

The US–China trade–tech stand-off

and the need for EU action
on export control

Clingendael Report

Brigitte Dekker
Maaïke Okano-Heijmans



Clingendael

Netherlands Institute of International Relations



Clingendael

Netherlands Institute of International Relations

The US–China trade–tech stand-off and the need for EU action on export control

Brigitte Dekker
Maaïke Okano-Heijmans

Clingendael Report
August 2019

August 2019

© Netherlands Institute of International Relations 'Clingendael'.

Cover photo: SRNL Developing Photonic Crystals © Savannah River Site / Flickr

Clingendael Report, August 2019. Research for and production of this report were conducted within the PROGRESS research framework agreement. Responsibility for the content and opinions expressed rests solely with the authors and does not constitute, nor should be construed as, an endorsement by the Netherlands Ministries of Foreign Affairs and Defence.

Unauthorized use of any materials violates copyright, trademark and / or other laws. Should a user download material from the website or any other source related to the Netherlands Institute of International Relations 'Clingendael', or the Clingendael Institute, for personal or non-commercial use, the user must retain all copyright, trademark or other similar notices contained in the original material or on any copies of this material.

Material on the website of the Clingendael Institute may be reproduced or publicly displayed, distributed or used for any public and non-commercial purposes, but only by mentioning the Clingendael Institute as its source. Permission is required to use the logo of the Clingendael Institute. This can be obtained by contacting the Communication desk of the Clingendael Institute (press@clingendael.org).

The following web link activities are prohibited by the Clingendael Institute and may present trademark and copyright infringement issues: links that involve unauthorized use of our logo, framing, inline links, or metatags, as well as hyperlinks or a form of link disguising the URL.

About the authors


Brigitte Dekker is a 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.


Maaïke Okano-Heijmans is a Senior Research Fellow at the Netherlands Institute of International Relations 'Clingendael' in The Hague. She is a Scientific Coordinator of the Asia-Pacific Research and Advice Network (#APRAN) for the European Commission and the European External Action Service.


Caspar Price is a student in the Master of International Relations and Diplomacy (MIRD) programme, offered jointly by Leiden University and the Clingendael Institute. He provided valuable research assistance, including to this project, during his internship with Clingendael from March-July 2019.

The Clingendael Institute
P.O. Box 93080
2509 AB The Hague
The Netherlands

Follow us on social media

 @clingendaelorg

 The Clingendael Institute

 The Clingendael Institute

Email: info@clingendael.org

Website: www.clingendael.org

Contents

Executive summary	1
Introduction	2
The US push for export control reform: ECRA	5
Export control and emerging technologies	8
From dual-use to omni-use and omnipresent	9
At stake: supremacy, standards and norms	10
Comparing the US and Dutch approaches	12
The Netherlands evolving...	14
...and the US moving yet further ahead	15
Potential levels of action for the Dutch government	18
US-Netherlands cooperation	18
European Union cooperation	19
The Wassenaar Arrangement and beyond	21
Trusted communities	22
<i>SWOT analyses</i>	
ECRA and US-NL cooperation	24
European Union cooperation	25
Wassenaar and beyond	26
Trusted communities	27
How to move forward from here?	28

Executive summary

As the great power rivalry and (technological) trade conflict between the United States (US) and China intensifies, calls for an export control regime tailored to so-called emerging technologies are growing. In August 2018 the US government announced the *Export Control Reform Act* (ECRA), seeking to limit the release of emerging technologies to end uses, end users and destinations of concern.

The contest is on for the leader in the development and use of emerging technologies, but also for shaping norms and writing the rules for their use. This requires the Netherlands and other EU member states – in coordination with key stakeholders from business and academia – also to redouble their efforts and recraft their own approach to export controls of so-called ‘omni-use’ emerging technologies. The Netherlands and the European Union (EU) share the United States’ concerns about the proliferation of non-Western norms and standards through emerging technologies. They do not, however, wish to use export control as an instrument to curb China’s rise as a technological power.

Set against this context of the United States’ push for reform, this Clingendael Report outlines four levels of action in the field of export control for the Dutch government to pursue in parallel: bilateral cooperation between the United States and the Netherlands; European Union-level action; action within the multilateral Wassenaar Arrangement; and nascent trusted communities. While continued bilateral dialogue with the US is important, now is the time to engage actively on the EU level to create a truly efficient EU-wide export control system for emerging technologies. Next to a coordinated response to the US shift, adoption of the proposed EU autonomous dimension and introduction of electronic licensing are crucial steps. These steps are required to uphold European norms for the use of certain technologies challenged by China, and to shield against US extraterritorial jurisdiction, which could well result in broad sanctions against European companies and disruption of the value-chains that businesses depend upon to innovate and competitively sell their products.

Introduction

As the trade war between the United States (US) and China evolves into a state of permanent conflict, it is apparent that a defining feature of the deepening geopolitical contest is technology. The contest is on for the leader in the development and (global) use of emerging technologies, and thereby the writing of norms and the rules for their use. In this context, the (screening of) foreign investments and the question of how to deal with China's telecom giant Huawei keep hitting the headlines, but few are aware that the issue of export control is equally, if not more, challenging.

Foreign direct investment (FDI) screening and export control may be considered as two sides of the same coin, as screening checks investments into a country against national or economic security standards, while export control does the same for exports that leave a country. Today's discussion in these fields is shaped by concerns that technologies being developed indigenously by China may undermine the national or economic security of Western countries, including the Netherlands.

Responding to this challenge, the US government today seeks to protect the technological advantage that the United States still has over China in high-tech and intellectual property (IP)-sensitive industries. Some US officials seem determined to contain China, or at least to slow its rise significantly until the US believes it has guaranteed its own technological superiority. Next to tariffs and investment screening, Washington now seems intent to use export controls as a tool to curb China's technological rise.

In a fashion reminiscent of traditional dual-use export control, Washington is pushing through expansive domestic regulations governing the export of emerging technologies.¹ The proposed reforms to control the export of US technologies and products, outlined in the *Export Control Reform Act* (ECRA), largely mirror the intelligent manufacturing sectors identified in the *Made in China 2025* (MIC2025) industrial policy.² In all this, Washington seeks to ensure not only its competitive advantage but also its power to

1 For a US perspective on the ('oftentimes covert and coercive') methods used by Chinese companies to acquire valuable technology, intellectual property and knowhow from US firms, see [this report](#) by the US-China Economic and Security Review Commission, 6 May 2019.

2 *GBTimes*, ["Made in China 2025" Plan Unveiled to Boost Manufacturing](#), 20 May 2015. The plan highlights ten priority sectors, including next generation information technology; high-end numerical control machinery and robotics; and aerospace and aviation equipment.

design the standards and norms of the future. Importantly, the United States demands support from its (alliance) partners in its trade–tech stand-off with China, as illustrated by the call to ban Huawei from providing 5G infrastructure.

Even though this unilateral move is aimed at China, the Netherlands and other European Union (EU) countries will also be impacted by US export control reforms, which will require action on their part. While European countries, including the Netherlands, share the United States' concerns regarding the application of certain emerging technologies by the Chinese government and the proliferation of Chinese norms and standards through the (re-)export of these technologies, they do not support US attempts to contain China's technological rise in this absolute way. The proposed measures have the potential to restrict significantly operations of companies working in and with the US and, as an extension, to fragment global value-chains and research and innovation networks.

These reforms will impact trading nations with a strong focus on high-technology sectors most drastically, including the Netherlands, which is home to leading companies in emerging technologies, including semiconductors, photonics and quantum technology. In charting a path forward, the Netherlands – as an EU member state – must now decide how and to what extent to engage actively with the US on its push for export control for emerging technologies.

