The Hague Centre
for Strategic Studies

Taming Techno-Nationalism
A Policy Agenda

Hugo van Manen, Tobias Gehrke, Jack Thompson, Tim Sweijs

September 2021

The Hague Centre
for Strategic Studies

Taming Techno-Nationalism
A Policy Agenda

Authors:
Hugo van Manen, Tobias Gehrke, Jack Thompson,
Tim Sweijs

Contributors:
Rob de Wijk, Benedetta Girardi, Sneha Mahapatra

ISBN/EAN: 9789492102812
September 2021

The research for and production of this report has been conducted within the PROGRESS research framework agreement. Responsibility for the contents and for the opinions expressed, rests solely with the authors and does not constitute, nor should it be construed as, an endorsement by the Netherlands Ministries of Foreign Affairs and Defense.

Contents

Key Takeaways

In recent years, the Netherlands and other European countries have been confronted with attempts by China and the United States (US) to force or prevent the transfer of sensitive technologies. Sensitive technologies are both transformative in nature and cost and time-intensive to create. Techno-nationalist practices thus have a significant negative impact on current and future Dutch and European economic prosperity and military capacity. It is likely that competition over access to sensitive technologies will cement itself as part of a new "normal" for the foreseeable future. It is therefore important for the Netherlands to keep close track of these dynamics and to implement policies that mitigate their impact.

This report outlines a policy agenda for countering techno-nationalism, building upon existing policies options outlined by the Dutch Ministry of Finance (MinFin), the Ministry of Economic Affairs and Climate (EZK), the Ministry of Foreign Affairs (BZ), and the Ministry of Defense (MoD). These recommendations can be summarized as follows:

- **Strengthen critical infrastructure protections.** Protecting sensitive technologies from foreign takeovers by enforcing the same regulatory framework and logic that applies to companies involved in maintaining critical infrastructure to companies working on sensitive technologies. The Netherlands should take concrete steps towards empowering the Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) and EZK to screen and block harmful forms of foreign direct investment (FDI). It should expand its existing definition of what constitutes a sensitive technology and what does not to feature software-based technologies more explicitly.

- **Make strategic use of public spending.** The Netherlands can make more strategic use of its public spending. Concretely, it should expand the cybersecurity and counterespionage-related requirements which are already included within military procurement processes to apply to companies working on sensitive technologies. It should also up its investments into research and development (R&D) beyond the current ±0.8 percent of gross domestic product (GDP) to meet, at the very least, the European Defence Agency's (EDA's) norm of two percent of military expenditures R&D. It should also preclude repeat techno-nationalists from participating in its public procurement processes where legally viable. Funding should be made available, whether through subsidies or otherwise, to strategically relevant private sector initiatives – such as Intel's bid to construct a foundry in the Benelux – with the goal of creating ecosystem effects.

- **Incentivize increased private spending.** Public spending is no substitute for private investments. Venture capitalist funding has picked up in Europe in recent years but still lags far behind American and Chinese counterparts. Importantly, despite these firms' increased expenditure in recent years, many are investing significant shares of their capital in international (non-domestic, non-regional) ventures. The Netherlands should engage in discussions with founders and venture capitalists to identify policy initiatives at the domestic and European Union-level (EU-level) that might contribute to increasing private sector investments into the trading bloc's startups.

- **Develop a more comprehensive deterrence posture.** The Netherlands should supplement its efforts to build up an infrastructure capable of mitigating techno-nationalism when it is practiced with initiatives to build a strong norm against such practices. One way of doing this is to seize upon the North Atlantic Treaty Organization's (NATO's) Article 2 – which outlines the need for "economic cooperation" on national security matters – to, amongst others, cooperate on (dis)allowing foreign vendors to supply sensitive technologies to critical infrastructure providers, and to formulate clear escalation ladders for responding to instances of state-sponsored economic espionage or sabotage.

- **Recognize the relevance of EU-level cooperation.** The Netherlands' competences to address techno-nationalist practices are limited, with the EU having exclusive competences in the key policy areas of the customs union, competition rules, monetary policy, and trade. Because of this, cooperation at the EU level is vital. Additionally, the Netherlands' robust R&D capabilities notwithstanding, the country will never achieve full self-sufficiency as far as securing access to sensitive technologies is concerned. It needs to be able to access other European Member States' innovations and it has a vested interest in those innovations taking place. It should cooperate with and contribute to European regulators' activities and coordinate its investments into sensitive technologies through agencies such as EDA and NATO to prevent redundancies.

»Techno-nationalist practices have a significant negative impact on current and future Dutch and European economic prosperity and military capacity.«

Executive Summary

States treat access to sensitive technologies as a zero-sum game and pursue policies to expand national control over and international influence through sensitive technologies.

