveness over time as the gaps left in the Chinese market by the withdrawal of US companies are successfully filled by non-US firms. This desire to bring allies along gives Europeans the ability to influence the direction of travel of US policy – if they manage to adopt a more united approach.

China's approach to strategic technologies

Since the founding of the modern Chinese state, the party leadership has explored ways of integrating the military and civilian sectors. From Mao onward, technological "self-reliance" – the absence of foreign dependencies – has been a strategic priority for Chinese leaders, first with regard to the Soviet Union and later Western democracies in the face of technology embargoes such as CHINCOM (a US-led committee coordinating export controls on China

during the cold war). These efforts rarely succeeded. But since Washington targeted Chinese national champions Huawei and ZTE in 2018, Chinese leader Xi Jinping reinvigorated this national security drive for technological self-reliance. "Only by grasping key core technologies in our own hands can we fundamentally guarantee national economic security, national defence security, and other securities" were his words as he explained this doctrine in 2021. Elsewhere, he directed his administration to "intensify the formation of unique advantages in some domains of strategic competition."

Alongside these developments, the inclusion of military-civil fusion into China's national strategy in 2014, the establishment of the Central Commission for Military-Civil Fusion Development in 2017, and a number of recent national security laws with vague and expansive knowledge-sharing obligations for companies have contributed to Western policymakers' change in attitude.

Indeed, China now enjoys a growing dominance in emerging technologies that are vital to determining tomorrow's economic and military balance. Artificial intelligence, which China's leaders see as foundational to economic and military power, advances in domestic surveillance systems, and advanced data analytics could give China significant military advantages. In quantum technologies, China's leading research positions in photonic sensors, quantum communications, and cryptography could also translate into significant warfare capabilities. And beyond such 'hard security' considerations, averting the risk of Chinese companies monopolising emerging dual-use industries should be a key concern for European governments as they consider how to address China's techno-security state.

China's toolbox for securing strategic technologies is large and growing. It includes its military-civil fusion framework, five-year plans, national and local sector-specific industrial plans, targets for localisation and market shares, research and development funding, the creation of national champions and innovation centres, selective foreign investment, joint ventures, espionage, and more.

China's strategic export control toolbox

In 2020, China reformed its Export Control Law, introducing the capability to place restrictions on a wide range of items and end users, including applying and enforcing its controls even outside its own borders if needed. While China has so far been reluctant to pull the export control trigger, it has equipped itself with a large potential weapon – the threat of which may give it powerful leverage in any future negotiations with the EU. For example, an ongoing revision of the items on its export control list is likely to include a range of technologies in which China enjoys asymmetric leverage over Europe, including rare earth

magnets, solar photovoltaic equipment, gene editing technology, computers, and automatic driving software. China's policies to increase its influence over the manufacturing of 'legacy' semiconductors could equally become a powerful form of leverage: in the EU, the production of electric vehicles, industrial robotics, drones, and medical devices relies on legacy chips from Chinese factories.

With this toolbox to hand, China could dial up its own technology controls on other states or on the EU – indeed, some in China are already calling for this publicly. And China has already significantly increased its use of economic coercion in recent years. China's advances in sensitive and emerging technologies could therefore not only amplify China's military power but also its coercive leverage, making it a risk to both the national and economic security of the EU.

Currently, however, the European policy debate suffers from a lack of domestic intelligence on the mechanisms through which China is aiming to develop a dominant position in strategic technology supply chains – and how exactly sensitive technologies leak to China and into its military-industrial complex. The EU needs to do more to gain its own intelligence of these processes in order to inform its strategic technology policy without having to rely largely on US assessments.

Russia lessons

Lessons from Russia's war in Ukraine demonstrate the importance of ensuring trade and technology policy work in support of security imperatives.

Within 24 hours of Russia's all-out invasion of Ukraine, the EU and the US implemented unprecedented export restrictions on strategic technologies traded with Russia and Belarus. They were shortly after followed by other key Western allies including the United Kingdom, Australia, Japan, Canada, and South Korea.

These measures marked a significant change for EU and allied policy, by significantly broadening the traditional scope of export restrictions beyond military and dual-use goods to incorporate a host of advanced commercial technologies. These included electronics, computers, telecommunications, information security, sensors, lasers, and aviation and maritime technologies. Since the end of the cold war, export restrictions had not been used with this strategic ambition, in such breadth, with such coordination among allies, and against an economy the size of Russia's.

For Washington, this allied strategic leap against Russia signified clear momentum to now also jointly target China through coordinated export controls.

However, the sort of broadened technology export restrictions applied against Russia are by no means an obvious next step for the EU to use with regard to China; nor for Japan, South Korea, or Taiwan. It is one thing for the EU to implement export restrictions as part of a sanctions regime against Russia. It is quite another to actively implement strategic export controls on largely commercial technologies against China – an economic giant, with which the EU is tightly economically entangled.