Similar to the EU, Japan – with its strong high-tech sector – will be heavily affected by the (extraterritorial) effects of US policies. Generally seen as a like-minded country with shared concerns and an approach similar to that of EU member states, Japan stands out as a valuable partner in dealing with the push for reform in Washington, even if this is complicated by economic competition in the high-tech sector. Japan's imposition in July 2019 of export controls on South Korea, set against a context of continued political tension between the two neighbours, is seen by some as a sign that the politicisation of export controls goes beyond the US alone. Although worrying, the fact that Tokyo's controls appear to be compliant with World Trade Organisation (WTO) rules suggests that for the EU and its member states the benefits of cooperating with Japanese stakeholders should still prevail.

This Clingendael Report aims to contribute to today's ongoing debates about export control for emerging technologies by outlining key developments – triggered by the US push for new legislation with its Export Control Reform Act – as well as differences between the US and the Netherlands in strategic thinking underpinning policies in this field. Addressing this underexposed issue in the current discussions about trade, technology and innovation will help policymakers to put the issue in the broader Dutch strategic agenda.

Going forward, the Netherlands should pursue four parallel tracks to shape tomorrow's regime for export control on emerging technologies: bilateral cooperation with the US; speeding up reforms in the multilateral framework, especially the Wassenaar Arrangement; strengthening the EU's role and mandate; and creating trusted communities. The detailed analyses of these four paths presented in this Clingendael Report aim to elucidate the pros and cons of choices that policymakers need to make in the months and years ahead.

Just as the EU has cooperated with the US on investment screening, through information exchange, regular consultation and cooperative action, the same must occur now regarding export control. Next to the bilateral and multilateral/multi-stakeholder tracks, improved coordination and EU-level action are thus particularly important to uphold European norms and to shield against US extraterritorial jurisdiction. The global reach of US export control laws could well result in broad sanctions against European companies and disruption of the value-chains that businesses depend upon to innovate and competitively sell their products.

The US push for export control reform: ECRA

Countering Chinese ambitions to dominate in technological innovation has become a defining feature of US economic, security and defence strategies, particularly since the inauguration of US President Donald Trump in January 2017. Although concerns over Chinese forced technology transfer and IP theft are certainly not new in the US, China's ambitious and far-reaching technology drive, as outlined in MIC2025, sent shockwaves through American governmental, strategic and security circles. As outlined in the United States' 2017 *National Security Strategy* (NSS),³ the US now regards China as a revisionist power that seeks actively to challenge the power, influence and interests of the US by eroding its prosperity and security.

In a bold step to update its export control regulations to include such emerging technologies, the US government announced the ECRA as part of its *National Defense Authorisation Act for Fiscal Year 2019*.⁴ ECRA enhances the priority and impetus for the US Commerce Department to designate (emerging) technologies for export control. It is motivated by concerns regarding the release of critical, emerging technologies to end uses, end users and destinations of concern, and highlights the US approach to countering the potential security risks posed by growing Chinese technological clout and capabilities.

The specific details of this (domestic) legislation have been the subject of intense public and private debate. In November 2018, the US Commerce Department's Bureau of Industry and Security (BIS) called for comments on the set of fourteen emerging technologies⁵ that it tentatively identified for control. This set includes Artificial Intelligence (AI), robotics, additive manufacturing (such as 3D printing) and advanced surveillance technologies. The public comment period closed in January 2019 and, to date, over 240 comments have been posted publicly,⁶ including submissions from

3 [National Security Strategy \(NSS\)](#), Washington, DC: White House, 2017.

4 A second key part of the National Defense Authorisation Act (NDAA) is the Foreign Investment Risk Review Modernisation Act (FIRRMA). Although ECRA and FIRRMA – i.e. export control and investment review – are closely intertwined, the focus here is on export controls (to be) governed under ECRA: *H.R. 5515, National Defense Authorisation Act for Fiscal Year 2019*.

5 Advanced Notice of Proposed Rule Making (ANPRM), [Review of Controls for Certain Emerging Technologies](#), 19 November 2018.

6 Comments on Advanced Notice for Proposed Rule Making, [Review of Certain Technology Transfers](#).

businesses (and their federations) and other relevant parties (including government). Comments were solicited on all elements of the process, from how to define emerging technology and apply it to specific technologies, to how far new technologies should be allowed to develop before they are considered for controls. The new regulation is expected to enter into force in 2020.⁷

Regulations that will follow from this process will have great implications for the operations of Dutch companies within the US. In fact, the impact extends beyond US borders, because of the extraterritorial jurisdiction of US law. This means that foreign products containing more than 25 percent of US material may require a re-export license from the United States.⁸ Additionally, the US routinely – and selectively – bans exports to actors on the so-called BIS Entity List, which includes foreign businesses, research institutions, government and private organisations and individuals that are subject to even more scrutinous license requirements for the export, re-export and/or transfer of specified items.⁹ One of the most prominent cases of such US extraterritorial jurisdiction in action occurred in May 2017 when ZTE Corporation, a Chinese telecommunications firm, agreed to a total penalty of US\$ 1.19 billion in a settlement agreement with the US Department of Justice and the Department of Commerce for violating US export laws and sanctions.¹⁰ As elaborated below, in May 2019 the Trump administration started to apply further pressure on businesses outside the US to comply with its export control laws by applying penalties on companies that violate US export laws.

The extraterritorial jurisdiction enshrined in the US Export Administration Regulations (EAR)¹¹ is contentious in international law. Nevertheless, companies whose products are subject to this law frequently adhere to EAR provisions and cease trading with banned entities to avoid punitive measures by the US.

7 Closely linked to emerging technology, another category of technology that has yet to be defined is ‘foundational technology’, such as semiconductor technologies, which are technologies that can enable progress and applications in a variety of problem domains. More details [here](#).

8 The extraterritorial application of US law in the case of export controls is of relevance to any company anywhere that is re-exporting American goods or technology; incorporating technology previously exported from the US; and by persons subject to the jurisdiction of the United States.

9 US Department of Commerce, Bureau of Industry and Security, *Entity List – Supplement No. 4 to Part 744 of the Export Administration Regulations*.

10 These same penalties could apply to any company whose goods contain components of US origin, and whose end use and end users exist outside of the US. Mondaq, [Non-US Companies Beware: US Export Laws May Apply to You](#), 10 July 2018.

11 Export Administration Regulations, [Bureau of Industry and Security](#).

The US thus has a much more powerful tool reserved than the tariffs currently applied to the Chinese market. These regulations could, however, also potentially hinder US interests, as companies trading products that contain US material will be banned from certain lucrative markets.¹² In the long run, this could result in reduced demand for American products, impacting these companies' profits and growth.

Recent history shows that the US is willing to bear such costs. During the Cold War, the US founded the Coordinating Committee for Multilateral Export Controls (CoCom) to coordinate restrictions on the export of military items and technology to the Soviet communist bloc.¹³ CoCom is now seen as the foundation for the export control regime that exists today. That said, today's measures will have far greater implications for existing trade, as well as research and innovation networks. After all, economic integration and interdependence between the US and China and the importance of trade with China to the rest of the world are far greater now than at the time of the Cold War with the Soviet Union.

12 Bloomberg, [Trump Wields More Powerful Weapon than Tariffs in Trade War](#), 23 May 2019.

13 ['Multilateral Export Control Policy: The Coordinating Committee \(CoCom\)'](#), Technology and East–West Trade Advisory Panel, 1979.