European interests in the crossfire

In this difficult context, the EU is at risk of being caught between the two superpowers. Without developing a robust common strategy on strategic technology policy, the EU will find itself drawn deep into the US-China struggle for technology supremacy and left unable to steer a course according to own interests. Crucially, Europeans will only be able to find their footing if they establish what their own security interests are. Otherwise, the US will continue to set the terms in bilateral deals such as the recent measures on semiconductors.

Technology risks

China's dominance over clean technology value chains – from the mining and processing of critical minerals to the production of solar cells, modules, and batteries – has already generated concern that the foundations of the EU's economic security are at risk. The spectre of strategic dependencies and economic coercion has led to calls to diversify imports.

In recent years the EU has significantly upgraded its economic security toolbox to tackle a range of different risks, including unfair trade competition, economic coercion, supply chain dependencies, and risks to critical infrastructure and strategic assets. To this end, the EU adopted an anti-coercion instrument (ACI) to combat economic coercion, introduced a foreign direct investment screening mechanism to protect strategic assets and infrastructure, and developed industrial policy tools to ensure the EU remains an innovation power.

But China's techno-security state still poses many challenges. The EU remains vulnerable to sensitive technology leakage (the unwanted transfer of technology), especially to China, where the state mobilises its national economy – from labs, to universities, to private companies, to the military – to become a "global leader in innovation," as Xi declared.

China actively works to facilitate the transfer of sensitive technologies from the EU and

European companies. It does so in a variety of ways. It employs open-market mechanisms – such as free trade and direct investments – legal mechanisms – such as rules that make market access conditional on the transfer of technology – and coercive mechanisms – such as espionage and the use of research and academic networks. Although China has tweaked these technology transfer mechanisms in response to foreign pressure, nearly a third of EU companies reported in 2020 that they had been compelled to transfer technology to China. And China's state-owned companies have consistently sought to replace foreign technology and push out foreign firms once they have secured the technology transfer. From wind turbines and solar energy to high-speed rail and telecommunications, technology transfers in these sectors have eroded EU leadership positions in technologies the Chinese state had designated as strategic. In April 2023, the Dutch intelligence service warned that China was targeting high-tech companies and institutions through "corporate takeovers, academic cooperation, as well as illegitimate (digital) espionage, insiders, covert investments and illegal exports." Such networks conceal the involvement of the Chinese government or army and would pose the "greatest risk to Dutch economic security," the agency warned.

Herein lies the rub: the EU's technology restrictions distinguish between 'purely' commercial technologies and dual-use technologies. For China, however, strategic technologies are identified in countless industrial plans and are framed as vital to Chinese national and economic security in the struggle for technological leadership. A focus on strategic technologies – those required for fighting climate change, those in which strong dependencies exist, or those that support key advantages in supply chains – is more recent for the EU, such as technologies identified in industrial policy frameworks such as the Chips Act and the Net Zero Industry Act. China's approach means that the EU cannot treat its strategic technology policy as something separate from agendas set in Beijing or elsewhere.

Finally, the advances in military-civil integration occurring in China – and other countries – and the increasingly central role commercial technologies play in military development mean the EU will need better intelligence on the links between civilian companies, universities, the military sector, and the role of commercial technologies in military end uses. Individual member states do not have the capacities to investigate these complex links alone.

The EU's fragmented China policy

A serious public discussion is still to take shape in the EU about how China's quest to become a technology superpower – and how the United States' determination to prevent this from happening – will fundamentally challenge European security and economic and political engagement with both countries. The EU now faces integrated economic strategies from more

than one source that will bend the global economy beyond recognition.

The EU's challenge is this: with national security returning as a powerful variable of economic strategy in other powers' capitals, the bloc's ability to deploy its economic leverage is shrinking. This was evidenced most recently in its relations with the US. Because the IRA forms part of a wider national security-driven China strategy, Washington acted without seriously consulting European allies, offering only ex-post coordinationsome relief through " ex-post coordination." It is apparent that the EU's deep and growing security dependence on the US, as exposed with American leadership on the Ukraine war, and its fragmented security positions with respect to China, have hastened the erosion of its economic bargaining power.

While many EU member states share the United States' concerns regarding the security threat posed by China, there is neither full alignment vis-à-vis China between the EU and the US nor between all EU member states. In fact, the EU has not formally adopted the maintenance of military superiority and technological leadership over China as objectives of its security or China policies. Indeed, the EU has no common security policy or China policy and, unlike the US, it has not clearly defined the role strategic commercial technologies and the trade thereof play in European security. As a result, the EU is yet to decide how European export control policy can contribute to advancing its security policy objectives in face of the rise of China, trade weaponisation, and new technologies.

In a seminal speech on EU-China relations, European Commission president Ursula von der Leyen this year identified these shortcomings when she urged a reassessment of European security interests for exports and investments in China "where dual-use purposes cannot be excluded." She also correctly identified that the EU will need to consider additional instruments, such as powers to screen investments from the EU to China, and link them up coherently in an overarching economic security strategy. In June this year, the European Commission is expected to propose an economic security strategy that could set out how the EU might pursue this.

Implementing such a de-risking approach will throw up difficult trade-offs. The EU wants to limit the military build-up of rivals – but not limit their economic fortunes. It wants to limit strategic dependencies – but not friend-shore. The EU wants to retain its powerful economic voice – but not share its national security competencies. The bloc wants to secure its economy, but not violate existing international trade rules. Yet its de-risking agenda must tackle these trade-offs head-on. To address this, the EU will require a strategic technology policy in peacetime that not only limits its own vulnerabilities but also identifies and ringfences asymmetric advantages needed for deterrence or even economic warfare.

The economic-security world order under strain

Recent difficulties in the WTO expose the tightly interwoven relationship between the economic order and the security order. They should compel the EU to move quickly ahead with enhancing its own policy grounding in the critical area of strategic export controls.

There is no doubt that retaining the WTO as the most important international trade body is in the EU's interest – to protect its place as a global economic power (not least since there are no better options currently available). But the WTO currently finds itself seriously struggling to handle the challenge presented by a securitised global economy in which the US has turned its back on much of the organisation. When the Trump administration's argument that tariffs on steel and aluminium were a matter of national security came under formal challenge at the WTO, the organisation was obliged to make a judgment as per the rulebook. Unsurprisingly, the Biden administration snubbed the WTO's recent ruling on the US measure. No American administration will allow a panel of three bureaucrats in Geneva to determine what is or is not in America's national security interests.

There is therefore a mismatch between the way in which powerful states are using economic means to pursue geostrategic ends, and the institutions available to manage such competition safely.

Challenging obvious protectionism under the guise of national security is important if the global trade system is to survive. But the legalistic approach to addressing trade and security issues as enshrined in the WTO is also reaching its limits: the geopolitical foundations on which this approach was built are eroding. There can be no functioning open trading order without a corresponding security order underwriting it. The General Agreement on Tariffs and Trade, the cold war predecessor to the WTO, was unequivocally linked to US great power competition with the Soviet Union, and was part of a wider strategy to strengthen allies against the communist threat. The drive towards open markets among Western economies was possible not least because bolstering the Western economic bloc assisted Washington in its geostrategic competition with Moscow. After the end of the cold war too, the WTO was not operating in a geopolitical vacuum, as some now claim in hindsight. Despite the push in the 1990s from companies to expand free markets globally, the strategic arguments to allow China to accede to the WTO in 2001 were deeply geopolitical in nature, based on a gamble that economic and political change in China would support American geopolitical interests.

With this gamble not paying off and having lost all favour in Washington, the security foundations on which the WTO was built will need to be relaid. Europeans cannot therefore

hope to save the open trade order if it continues to lack a security underpinning. They must honestly consider that in the absence of a national security valve that allows for US-China strategic competition, the WTO will be further relegated to the backbench of international organisations. “The commonest error in politics is sticking to the carcass of dead policies,” former British prime minister Lord Salisbury remarked in 1877. For the EU, this means it must table experimental models for managing trade in a geo-economic world, such as through a political body or a mediation process. The aim would be to ensure certain contested trade matters do not undermine the wider rules-based system of international trade.

The Wassenaar Arrangement and EU export control policy

In 1994, the Coordinating Committee on Multilateral Export Controls (CoCom) – the Western bloc’s mechanism during the cold war to jointly limit the flow of strategic technologies to the East – was dissolved. The Wassenaar Arrangement (WA) that succeeded it in 1996 narrowed strategic export controls to use against security threats such as the proliferation and accumulation of WMD, delivery systems, conventional weapons, and dual-use technologies.

The WA is one of four multilateral export control regimes and has 42 participating states. Importantly, under the WA, participating states agree to a common list of dual-use technologies to be controlled for export. These controls are then implemented through national measures on a voluntary basis, as the WA is not a treaty and hence not legally binding.

Although the EU’s 2021 regulation significantly improved union-wide coordination of controls and expanded the scope of EU export controls, the competency to control the export of additional items not listed in the WA rests entirely with member states. While member states have the authority to restrict the export of non-listed dual-use technologies, such unilateral measures are rare in the EU and – unlike in the US – have historically only been used to achieve narrowly defined security or human rights objectives.

Moreover, the EU – in line with the WA and in contrast to US – has traditionally retained a country-agnostic approach with regard to export controls. Sustained controls targeted against a specific country outside sanctions regimes or arms embargoes have not formed part of EU and member state policy.

The drawbacks of Wassenaar and current EU export control policy

For these reasons, the EU used its sanctions regime to implement export restrictions on advanced technologies against Russia, rather than through its export control regulation. This is also why export controls on technologies not listed in the WA and not unequivocally falling within the traditional dual-use scope targeted at China would not only require a change in the EU's China policy but would also mean a significant change in EU export control policy. In this and other regards, the EU's export control policy is no longer adequate to deal with today's challenges, for several reasons.