Export control and emerging technologies

Export control is best described as measures that governments implement to limit the spread and/or use of certain goods and services with the ultimate aim of protecting national security and promoting foreign policy. Restrictive measures – primarily customs and licensing – implemented by the government currently cover two categories: (conventional) military goods;¹⁴ and (traditional) dual-use items, consisting of goods, software and technology that can be used for both civilian and military applications.

Governments can implement and design their own export control systems based on the lists conducted by four international regimes that currently exist: the Wassenaar Arrangement (for conventional arms and dual-use goods and technologies); the Nuclear Suppliers Group (for nuclear-related technology); the Australia Group (for chemical and biological technology that could be weaponised); and the Missile Technology Control Regime (for aerial vehicles capable of delivering weapons of mass destruction). By promoting transparency and greater responsibility in transfers, these arrangements aim to contribute to regional and international security and stability.

The focus of export control (regimes) on conventional military technologies may have seemed natural during a time when wars were fought between militaries. It is less so today, however, as power rivalry moves into (cyber)space and involves control (and potential disruption) of societies at large. As the only international arrangement on export controls for dual-use goods and technologies, the Wassenaar framework is challenged with keeping up with rapid changes – in technologies as well as in modes of power.¹⁵ Established in 1996, the regime now counts 42 members, including all of the EU member states (except Cyprus), the United States, Japan, Russia and India, but not China. Its list of restricted technologies primarily consists of items that cross borders physically, such as remotely operated vehicles, explosive material or technical assistance that is related to the development of nuclear weapons. Members gather twice a year to discuss current affairs and potential dual-use items, with a view to updating the list of restricted technologies.

14 The Netherlands ratified the following export control regimes for strategic goods: Chemical Weapons Convention (CW); Biological and Toxin Weapons Convention (BTWC); Non-Proliferation Treaty (NPT); Arms Trade Treaty; Convention on Cluster Munitions; Ottawa Convention; Australia Group; the Missile Technology Control Regime; Nuclear Suppliers Group; and the Zangger Committee – plus the Wassenaar Arrangement, which addresses dual-use items. [Handboek strategische Goederen en Diensten](#), 2018.

15 [User Guide on Strategic Goods and Services](#).

From dual-use to omni-use and omnipresent

To add clarity to the essence of what today's export control reform is about, it is useful to distinguish two additional categories that governments may wish to control, besides military and dual-use items: critical infrastructure, such as gas, water and light; and emerging technologies, or omni-use technologies, as we prefer to label them.

Critical infrastructure is deemed of paramount importance for national security as well as the economic safety of any country. Companies delivering these items should be protected against hostile takeovers at all costs, as they are critical for a country's sovereignty and functioning. Export control policies contribute to this purpose by making critical infrastructure resistant to state threats, such as the export of strategic dual-use goods or technologies with potential (indirect) undesirable consequences.¹⁶ In the 21st century, the increasing reliance on information and communication technologies (ICT) to secure critical infrastructure complicates these considerations. The controversy surrounding the adoption of Chinese 5G technology in critical government networks is a clear example of this dilemma.

Emerging technologies are increasingly digital technologies that can be transferred between countries without physically crossing national borders, thereby bypassing the customs authorities that are normally tasked with dual-use export control. The ease with which software can be developed and transmitted worldwide highlights the need for a modern approach to the regulation of its trade, because software underpins many of the technologies currently subject to debates on export control reform. More so than traditional 'dual-use' technologies, emerging technologies could be used for a range of purposes simultaneously, from improvements in healthcare and infrastructure to exceptionally efficient surveillance and military operations. Moreover, emerging technologies are integrated at all levels of society, especially amid the increasing convergence of software and information flows, making them also omnipresent in society.¹⁷ One can therefore speak about the 'omni-use' of those technologies rather than a clear dual-use, whereby most countries agree on the potential civilian and military purposes of an item.

The extremely complicated composition of such technologies, consisting of multiple components that are themselves omnipresent, makes them difficult to subject to government oversight. These emerging technologies – such as AI and 3D printing – are currently not fully controlled by any export control system and, despite growing

16 For the Dutch case, see NCTV, *Nationale Veiligheidsstrategie*, 2019.

17 For example, artificial intelligence (AI) consists of hardware, datasets and software. Each of these three components are omnipresent – that is, the same hardware, datasets and software are individually present across a wide range of products.

calls to regulate them, many of their components can be traded with relative ease. Hence, considering the rapid development of emerging technologies, the current dual-use export control regime is now facing two challenges: keeping up with regulation of the new (applications of) technologies and their classification; and the digital nature of the new technologies making customs regulations obsolete. These definitional and normative debates concerning the omni-use and omnipresence of emerging technologies complicate discussions and timely policy adjustments on export control regulations within the Wassenaar Arrangement. Agreeing on what constitutes ‘good’ and proportional regulation is further confounded by the fact that every actor’s opinion is informed by a combination of economic, ethical, legal, political and strategic considerations.

At stake: supremacy, standards and norms

These considerations precisely underpin the underlying reason for the United States’ push for action: an increasing norm division between the US and China and the possibility of China spreading, regulating and controlling its norms and standards through emerging technology. The potential for non-civilian use of emerging technologies is much more diverse and contested compared to dual-use technologies. There is a vast grey area where certain actors’ views are informed by ethical questions, such as the right to privacy or balancing the rights of the individual with the collective. While the anti-competitive and mercantilist character of MIC2025 is concerning on its own, American and European governments and businesses are particularly troubled by the accompanying proliferation of Chinese norms and practices in high-technology sectors, especially relating to network intrusion software and surveillance technologies.¹⁸ Seen from this perspective, and considering today’s rapid pace of innovation combined with high levels of trade, the US push for new regulation is unsurprising.

The Netherlands shares US concerns regarding the proliferation of non-Western norms and standards through emerging technologies. It does not, however, support US attempts to curb China’s rise as a technological power by way of imposing export controls. In May 2019, the much anticipated China Strategy of the Dutch government specifically acknowledged the ongoing concerns relating to espionage, cyberattacks and involuntary knowledge transfers, which in many cases can be directly attributed to China.¹⁹ In this light, it is also noteworthy that the Dutch government stopped issuing licences to a company that was exporting sensitive surveillance equipment

18 See, for example, Cristina Maza, ‘Experts Warn China’s Technology Could Spread Authoritarianism around the World’, [Newsweek](#), 17 May 2019.

19 Stefan Blok, Speech [on the presentation of the Dutch government’s China strategy by the Dutch Minister of Foreign Affairs](#), 15 May 2019.

and technology products to China and Hong Kong as early as September 2018, on the grounds of privacy and human rights protection.²⁰ Hence, a new export control regime is not only necessary to protect the Dutch national, economical and international security in the 21st century, but also to protect our Western standards and norms during the fourth industrial revolution.²¹

20 'How Tensions with the West are Putting the Future of China's Skynet Mass Surveillance System at Stake', [South China Morning Post](#), 23 September 2018.

21 The fourth industrial revolution is a way of describing the blurring of boundaries between the physical, digital and biological worlds. It is a fusion of advances in AI, robotics, the Internet of Things (IoT), 3D printing, genetic engineering, quantum computing and other technologies. See Klaus Schwab, [The Fourth Industrial Revolution](#), World Economic Forum, 2016.

Comparing the US and Dutch approaches

The rapidly evolving complexity of global value-chains is accompanied by a proliferation of real and perceived security threats to which governments have developed their own security strategies. Focusing on possible avenues for cooperation with the United States, comparing US and Dutch economic and strategic considerations in the area of export control illuminates areas for cooperation and of divergence.