Firstly, as highlighted by the war in Ukraine, commercial technologies are becoming increasingly foundational to military strength. As the military-civil integration of the EU's systemic rivals progresses, narrow dual-use controls no longer suffice to uphold European security. Secondly, as technology trade becomes increasingly weaponised and economic security becomes a matter of national security, the EU's narrow understanding of national security in export control policy finds itself ever more outdated. Thirdly, multilateral regimes such as the WA are becoming increasingly dysfunctional. The regime's processes are protracted – it can take around three years for a new technology to be listed, which prevents the WA from keeping up with today's rapid technological advances. [1] Moreover, Russia's membership of the WA, combined with the arrangement's consensus-based system, is now further impeding progress of adding new dual-use technologies to WA control lists.

In the absence of an EU approach geared to handling the latest challenges, the Netherlands – under increasing pressure from the US – made its own strategic leap. The Dutch government's March 2023 announcement of novel national export restrictions applied to deep ultraviolet (DUV) lithography machines, which are one of the most important tools for making advanced chips. The Netherlands is the world's only supplier of the most advanced lithography equipment, including DUV and even more advanced extreme ultraviolet (EUV) lithography machines, whose export to China the Dutch government had already prohibited in 2018. This means the Dutch company that produces the lithography machines, ASML, occupies a key position in advanced semiconductor supply chains. It was a White House priority to persuade the Netherlands, and Japan, to act.

Importantly, with these new measures, The Hague expanded the Dutch conception of national security in export control policy. It implemented national controls on a primarily commercial technology that is not listed multilaterally under the WA, and – unofficially – targeted the measure against China as a single country of concern. This marked a big strategic leap. But it also entailed a great strategic risk and significant strategic challenge, particularly

for the EU.

The risks of going it alone

The Dutch decision was apparently made in consultation with the European Commission and some key EU member states. But this national measure brings to the fore a whole set of new challenges underscoring the ways in which the EU's institutional set-up is increasingly challenged as security and economics merge.

Firstly, an export control measure taken by a single member state inherently pressures all other member states to enforce such controls; if they do not, the integrity of the EU's single market and common trade policy is put at risk. If, for example, ASML was to sell such a machine to a company in another EU country, it would then be entirely up to that country's government and export control authorities to decide on the need for, and approval of, an authorisation to export that machine to China – possibly undermining the Dutch government's decision. While such a scenario is currently improbable because of the scarcity of these machines, the complex nature of the semiconductor supply chain, and the political fallout of such a decision, with more controls on more technologies on the horizon, similar scenarios will become more likely and more problematic.

Secondly, if one member state determines which additional technologies are critical for its national security, other member states are pressured to align. For example, if Chinese companies sought to purchase the lasers and optics that are key to making advanced lithography machines from globally leading companies Zeiss and Trumpf, legally nothing would prevent these two German firms from selling these components. Because, although DUV and EUV machines are controlled by the Dutch, key components for these machines would not automatically be controlled as well, especially when made in another EU country. Selling these key components to China, however, would certainly erode ASML's and the EU's leading position in lithography machines over time and hence undermine the Dutch measures.

Thirdly, the lack of a common European approach exposes individual member states and their companies to external pressures to align controls as well as to retaliation by the targeted country. This inevitably exposes the entire single market and all of the EU to countermeasures – as highlighted by Chinese sanctions against Lithuania. When a Taiwanese Representative Office opened in Vilnius in 2021, China not only cut off all trade with the Baltic nation, but threatened sanctions on EU firms that used products from Lithuania, such as German car manufacturers. Because of deep EU single market integration, such 'secondary sanctions' (those applied beyond Lithuania's borders) can therefore significantly impact on

intra-European trade and the EU's internal market.

Fourthly, a broadened understanding of national security and the corresponding expansion of export controls by a single member state tests international trade rules and thereby inevitably affects the EU's overall stance towards multilateralism. For example, the decision by the Dutch to implement export controls on DUV machines for reasons of national security could be challenged at the WTO by China. Because of the EU's single trade policy, the European Commission would then have to defend the Dutch measure at the WTO and the consequences of the WTO decision would possibly be borne by the EU as a whole.

The lack of a more coherent EU approach adequate to the current geopolitical environment is hugely problematic. Despite the fact that export controls are increasingly becoming a geostrategic matter, many member states as well as the EU itself do not have dedicated forums to discuss the strategic and foreign policy dimensions of export control policy. And as commercial and security policy increasingly overlap, the EU's institutional framework is set to become severely challenged: foreign and security policy, including export control policy, largely rests with member states while commercial policy is an exclusive EU competency.

Recommendations: How to rebalance EU technology, trade, and security policy

To address the major challenges set out in this paper, the EU should assess its strategic technology capabilities and technology trade links, especially with China. The bloc must augment and further harmonise its export control policy, and it must integrate export controls into its broader security toolbox. It should also revisit existing multilateral export control frameworks and develop new fallback mechanisms.

Develop a European strategic technology doctrine

The EU needs a strategic framework to set out the goals, means, and risks involved in the use of strategic technology measures. It should draw this up in such a way to enable coordination between member states, allow joint assessment of both risks and (unintended) consequences, and help policymakers develop cost-benefit analyses for strategic measures. A deeper discussion on what European security interests entail in a geo-economic era, what strategic technology tools the EU has, and how they are interconnected is therefore a crucial precondition for the EU to be more coordinated on these questions. A strategic technology doctrine could be a deliverable under a forthcoming European Commission proposal for an

economic security strategy.

The first stage of developing such a doctrine should be to develop a high-level strategic technology assessment, in which the EU commonly defines and then identifies technologies that are essential to its security. Similar to the assessment of the European Commission proposal for a Net Zero Industry Act, which developed criteria and then identified eight strategic clean energy technologies, a strategic technology doctrine should expand on this agenda in other sensitive and emerging technology fields, such as quantum computing, biotechnologies, or artificial intelligence. It should identify essential security risks – how military-civil integration strategies and the centrality of commercial technologies to military modernisation could threaten Europe or international stability – and economic security risks – how supply chain dependencies or loss of technological know-how and edge could erode European sovereignty. It should also build on the analysis of other EU bodies and tools, such as the Observatory of Critical Technologies and the strategic dependencies analysis.

This should go hand in hand with a capability assessment. The economic war with Russia shows that retaining key technology advantages is crucial in a weaponised economy. It is therefore compelling for the EU to gain a better understanding of how its own technology advantages can contribute to its security, even where they may not directly relate to dual-use or military equipment. This EU capability assessment could also include an analysis on the capability gap in these strategic technologies between the EU, China, and other powers and identify trade, investment, and research patterns.

The next stage in developing a doctrine is for the EU to agree on the goals and boundaries of applying strategic technology measures. The EU should ensure that strategic technology measures address both essential security and economic security risks highlighted above. At the same time, the goal of a European strategic technology doctrine should not be to limit another country's technological advancement. The EU must tightly define these economic security risks so as to not support a broader technological decoupling. Drawing precise red lines around certain strategic technology links as they relate to European security can and should go hand in hand with a policy of economic cooperation with China, for much of the EU's economic relationship with China does not challenge European security interests. Clearly establishing which technologies are relevant for European security – and which are not – will strengthen the EU's ability to shape its own geo-economic approach.

Finally, a strategic technology doctrine must promote synergies between different instruments, such as export controls, investment screening, and research and development funding, binding these instruments together with common objectives. Likewise, it should promote better coordination between the public and private sectors and between national

agencies. It could, for example, commit member states to develop: national economic intelligence offices, which would be tasked with preventing security-relevant and illegal technology leakage; risk monitoring; and information exchange on strategic technology risks with the private and research sector. In the future, a dedicated and centralised EU office could be created, tasked with developing stronger regulatory and procedural linkages between national export control, investment screening, research security, and cyber-security tools.

Enhance the European export control framework

The strategic context has shifted considerably even since 2021, when the EU adopted its dual-use regulation. The EU should consider ways to enhance its toolbox in this regard. Several options are available for the EU to pursue. Each comes with advantages and drawbacks.

Option A: Keep things as they are

The 2021 regulation provides member states with significant room to implement national export restrictions to address some of these new challenges. For example, the regulation permits member states to unilaterally implement controls to prevent the export of dual-use items intended for WMD development and of items destined for military end use in a country subject to an arms embargo (a non-binding EU arms embargo against China has been in place since 1989). The regulation enables capitals to prohibit the export of "cyber-surveillance" technologies. Member states can also restrict the export of any dual-use items to safeguard "public security" and human rights.

In its decision to nationally control the export of advanced lithography machines – to China – the Dutch government made use of its national authority to restrict the export of non-listed items for reasons of "public security." This indicates that the current framework suffices to address potential security issues related to the trade of commercial technologies with the EU's systemic rivals.

The advantage of the current set-up is that the competency in this delicate policy field of national security remains largely with member states. During negotiations for the recast 2021 regulation, member states maintained this position, as they do on foreign and security policy more generally. Moreover, the framework provides the flexibility for member states to adjust national controls dynamically to a changing international environment and evolving technology landscape. No lengthy negotiations between member states to agree common EU listings are needed. In addition, a member state home to a technology under consideration for control, such as the Netherlands for lithography machines, can move ahead with national

export restrictions that can – under Article 10 of the dual-use regulation – then also be adopted by other member states.

As noted, however, the problem with the current framework is that national decisions by individual member states impact on the EU as a whole. Not only are companies in other member states directly affected but the member state implementing the measures can become individually exposed to external pressure and retaliation, with possible implications for the whole bloc. Ultimately, such national decisions threaten the integrity of the single market and are inherently geostrategic, with ramifications for both the common commercial policy and the common foreign and security policy.

Option B: Draw up a new EU regulation

The EU could introduce a new regulation to replace the existing regulation. Along with other advantages, this option could more clearly define and expand the objectives of EU export control policy to include economic security considerations, mandate expanded coordination between member states' national measures, and implement a common EU control list in addition to listings agreed in multilateral regimes such as the WA. This would help the EU address the question of member states fragmenting the single market by undertaking national measures. By implementing measures jointly, the bloc would be better positioned vis-à-vis friends and foes than individual member states would.