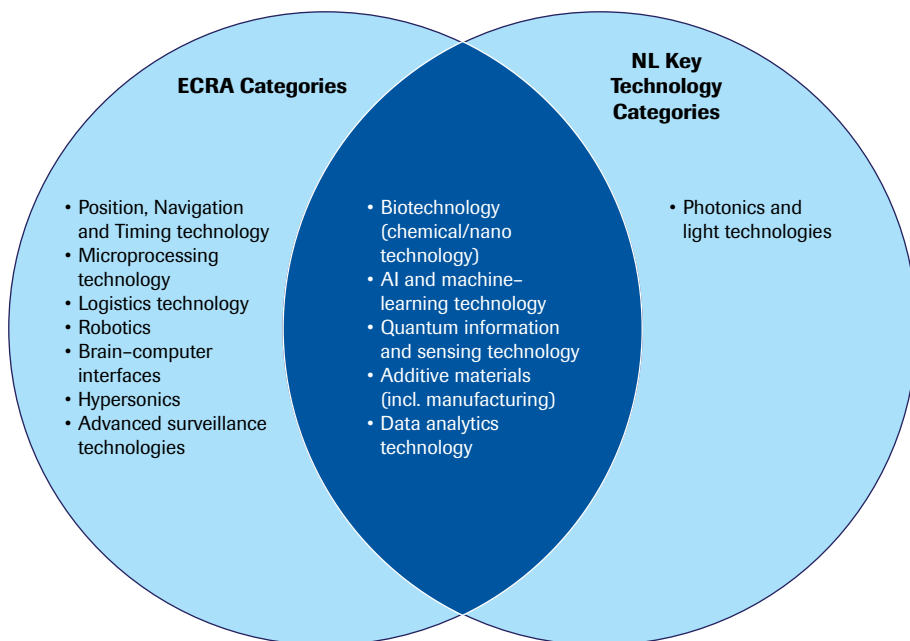
The concerns of many Dutch stakeholders about the (long-term) implications of China's use and control of emerging technologies overlap with those of the United States. In a similar process to the US Department of Commerce's call for public comment, which identified fourteen technological categories of interest, the Dutch government has developed a similar list of so-called 'key technologies'.²² While the categories identified by each counterpart differ, the actual technologies covered by these categories reveal a significant overlap, as portrayed in Figure 1.²³

However, the differences between the Dutch and US understandings of economic and national security, and how to mitigate risks and protect economic and national interests, complicate Dutch efforts to cooperate with the United States, as well as the difference in relations between the government and industry in each case. Moreover, the approaches envisaged in the Netherlands are not fully aligned with the United States' explicitly China-focused approach.

22 Elsevier Research Intelligence, [Quantitative Analysis of Dutch Research and Innovation in Key Technologies: A Report for the Ministry of Economic Affairs and Climate](#), 2018.

23 For the full lists, see [here](#) and [here](#).

Figure 1 Overlap in technology categories of US and Dutch technology



In the United States and the Netherlands, national security interests are closely tied to successes in the international trading system. A significant overlap exists in both countries between economic security and national security. However, the Dutch government, like most other EU member states, makes a clearer distinction between the two. Economic security relates first and foremost to the undisturbed functioning of an effective and efficient economy that generates prosperity for the citizens of a country. Achieving economic security in a globalised world is a core strategic interest for the Netherlands because of its extensive integration into the global economy: in 2017, for example, exports of goods and services accounted for 86 percent of the Dutch GDP.²⁴ Meanwhile, national security relates to protecting the Netherlands' vital interests against various threats that could disrupt society, ranging from terrorist threats to pandemics and floods.²⁵

24 [World Bank](#).

25 See <https://www.inspectie-jenv.nl/toezichtgebieden/n/nationale-veiligheid>.

The Netherlands evolving...

Although a distinction between national and economic security is still defining Dutch policy, there has been a gradual convergence of the two concepts in recent years, visible in the *National Security Strategy* published by the Dutch government in 2007 and 2013.²⁶ This convergence has also become more evident through the various *Annual Reports* of the Military Intelligence and Security Service – which commonly pays substantial attention to dual-use as well as to China – and the *Integrated International Security Strategy* (IISS) published by the Dutch Foreign Ministry.²⁷ The IISS provides a threat analysis of the most urgent security threats facing the Netherlands. A core feature is its direct acknowledgement of the opportunities and risks that accompany developments in emerging technologies and the need for joint innovative strength of knowledge institutes, companies and government policy input, again showing the increased overlap between economic and national security. Moreover, the call for cooperation with the private sector emphasises the importance of an exchange of knowledge and skills between companies and knowledge institutions and the role that these connections play in protecting Dutch economic security interests.

In the United States, the overlap between economic and national security is much more evident and originates from the industry’s ability to link IP protection to innovation, innovation to competitiveness and competitiveness to national security. In the 1980s, the US semiconductor and chemical industries were able to secure greater IP protection in the trade deals that the US signed to counteract competitiveness lost through tough export control laws.²⁸ Hence, this linkage blurred the line between US economic and national security policy, guaranteeing government support for those companies and integrating economic security within national security.

Today, US concerns relate to technologies and items that foreign powers are likely to seek to eliminate the United States’ current supremacy in high-technology or IP-sensitive industries. Such concerns are shared by the US defence, industry and intelligence communities, and the provisions outlined in ECRA thus seek to address these concerns under one roof. However, the measures outlined in ECRA are causing the first signs of divergence between government and company interests, highlighting the US domestic debate on economic and national security interests. While US industry agrees with the IP-protection aspect of the US export control laws, it opposes many of the measures imposed on national security grounds. For example, US industry prefers

26 Available [here](#) (2007) and [here](#) (2013).

27 Dutch Ministry of Foreign Affairs, [Integrated International Security Strategy 2018–2022](#).

28 See Susan Sell, *Private Power, Public Law: The Globalisation of Intellectual Property Rights*, Cambridge University Press, 2003.

investment arbitration courts in instances of IP theft, while the US government enforces sanctions. Moreover, US industry argues that the regulations are defined too broadly and should instead target specific technologies of concern. Otherwise, the new export control system could disrupt the value-chains that businesses depend upon to innovate and competitively sell their products.²⁹ These concerns overlap with Dutch concerns regarding the measures currently outlined in ECRA.

...and the US moving yet further ahead

In May 2019, amid intensifying conflict and stalling trade negotiations between the US and China, President Trump unveiled a new instrument of export control. Executive Order 13873 prohibits high-risk information technology transactions with entities designated as a 'foreign adversary',³⁰ loosely empowering the US Secretary of Commerce to block any trade deemed to be against the United States' national interest. Blocking trades on a transactional basis allows the US government to target specific actors of concern rather than entire industries – thereby satisfying some of the business community's concerns, while simultaneously addressing perceived national security risks.

Similar to ECRA, extraterritorial jurisdiction applies also to cases falling under this Executive Order. As the US starts to apply this rather selective instrument of export control, however, a risk of global decoupling arises. This relates to the concern that global companies – allied or adversarial – will be forced to reorganise their supply chains (or corporate structures) in such a way to avoid the 25 percent threshold laid out in EAR, by either working within the 'US sphere' or outside it. An overuse of extraterritorial jurisdiction may harm US interests in the long run as well, through reduced US presence and influence in certain crucial fields.

29 Such concerns were raised during the period for public comment on ECRA by many industry associations, notably the [Semiconductor Industry Association](#) and, in a joint submission, the [Association for Computing Machinery and the Computing Research Association](#).

30 This executive order loosely defines foreign adversary as 'any foreign government or foreign non-government person engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons'; Executive Order 13873, [Securing the Information and Communications Technology and Services Supply Chain](#), 15 May 2019.

A fine line: protecting but not suffocating businesses

The relationship between the US government and companies based in the US has long served as an effective engine of innovation and growth. However, certain aspects of US export control law (and proposed updates contained in ECRA) highlight divergences between the actor types about how to balance economic and security concerns in the coming years, even when those are not strictly divided in US policies. In 2015, the US banned the sale of Intel chips to Chinese entities over concerns of their use in supercomputers with potential military application. While the US chip giant complied with the restrictions, arguments against such measures usually cite the fact that these entities will be able to source chips from elsewhere, or develop their own to bypass the restrictions. Furthermore, the incident struck at the heart of Intel's business model and the company has still not fully recovered; it has since effectively lost its monopoly position as competitors such as Samsung become more influential in the semiconductor market.³¹ Since the ban, China's top state-backed chip-maker has ordered the very same equipment used by Intel to develop its own chips – from ASML, the world-leading Dutch manufacturer of high-tech semiconductor lithography systems.

This case serves as one of many examples of the restrictions placed on US companies resulting in other companies filling the void left by the absence of US companies. In the absence of leading US companies in high-tech markets, partnerships such as German–Chinese Innovation Partnership will flourish, which representatives of German industry have said will primarily strengthen Chinese competitors.³²

Indeed, parts of US industry are concerned that while new export control regulations are designed to bring innovation and value-chains back within reach of the US, they may have the unintended side effect of spurring on competitors in China and Europe to fill the void left by American companies. This could potentially impact the United States' status as the world leader in technology as the 21st century progresses.

Summing up, the discrepancy between the US and Dutch understandings of national and economic security complicates talks between the Dutch and US governments on ECRA and its consequences, as well as on the reform of export control regulations more

31 [Samsung Topples Intel to Become World's Largest Chipmaker](#), January 2018.

32 [Industry 4.0: Will German Technology Help China Catch Up with the West?](#), Merics, April 2015.

broadly. While the Dutch government is still contemplating its next steps, it shares with US businesses the concerns about the (too) broad scope of ECRA and the specific focus on China underpinning that regulation.

Today's divergence between US industry and the US government could thereby include an opportunity for the Dutch government to mediate between these two parties with the experience of both economic and national security. When considering how to respond to the broadening scope of US export control laws, Dutch policymakers should also keep in mind the Chinese policies that sparked these reforms in the first place. The Dutch intelligence agency has included warnings in its annual threat assessments for the last few years that China is targeting technology companies in the Netherlands, as it does in other countries, for IP theft.³³

33 [AIVD Annual Report 2017](#); [MIVD Annual Report 2018](#).

Potential levels of action for the Dutch government

Although the particulars of the new US export control regulations outlined in ECRA are not yet certain, the Netherlands' close linkages to US industry mean that the Netherlands will be considerably affected. Consequently, the Dutch government must reconsider its own approach to export control in order to deal with rapid technological developments and the changing international context.

Four paths forward in this new era of great power politics and divergence in norms are schematically presented below by outlining the strengths, weaknesses, opportunities and threats (SWOT) of each level of action. These are: cooperation with the US; EU and intra-European cooperation; the Wassenaar Arrangement and beyond; and so-called 'trusted communities' that facilitate information exchange and best practice learning among key stakeholders, especially in business and academia. The SWOTs are schematically presented on pages 24-27.

US–Netherlands cooperation

Although small in size, the Netherlands is a global leader in various high-tech sectors, making it an important bilateral partner for the US. Building on this, future regulatory coordination could be deepened between the two countries to help businesses based in both the US and the Netherlands. Bilateral engagement and cooperation between the Netherlands and the US must therefore be part of the Dutch government's response to the United States' export control reform proposals.

Especially with the United States' focus shifting from EU engagement to bilateral cooperation with EU member states, the Dutch government can push for constructive dialogue between the US and the Dutch government and businesses. Bilateral talks should address the differences in national and economic security interpretation, explore new avenues to address the concerns of industries affected by export control regulations, and share best practices. Moreover, in order to have fruitful discussions in the future, the Dutch government needs to decide whether and how it wishes to shape or eventually adopt the regulations included in ECRA. A significant degree of regulatory coordination already exists between the Netherlands and the US with regard to export control of dual-use items, and the Netherlands can only engage in discussions as an equal partner when it presents a clear position on future export control regulations.

That said, bilateral agreements are no substitute for an effective, multilateral export control regime for emerging technologies in Europe. While improved alignment will promote US–Dutch business cooperation, effective Dutch export control requires that the Schengen zone adopts the same regulations. After all, if only the Netherlands adopts specific export control regulations for emerging technologies, companies can engage in so-called ‘licence shopping’ – that is, using the free flow of goods, services and persons within Schengen to export technologies that are subject to export regulations in one EU member state to another EU member state Schengen country that has not (yet) adopted such export control regulations, in order to allow for export to a third country. By using another country as an intermediary, emerging technologies can then still be exported outside the Schengen zone, thus avoiding strict export control regulations of specific EU member states. Hence, while US–Dutch bilateral cooperation can address the differences and possible risks for and with the affected industry in both countries, EU involvement is a necessary condition for an effective export control system. However, while export control is heavily debated in the US, it is not yet prioritised in Europe.

European Union cooperation

A coherent EU policy would be a stronger stance against the extraterritorial jurisdiction of the US and a powerful and a respectable force for multilateral reform. First and foremost, the EU and its member states should understand, respond and adjust to the changes in US policies and approaches. This includes preparations for a possible expansion and acceleration of the extraterritorial enforcement of the US export control law that will result in broad sanctions against European companies. Moreover, EU member states should make haste with existing initiatives to strengthen cooperation, coordination and monitoring of export control across Europe.

As a frontrunner in the field, the Dutch government and Dutch high-tech companies are well placed to appeal about this cause to other EU member states and institutions. Dutch company ASML, for example, is concerned that its lithography systems could be subject to tightened US export control policies. This should be a worry to others in Europe as well, as a hit to ASML (the end-producer) would negatively affect all companies involved in the company’s innovation ecosystem, which crosses EU internal borders. The growth of the European industry and jobs in more than a few EU member states would thereby be affected, also through (declining) tax revenues.

Already in September 2016, the European Commission adopted a proposal to modernise the EU export control system.³⁴ However, EU-wide technology and data discussions are not gaining the momentum they need, and the EU has no mandate in this field to act on behalf of its member states. EU member states remain preoccupied with national concerns – importantly, economic interests, which still trump the clear benefits of pooling resources and aligning approaches.

The Netherlands recognises the need to act, but for now wishes to have the debate domestically before bringing it to the EU-level. Other EU member states are not inclined to pursue the issue because it does not concern their industries much. As a result, export control regulations are still barely mentioned in recent strategic documents published in Brussels – specifically in *EU–China: A Strategic Outlook* and the *EU Industrial Policy* – or at the national level – for example in the notes of the Dutch government on competitiveness and China strategy.³⁵

In this context, the Dutch government can draw EU member states’ attention to the demands of this new US export control regime and make endeavours to align thoughts on a new export control regime within the EU. This includes equipping the EU with capacity of its own, such as through an electronic licensing system that helps prevent licence shopping. Also needed is a mandate to discuss and cooperate on export control with third parties – especially the US – on behalf of the EU member states.