Updating the dual-use regulation would also allow the EU to more flexibly bind its controls to multilateral regimes in face of the WA's dysfunctionality and the likely emergence of new multilateral mechanisms. Furthermore, a new regulation could help create ways to apply strategic controls beyond the borders of the EU, such as by taking action against non-EU companies that facilitate the circumvention of EU controls. The EU is also negotiating such an approach in the context of preventing circumvention of the EU's Russia sanctions.

Yet, given that the current dual-use regulation only entered into forced in 2021, after nearly five years of negotiations, and that member states will largely be reluctant to swiftly cede more competency on export control policy to the EU, it is unlikely that member states will agree a new, broadened regulation in the near term. Moreover, as EU discussions on the economic security dimension of European security are only just beginning, and member states only just starting to adjust their security, foreign, and trade policy strategies to this new era, it appears too early to hurry into negotiations to recast the regulation again.

Option C: Augment the current framework

The best choice for the EU to pursue right now is a third option. This would see the bloc leverage the flexibility of the 2021 regulation, but additionally undertake joint analysis and agree broadened but clearly defined security objectives through a new joint risk framework for EU export control policy.

The EU should develop a joint risk framework for EU export controls, similar to the 5G security toolbox. This should be embedded in the overall strategic technology assessment proposed under the strategic technology doctrine. Like the 5G toolbox, this risk framework must take into account a number of technological, economic, and political considerations and identify main risks and risk scenarios related to technology exports. Among the main risks to be assessed under such a framework is, of course, the issue of whether an exported technology contributes directly to military development or human rights abuses. But, importantly, the process must also assess to what extent a commercial technology to be exported may be foundational to military modernisation, even if the technology itself is not component to a weapon system, but, for example, foundational to develop new weapon systems. Clearly, the risk of whether an export to a civilian research organisation or commercial company may contribute directly or indirectly to military modernisation in the context of military-civil integration must be closely examined through such a framework.

Yet, this framework should also take into account additional risks to European security, including economic considerations. This also means that member states must arrive at a common understanding of "public security" in export control policy (Article 9) in today's geopolitical context.

To a degree, the Dutch government has already done this with its decision to unilaterally control the export of lithography machines for reasons of public security. By invoking Article 9 for the first time in EU export control policy, the Dutch government moved ahead and defined three clear "public security" objectives justifying the restrictions: preventing Dutch goods from contributing to undesirable military and WMD end use; preventing undesirable long-term strategic dependencies; and maintaining Dutch technological leadership. The second and third objectives mark a big leap in EU export control policy – they reflect a broader yet clear understanding of national security that encompasses economic security considerations historically not integrated into EU export control policy.

Building on this, and acknowledging the spread of coercive practices by other powers, member states should jointly affirm that specified economic security considerations can

legitimise national controls and that such risks ought to be considered for technology exports.

It is crucial that member states define such legitimate objectives together. Preventing the development of asymmetric dependencies and safeguarding European technology leadership in technology ecosystems is of real importance to European security – this could form one key objective. Doing so would mean, for example, that the export of key European components for advanced lithography machines, such as specialised lasers and optics, should also be controlled in order to defend European leadership in this choke point, a technology that provides the EU with invaluable deterrence and leverage.

The decision to control and restrict exports for these reasons would, of course, remain a member state competency. However, the new joint risk framework should form the analytical basis for such national measures and the analysis should be shared with all member states within the Dual Use Working Party when member states implement their own measures. Crucially, the member state must outline the expected effectiveness and possible implications – economic and political – of such national measures and other member states should have the opportunity to contribute to such analysis. To this end, the EU should also push forward the work of the Dual Use Working Party's new Technical Expert Group on emerging technologies. This group is tasked with identifying additional security-relevant emerging technologies that may require controls; it should contribute to any such analysis.

None of this would require a new regulation, which means it would also not be binding. Nevertheless, these measures together would greatly contribute to more informed, coherent, and strengthened EU export control policy adequate to today's European security challenges. Importantly, as with the EU's 5G toolbox, such a common framework would help legitimise additional controls, or indeed decisions to refrain from imposing controls on certain items. This framework would strengthen individual member states' position vis-à-vis third countries by, to some extent, Europeanising such decisions.

All that being said, the EU should agree common standards and refrain from controlling technologies that are currently immature – those that are below Technology Readiness Level (TRL) 1-4 – and can be considered 'neutral' because their potential use – including for military applications – generally only becomes clear at TRL 5-6. Trade in such immature technologies is often essential to international research cooperation and member states should commit to not restricting their export. For example, most quantum information technologies are currently below TRL 5 and should therefore not be controlled. But member states should consider additional controls for certain more mature quantum technologies where Europe is leading and that have clear defence applications, such as quantum sensing.

Adopt a strategic technology control instrument

Ultimately, despite its flexibility the EU's dual-use export control regime has its limitations. Importantly, the EU dual-use regulation does not allow for the implementation of export controls for non-dual use items, i.e. items that have purely commercial applications but have been identified as strategic, such as clean energy technologies. And current EU export control policy is not designed to control items destined for a specific country.