This will be a challenging task, as various EU member states do not have a high-tech sector themselves and many have diverging interests and relations with both the US and China. Even so, taking the frontrunner position now – rather than later, after having defined its own position – can benefit the Netherlands in the long run, as it will engage all member states throughout the process rather than present them with a ‘fixed’ Dutch position for others to follow. It will also ensure that EU member states that now see little need for (joint) action will recognise that – because of Schengen and innovation ecosystems that cross internal borders – this does concern all EU member states.

Additionally, greater coordination between a leading group formed by the Netherlands, Belgium and Germany could serve as a stepping-stone for EU-wide activism on these matters. For example, the semiconductor industry ties these countries together through

34 Consisting of two main parts, this proposal includes more than 50 amendments to the current system, as well as the establishment of a European autonomous dimension. See European Commission, [Proposal: Setting Up a Union Regime for the Control of Exports, Transfer, Brokering, Technical Assistance and Transit of Dual-Use Items](#), 28 September 2016.

35 European Commission, [EU–China: A Strategic Outlook](#), 12 March 2019; European Political Strategy Centre, [EU Industrial Policy after Siemens–Alstom](#), 18 March 2019; Government of the Netherlands, [The Netherlands and China: A New Balance](#), 15 May 2019.

its supply chain and innovation ecosystem. The efficiency and effectiveness of pushing for EU action in this formation could thus be further explored. In doing so, care should be taken not to run too far ahead of others, as a proposal initiated only by EU member states with advanced economies could encounter resistance from Southern, Eastern and Central European EU member states that do not have a high-tech sector themselves. After all, the positions and interests of many of these countries towards the US and China differ substantially from those of advanced economies in (North)Western Europe.

While pushing for EU-wide talks on the consequences and a desirable response to US initiatives in the field of export control, the Dutch government should also pursue strengthening the existing initiatives and networks, including the Dual Use Coordination Group, a major initiative that was part of the 2016 modernisation proposal.³⁶ This coordination group consists of experts from various fields and all EU member states who meet regularly and are developing the IT infrastructure that will underpin the EU's planned autonomous export control regime. Current EU-wide discussions are geared towards implementing a fully functional electronic licensing system, which would partially detach the EU from the United States' future regulations.³⁷

The Wassenaar Arrangement and beyond

A third path that can be pursued is pushing for an improved export control regime through an already existing intergovernmental forum: the Wassenaar Arrangement. This agreement is not only signed by most large economies, such as the United States, India, Japan and Russia, but it also has the sole objective of promoting a common approach to international standards and harmonised control lists on dual-use goods and technologies.

In recent years, emerging technologies such as 3D printing have been discussed and subsequently added to the control list of the Wassenaar framework. More needs to be done, however, to expand the responsibilities of the Wassenaar Arrangement and incorporate more items and technologies that are not currently listed for export control. This responds to the challenge to keep pace with the high speed of innovation when identifying emerging technologies of concern – both new technologies and new applications of old technologies. It could also be useful to harmonise standards in the US and the Netherlands/EU, and to discuss whether and how to take a stronger stance against China if necessary. In fact, Washington will likely seek to bring new items and issues in through Wassenaar, thus allowing all members to discuss export control

36 European Commission, [Proposal: Setting Up a Union Regime for the Control of Exports, Transfer, Brokering, Technical Assistance and Transit of Dual-Use Items](#), 28 September 2016.

37 Authors' interview with officials at the Directorate-General for Trade in Brussels, April 2019.

determinations – including decisions to list, revise or remove a control – with the US, aiming for greater alignment of policies where possible and allowing for pushback when perceived necessary.

The Netherlands can advocate for this debate directly within the Wassenaar Arrangement meetings, but can also try to push for talks between the European Commission and the US government in order to promote a better-configured version of ECRA together. This way, the EU can gain the United States' trust – by showing that it agrees with many US concerns with regard to China, in particular. The US and the EU have a strong position within the Wassenaar Arrangement meetings to introduce similar future export control regulations on the other states present as well. The broad scope of rolling out the ECRA policy could be a useful mechanism to align many countries at once and strengthen the multilateral export regime. The downside of this track is the slow pace and lack of consensus in identifying which actors present a proliferation threat and which items have omni-use potential. Moreover, the divergent stances within the Wassenaar Arrangement towards the US and China complicate this avenue even more.

Trusted communities

Lastly, the Netherlands can opt to establish new initiatives to exchange information and best practices among key stakeholders: so-called trusted communities. These can be defined as partnerships linking a range of stakeholders – including government officials, businesses and researchers – in one country or across like-minded countries. When crafting a new multilateral regime governing the export control of emerging technologies, such collaborative forums of organisations will be valuable for sharing lessons learned, preferences and sensitive information internationally.

The Dutch government could explore which are the key stakeholders domestically, as well as in like-minded countries and organisations, in the domain of the export control of emerging technologies and facilitate the creation of stronger networks through these multidimensional forums. Through trusted communities, industry and academia can provide input for suitable adjustments to the export control regime without forcefully tearing up global value-chains, and can cooperatively balance innovation, economic benefits and security. At the same time, the Dutch government can share with these stakeholders new and evolving concerns with regard to specific end-users or usage. This can help raise awareness of the power balances and diverging norms that inform export control policy, especially with high-tech start-ups and small and medium-sized enterprises that may not be aware of the potential (mis)use by certain players of their technologies.

Within the Netherlands, the first signs of trusted communities are already appearing. In February 2019, the Dutch government supported the opening of the Microsoft Quantum Lab for emerging (quantum) technology at TU Delft, known as QuTech: a collaboration between Microsoft and the advanced research centre for Quantum Computing and Quantum Internet.³⁸ Establishing trusted communities serves as a vital preliminary step towards developing common standards and frameworks for sector-specific export control that take into account the voices of different actor types, and should be supported and initiated by the Dutch government.

In this respect, Japan stands out as a country that shares many of the Netherlands' concerns pertaining to the current Sino-American trade war and Chinese strategic behaviour, as well as the need to uphold the multilateral rules-based order. Moreover, the high-tech industries in Japan, the US and the Netherlands share many similarities. This makes Japanese government actors, companies and experts natural partners with shared objectives in multilateral discussions, even if Dutch and Japanese companies are economic competitors at the same time. Despite fierce competition between Dutch company ASML and Japan's Nikon in the past, the decision to settle ongoing litigation between them in January 2019³⁹ signals a desire to move forward amicably. It also shows that differences and competition can be set aside when cooperation is the preferable way forward with regard to a new trusted community. Trusted communities are also a valuable tool to engage the US government or US businesses that have the same objectives.

Clearly, the success of a trusted community requires substantial and long-term effort. After all, a trusted community depends on a high level of trust between all the actors, as exploiting dependencies in strategic value-chains is becoming more frequent. A downside to this path is thereby the significant time and effort involved, especially where communities need to be built from scratch. Separately, care should be taken to avoid a patchwork of parallel trusted communities that complicates business relations or disadvantages countries or companies 'outside' one's own trusted community.

38 QuTech, [About Us](#).

39 Nikon, ['Nikon, ASML and Carl Zeiss Sign Agreement to Settle All Litigation'](#), 23 January 2019.

STRENGTHS

S

- ECRA is a push for needed policy reform in the US/internationally to regulate emerging technologies and address a growing norms gap. If the Netherlands and US can agree on new regulation, this can incentivise others also to adopt those measures.
- Strong stance on reciprocity is beneficial in bilateral relations with China by setting ground rules and clarity. Most beneficial when more countries take same stance.
- If ECRA can be a push for bilateral US–NL business cooperation and policy alignment, Dutch companies affected by ECRA benefit, as most have headquarters in the US and branches in NL (Schiphol/Brainport Eindhoven area).

WEAKNESSES

W

- ECRA's size and impact may be (too) broad in scope. Dutch government will lack the capacity needed to control the listed products.
- Divergent objectives and talks at cross purposes because of divergence in US–NL definitions and concepts: broad national security (US) vs. more narrow economic security (NL).

ECRA and US–NL cooperation

O

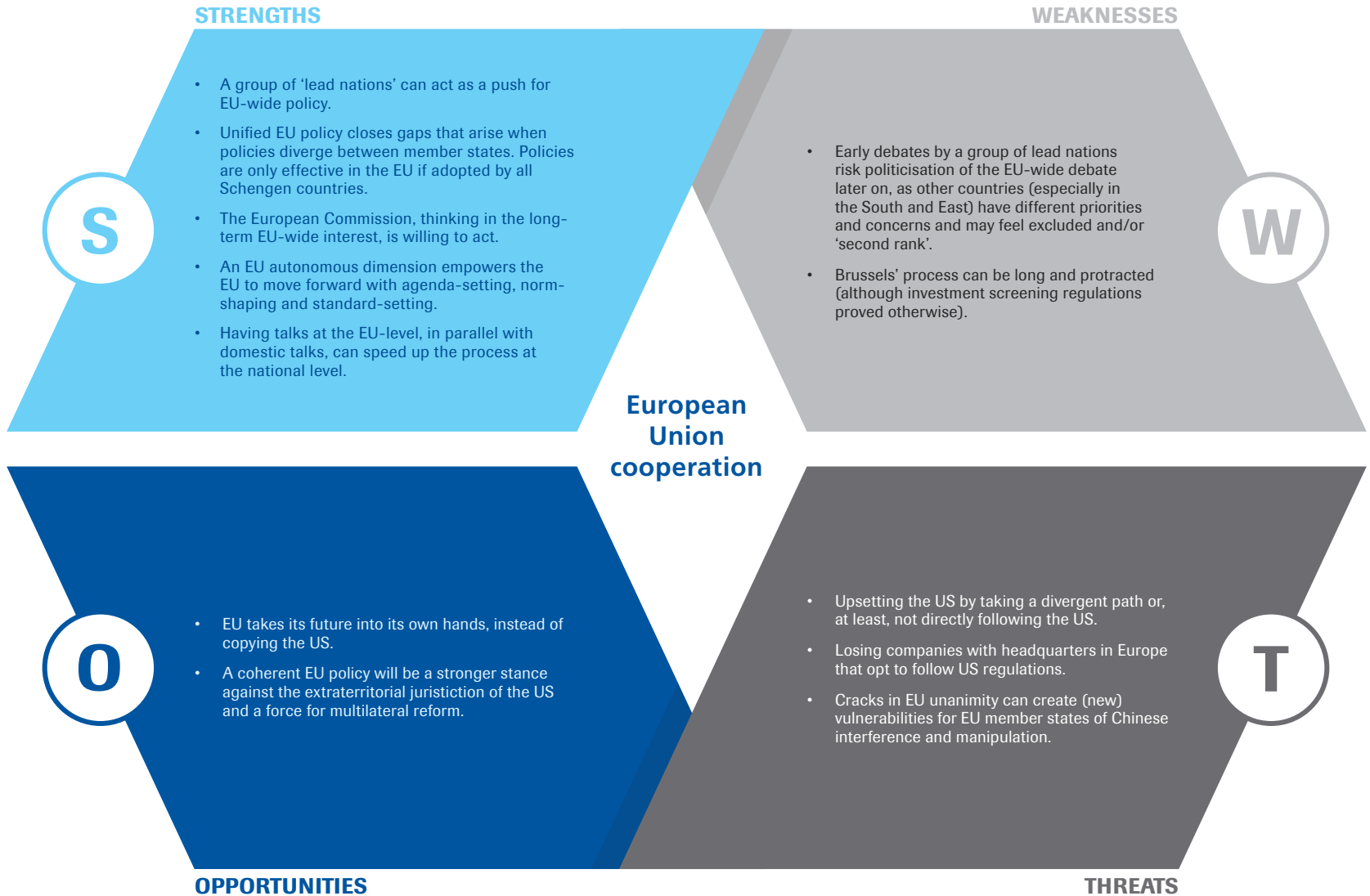
- ECRA as a push for needed revision of NL regulations.
- US–NL bilateral cooperation on new export control rules helps to build trust between US and NL governments. As such, valuable for engagement, mutual understanding and aligned cooperation to maintain innovational edge over China.
- Improved US–NL cooperation leads to increased exchange of information about cases, compliance and best practices.
- Improved alignment of US–NL policies promotes US–NL business cooperation.
- Adopting elements of ECRA improves alignment of NL export control policy with Dutch defence strategies (SNV/IVS).