Meanwhile, the EU sanctions regime does allow for broader and country-specific restrictions, but is reactive in nature and carries more geopolitical risk. The unanimity required in decision-making also means sanctions are ill-suited for the sort of strategic measures now required.

The EU should therefore consider adding a new instrument to its toolbox. This instrument would provide the EU with more flexibility to impose export controls outside the conventional weapons, WMD, and dual-use scope and allow the bloc to address essential and economic security challenges. Under the new instrument, if the EU considered trade in a technology with a given country to be a risk to its essential security, it would have the power to restrict its export.

It should only use this for well-defined and targeted cases, such as when the export of a certain technology clearly contributes to the development of a strategic dependency or choke point to the EU's disadvantage.

The EU has recently adopted an ACI, which offers a blueprint for using export controls in a strategic manner. The ACI includes export controls in the list of possible countermeasures against coercion. While the ACI remains necessarily reactive to instances of coercion, it opens up new possibilities to use export controls strategically.

The process for deciding on the use of this tool should commence when a member state or the European Commission puts forward a proposal to control a certain item to a certain destination. Following receipt of the proposal, the commission should lead a joint analysis with the member state on the implications for EU security interests. If a key EU security concern is at stake, the council of ministers could vote by qualified majority to introduce EU-wide controls. This tool would thus be limited to a narrow set of instances, filling gaps left by other, existing tools. It would nevertheless help incrementally build a common strategic technology policy.

Draw up a Wassenaar interim arrangement

Beyond upgrading its own structures and instruments, the EU should look again at existing international security and economic architecture. This includes answering the question of whether current multilateral frameworks are adequate to safeguard European interests.

The CoCom and the WA export control regimes reflected the geopolitical, economic, and technological realities of the cold war and post-cold war era. But with Russia's full-scale invasion of Ukraine, the WA's days also appear numbered. Yet thus far the EU has failed to set out a common vision for the future of the WA and multilateral export controls.

Fully relying on the WA is certainly no longer an option – but nor is its complete abandonment. This is because the EU's export control framework, as well as that of many other allies, is closely linked to the WA and its lists of items that can be controlled. Any sudden departure from the WA would necessarily require significant changes to the EU's export control framework. Moreover, maintaining agreed controls among WA members remains a valuable contribution to international security. Abandoning the WA could alienate non-Western powers and countries from the global south, including India, which only joined the WA in 2017. China (not a member of the WA) has actively pushed the narrative that the West is unjustly restricting developing countries' access to technology through export restrictions. The EU must therefore be careful not to fuel this narrative by pushing for frameworks that will only find approval among Western allies.

Generally speaking, the WA has proven to be a good mechanism for aligning and improving the transparency of export control policies, including among countries that are not fully aligned.[2] And its sizeable membership has helped the WA be particularly effective at limiting the uncontrolled proliferation of conventional weapons and dual-use goods.

A broader reform of the WA would no doubt be desirable but is currently implausible given that Russia is a member and decision-making takes place by consensus. In any case, the lengthy process of reform would also prevent the EU and its member states from addressing pressing risks around emerging technologies.

So instead of retaining, reforming, or abandoning the WA, the EU and its allies should remain committed to the WA's current controls while building complementary multilateral mechanisms to control new dual-use technologies that have not been added to the WA list due to the issues described at the WA

Given this situation, the EU should draw inspiration from fallback mechanisms in other

dysfunctional multilateral organisations, such as the multi-party interim appeal arrangement at the WTO. The EU should therefore work towards establishing a Wassenaar interim arrangement (WIA) whereby all WA members willing to work together discuss and add additional technologies to a common WIA control list in a coordinated way. The WIA list would simply supplement the WA list with new technologies that require multilateral controls. Adopting this approach would circumvent Russia's blockades in the regular WA process.

Importantly, the WIA would not expand the WA's objectives – and would not include economic security considerations, for example – nor would it target specific countries. It would simply create a way to continue to exchange information and facilitate common controls on new technologies based on the principles and objectives agreed under the WA. As with the WA, the WIA and its control lists would not be legally binding, but members would use their national powers to implement the WIA's politically binding agreements. For the EU, this would probably mean member states using Article 4 or Article 9 of the recast dual-use regulation to add WIA items to the EU's common list in a coordinated way.

The WIA would not solve the many challenges related to potential coercion by China and its military modernisation. It would, nevertheless, make a strong contribution to the traditional nonproliferation objectives of the WA while reflecting the EU's support for broad multilateralism.

Forge an economic security alliance

Beyond a WIA and export controls, the EU must build new economic security alliances that can effectively address strategic technology control matters (and other issues such as strategic industrial policy, supply chain security, and economic coercion). While the EU has several new channels with allies which focus on individual trade and technology aspects, such as the EU-US Trade and Technology Council (TTC) and the EU-Japan Digital Partnership Agreement, in these dialogues it is missing a way to examine how strategic technology developments are affecting European and allied security. The EU's divided competencies on trade and security also leave the scope and relevance of these platforms to address strategic technology concerns in question.