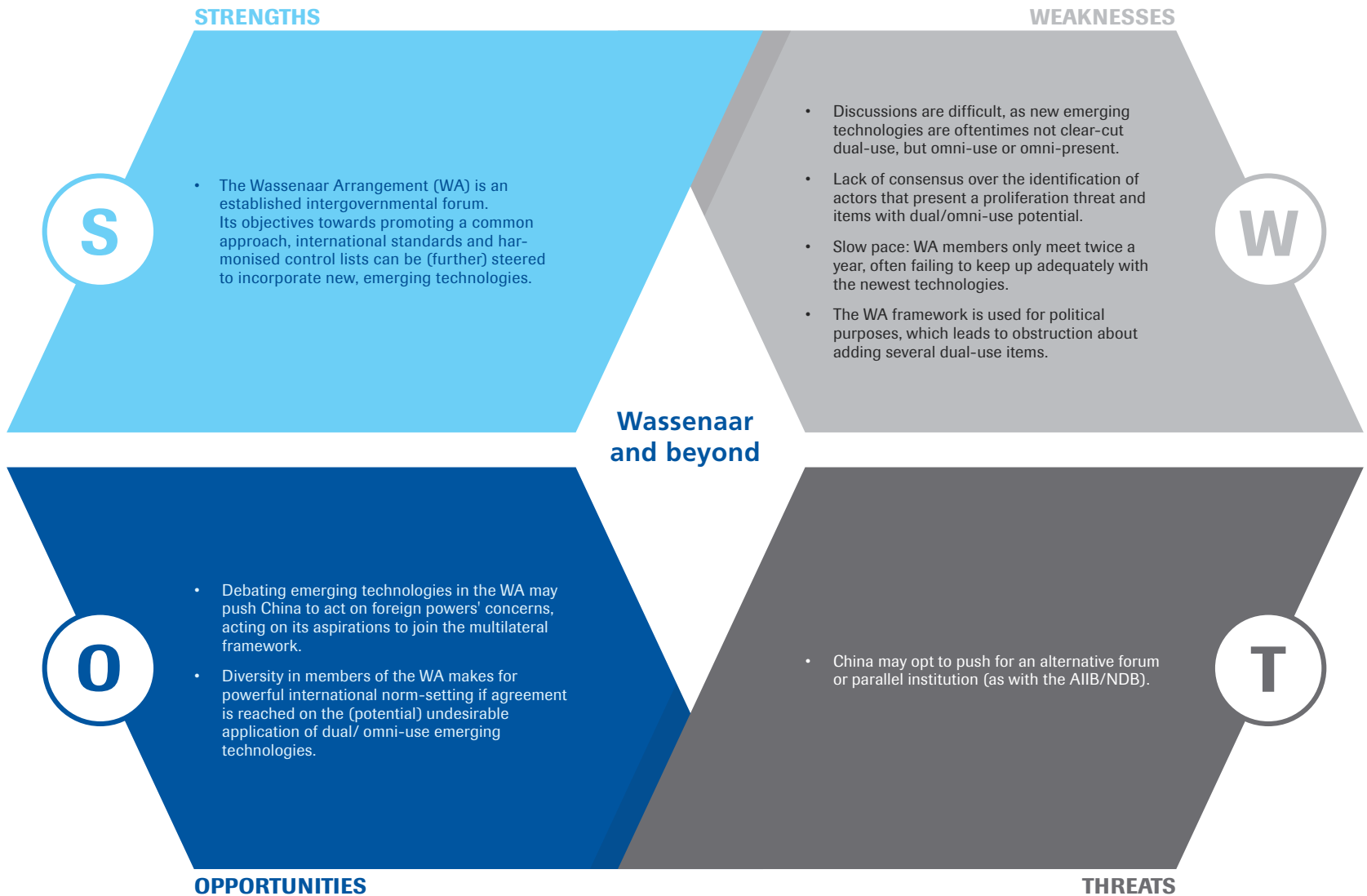
OPPORTUNITIES

- Dutch government does not recognise extra-territorial jurisdiction claimed by the US. Dutch government is likely to lose out because of its relative power in bilateral engagement with the US.
- Having different systems in the US and NL will force companies located in both countries to choose between regulations.
- US–NL cooperation on ECRA alone is no guarantee for policy success; Schengen zone/EU needs to be aligned.
- The US threatens countries that do not cooperate with US rules, using intelligence, large market and global security role as leverage.
- Strong alignment with the US may backfire in relationship with China (retaliation by Chinese Communist Party).

T

THREATS





STRENGTHS

S

- Like-minded states, businesses and knowledge institutes can be further engaged with the decision-making process.
- Trusted communities can be built around one specific group of technology, allowing for a case-by-case approach.
- The Netherlands can be a frontrunner in engaging like-minded countries, making use of its standing as a world leader in areas of multiple omni-use/emerging technologies.
- Initiatives can run in parallel to talks in the Wassenaar Arrangement.
- Japan shares the desire to move forward and could bring leverage in negotiations with the US.

WEAKNESSES

W

- Cultural barriers complicate talks with like-minded countries, such as Japan.
- Companies have vastly diverse interests: need to balance between constructive engagement and vulnerability to lobbying.
- The trusted communities have to be built from scratch, which involves significant time and effort.

Trusted communities

O

- Including one or more other like-minded country (with an advanced high-tech industry) into already ongoing talks with Japan at the global and technical levels requires a relatively small investment.
- Potential to agree on fast-track systems for export control between like-minded countries.
- Potential stepping-stone to pan-European debate.
- Discussing innovation challenges with stakeholders can stimulate R&D cooperation and can contribute to upholding the Dutch business innovative lead, complementing policies that protect technology.
- Inclusion of businesses and academia in the making of new policies contributes to self-constraint, and greater sharing of responsibilities between government and stakeholders.

OPPORTUNITIES

T

- Japan, as the most like-minded country, is also one of the biggest competitors for Dutch businesses in emerging technologies.
- China could seek to exploit the few divergences that do exist, e.g. competition between Dutch and Japanese companies.
- Countries that are excluded from the like-minded group may feel left behind. This risks greater difficulties in EU-wide debate later and cosyng up to China as a response.
- Trusted communities as exclusive networks could undermine multilateral export control regimes like the WA.

THREATS

How to move forward from here?

In recent years, geopolitical trade tensions have increased immensely and challenges to the open, transparent and rules-based system of international trade have grown. The United States' push to develop a new export control regime, as portrayed by ECRA, has only been a small, but significant, part of this larger shift underway in the geopolitics of the 21st century. While historically, the US also unilaterally pushed for an export control regime for dual-use items, the world was now taken by surprise, especially by the scope of the proposal. Moreover, the currently diverging stances of the US and the EU on various geopolitical issues, including approaches to dealing with China, increased Chinese economic influence in EU member states and the ongoing Sino-American rivalry complicate direct alignment with the US even more.

The time has therefore come for action, particularly at the EU level. In recent years, steps that were unimaginable ten years ago have now been taken in the field of FDI screening, to halt investment from non-EU countries that may affect security or public order. Action is now also needed to address new concerns on the other side of the coin: export control. As the trade–tech stand-off between the United States and China intensifies, this new form of conflict necessitates an update of regulations that prohibit the unlicensed export of certain new technologies to specific end users.

First, the Netherlands needs to determine its position regarding export control regulations for emerging technologies domestically. Interdepartmental cooperation is needed and must be strengthened to address and discuss the current convergence of Dutch national and economic security. That being said, the global interconnectedness of the technological fields in question requires that this cooperation takes place internationally as well, with like-minded partners. Seemingly caught between a rock and a hard place, the Netherlands ought to dedicate particular attention to updating the EU-wide export control regime and to equipping the EU with capacity of its own. This will require all Schengen-zone countries to be involved in implementing similar regulations in order to make the regime effective.

An autonomous European export control regime not only increases leverage towards the US, but could also be a stepping-stone towards making the EU and its member states more influential actors in existing multilateral forums, such as the Wassenaar Arrangement. Specifics of the EU export control regime could be initiated by the Netherlands, Belgium and Germany, with the caveat that Southern and Eastern European EU member states should be involved as soon as possible to prevent

them from interpreting it as an initiative of the economically advanced EU countries. It is therefore of paramount importance to know upfront how the individual EU member states interpret ECRA and a possible EU export control regime for emerging technologies.

The SWOT analyses also suggest that there is a substantial benefit from engaging with like-minded countries, and preferably also businesses and knowledge institutes, outside the EU. A natural move would be to strengthen and broaden the discussion about export control for emerging technologies into the Wassenaar Arrangement meetings. However, many discussions within the Wassenaar Arrangement are highly politicised, and meeting only two times a year results in a packed agenda of possible dual-use technologies. This leaves little room to include even more possible omni-use technologies into this agenda.

The Netherlands should therefore consider reaching out to businesses and knowledge institutes at home and in like-minded states through trusted communities. Such networks have the ability to bring together key actors to provide input for developing an export control regime that is based on mutual trust and respect, wherein special arrangements and waivers could apply to the members of such a group. Trusted communities do not exclude Chinese companies or knowledge institutes upfront, which makes them a less aggressive international forum for cooperation than the Wassenaar Arrangement, for example, as the Chinese government is not involved in these talks. Moreover, trusted communities leave room for cooperation with specific Chinese companies' emerging technologies, thereby preventing exclusion of a particular country or company in the global value-chain.

In conclusion, as the US–China trade war evolves in a state of permanent conflict at the nexus of trade, technology and data, the Netherlands and the EU need to embark on offensive and defensive policies. For the Netherlands, it is important to decide what is possible concerning scope and human capacity. Most of all, the Netherlands should push for EU talks on export control, as it is only possible to establish an effective export control system if all of the Schengen countries adopt the same measures. Moreover, the EU needs capacity to act in order to prove that it is a player in this field. As a trusted EU member state with a strong high-tech sector and an interest in EU-level action, the Netherlands is well placed to take a leading role, pushing for much-needed EU action. These are the necessary first steps if the Netherlands and EU want to engage with the US as equals and, eventually, establish a new export control regime for emerging technologies – ideally through the group of countries in the Wassenaar Arrangement and facilitated by newly established trusted communities.