While the US has leveraged its dominant position in the microchip supply chain, Europe has more possibility to co-shape strategic technology policy in other frontier technologies, where it is not yet clear which economies have achieved leadership positions and which are subject to choke points. The EU has a strong interest in ensuring emerging technology ecosystems of the future do not produce choke points that could be used against it. The focus of economic

security alliances must therefore be to coordinate with partners proactively to ensure these risks do not materialise or can be addressed together. This will require not only closer alignment of export control standards with economic security allies, but also the development of joint research projects, joint industry consortia, and joint investments in strategic technologies that ensure Europeans remain indispensable partners.

The G7 offers an important platform for the EU and some member states to receive and share information about the security implications of technology trade and to work on defining common standards for export controls, investment controls, and research security. The EU should support the development of a G7 economic security coordination mechanism in which different standing working groups could exchange information and build trust on export control standards, economic coercion, research security, and more.

At the same time, India, Brazil, and Indonesia are key players in emerging technology ecosystems and the EU should aim to engage these countries directly beyond the multilateral export control regimes or the bilateral free trade agenda. The TTC with India in particular is an important geo-economic milestone that can allow its participants to upgrade their relations on questions of strategic technology. The EU must ensure that it can develop a level of transparency and trust with India and others regarding its economic security and strategic technology policy, allowing for convergence, for example, by investing in capacity building in these countries.

A better balance is possible

With the proposals set out in this paper, the EU will be better equipped to defend its interests in this new geo-economic era. The bloc's interests certainly do not lie in contributing to the military build-up of its systemic rivals or allowing advanced EU technology to enable human rights violations. It is, however, in the EU's interest to strike a better balance between the benefits of trade and technological engagement with China and the threat of such trade fuelling the development of asymmetric dependencies on China in critical technologies. Although difficult to achieve, the EU should aim to arrive at more unity in security, trade, and technology policy vis-à-vis both China and the US, rather than exposing individual member states to external pressure. It is also in the EU's strong interest to ensure the integrity of the single market is not undermined as export controls proliferate. The bloc will benefit if it maintains and strengthens existing multilateral frameworks that help it achieve these objectives – but it should not shy away from establishing complementary multilateral and plurilateral mechanisms where existing frameworks fail.

About the authors

Tobias Gehrke is a senior policy fellow at the European Council on Foreign Relations, based in the Berlin office. He leads ECFR's Geoeconomics Initiative. His area of focus includes economic security, European economic strategy, and great power competition in the global economy.

Julian Ringhof is a policy fellow with the European Power programme at the European Council on Foreign Relations. His research focuses on the implications of digital and emerging technologies for international affairs, including the topics of EU digital diplomacy and EU technological sovereignty.

Acknowledgments

We extend our gratitude to the many conversations we had with experts from foreign and economy ministries, law firms, think-tanks, and businesses on the ins and outs of export controls. Special gratitude goes to Thomas Loussouarn, whose research support during his stay at the European Council on Foreign Relations, was instrumental to concluding this work. We also want to thank the many ECFR colleagues who have helped shape the content, language, structure, and visualisation of this brief: Jeremy Shapiro, Janka Oertel, Filip Medunic, Nastassia Zenovich, and Adam Harrison.

[1] Authors' interviews with EU export control officers, 2022-2023.

[2] Authors' interviews with EU export control officers, 2022-2023.

ABOUT ECFR

The European Council on Foreign Relations (ECFR) is the first pan-European think-tank. Launched in October 2007, its objective is to conduct research and promote informed debate across Europe on the development of coherent, effective and values-based European foreign policy. ECFR has developed a strategy with three distinctive elements that define its activities:

- A pan-European Council. ECFR has brought together a distinguished Council of over two hundred Members – politicians, decision makers, thinkers and business people from the EU's member states and candidate countries – which meets once a year as a full body. Through geographical and thematic task forces, members provide ECFR staff with advice and feedback on policy ideas and help with ECFR's activities within their own countries. The Council is chaired by Carl Bildt, Lykke Friis, and Norbert Röttgen.

- A physical presence in the main EU member states. ECFR, uniquely among European think-tanks, has offices in Berlin, London, Madrid, Paris, Rome, Sofia and Warsaw. Our offices are platforms for research, debate, advocacy and communications.

- Developing contagious ideas that get people talking. ECFR has brought together a team of distinguished researchers and practitioners from all over Europe to carry out innovative research and policy development projects with a pan-European focus. ECFR produces original research; publishes policy reports; hosts private meetings, public debates, and "friends of ECFR" gatherings in EU capitals; and reaches out to strategic media outlets.

ECFR is a registered charity funded by the Open Society Foundations and other generous foundations, individuals and corporate entities. These donors allow us to publish our ideas and advocate for a values-based EU foreign policy. ECFR works in partnership with other think tanks and organisations but does not make grants to individuals or institutions. ecfr.eu

ISBN: 978-1-914572-95-1. Published by the European Council on Foreign Relations (ECFR), 4th Floor, Tennyson House, 159-165 Great Portland Street, London W1W 5PA, United Kingdom.