In recent years, the Netherlands and other European countries have been confronted with attempts by the United States (US) and China to force or prevent the transfer of sensitive technologies. The geopoliticization of such technologies is emblematic of a far wider and more worrying trend at the global level. Awareness of the economic, military, and strategic relevance of access to and control over the distribution of modern technologies is growing. Recognition that a nation's technological innovation and capabilities are directly linked to its national security, economic prosperity, and social stability is driving a new wave of "techno-nationalism" or "innovation mercantilism". States treat access to sensitive technologies as a zero-sum game and pursue policies to expand national control over and international influence through sensitive technologies. These technologies are extremely costly and time and human capital-intensive to develop. The technological know-how necessary to pioneer breakthroughs and to engineer and realize real-world applications takes years to cultivate.

States leverage a variety of tools to expand their access and control over sensitive technologies and to undermine the competitiveness of allies and adversaries alike. Policy instruments include, but are not limited to, traditional mercantilist practices such as import and export controls, the subsidization of national champions, espionage, laws designed to force foreign companies to transfer core technologies, initiatives to revise international technical standards, and even global infrastructure development strategies.

The practice has, in Europe, contributed to an intensification of discussions surrounding the need for a European strategic autonomy. European strategic autonomy has grown to encapsulate not only the need for European autonomy in military operations, but, more generally, the notion that the EU and its Member States ought to be able to make decisions without being constrained by their relationships with external actors. European Union (EU) officials have made repeated reference to the importance of safeguarding the bloc's "digital" and "technological" sovereignty, highlighting their recognition of science, technology, trade, data, and investments as emerging sources of influence in international politics. The sentiment has resulted in the introduction of a bevy of new pieces of legislation, with the Digital Services Act (DSA), the Digital Markets Act (DMA), the Cybersecurity Strategy, and the General Data Protection Regulation (GDPR) all being geared towards protecting EU consumers, eroding the monopolistic market power of US and Chinese tech giants, and incentivizing the emergence and growth of EU-based competitors.

In dealing with techno-nationalism, European states will need to implement new policies and oversight processes to safeguard security and promote prosperity. They will need to reduce the negative impact of techno-nationalist policies by putting safeguards in place on the one hand, while working to bolster the competitiveness of their innovative ecosystems on the other. This study identifies and evaluates a portfolio of policy measures that can, within the confines of existing EU initiatives and regulations and in-keeping with international law, be implemented by the Netherlands and other EU Member States to achieve these ends.

The Impact and Timing of Sensitive Technologies

Technologies such as artificial intelligence (AI), quantum computing, and modern gene editing tools combine a transformative impact on national industries and warfighting capabilities with extremely high barriers to entry, allowing for the creation of long-term dependencies. Table 1 depicts the estimated impact on international security and economic prosperity, and the timing of that impact, of the twelve sensitive technology areas examined. The list of technologies was compiled based on an extensive meta-review of scientific and policy-oriented literature and in-depth interviews with experts on sensitive technology areas.

Table 1 - Sensitive technologies' impact on international security and prosperity

Technology	Military vs Economic	Estimated Impact[1]	Estimated Timing[2]
AI	Military	Revolutionary	Long Term
	Economic	Revolutionary	Now
Big Data	Military	Revolutionary	Soon
	Economic	Modest	Now
Bio and Human Enhancement Technologies (BHET)	Military	Modest to Significant	Soon
	Economic	Significant	Now
Chemical Technologies	Military	NA	NA
	Economic	Modest to significant	Now
Photonics	Military	Significant	Now to Soon
	Economic	Significant	Now
Quantum Technologies	Military	Revolutionary	Soon to Long Term
	Economic	Significant to Revolutionary	Soon
Robotics and Autonomous Systems (RAS)	Military	Significant to Revolutionary	Soon
	Economic	Significant to Revolutionary	Now
Semi-conductor Lithography	Military	Significant	Now
	Economic	Significant to Revolutionary	Now
Sensor Technologies	Military	Modest	Long Term
	Economic	Modest	Now
Space Technologies	Military	Modest to Significant	Soon to Long Term
	Economic	Significant to Revolutionary	Now to Long Term
Weapon Technologies	Military	Modest (directed energy weapon – DEW) to Significant (Hypersonics)	Soon
	Economic	NA	NA
3D printing and advanced materials	Military	Modest to Significant	Soon to Long Term
	Economic	Significant to Revolutionary	Now

1 **Modest** indicates that the technology will lead to a limited increase of the performance of military equipment or systems or increase economic growth only by a few percent. **Significant** suggests a much larger increase in performance or growth, at a minimum in the double digits. **Revolutionary** signifies that the technology will potentially render current military equipment/systems obsolete or create entirely new economic categories or processes. See Box 3.

2 **Now** indicates that the technology currently has a substantial impact. **Soon** suggests a substantial impact by 2030. **Long-term** predicts a substantial impact after 2030. See Box 3.

The Netherlands has punched far above its weight as far as building up an innovation ecosystem is concerned. A survey of 26 experts found that the Netherlands has robust research capabilities in at least five of the twelve sensitive technology areas (see Figure 1).

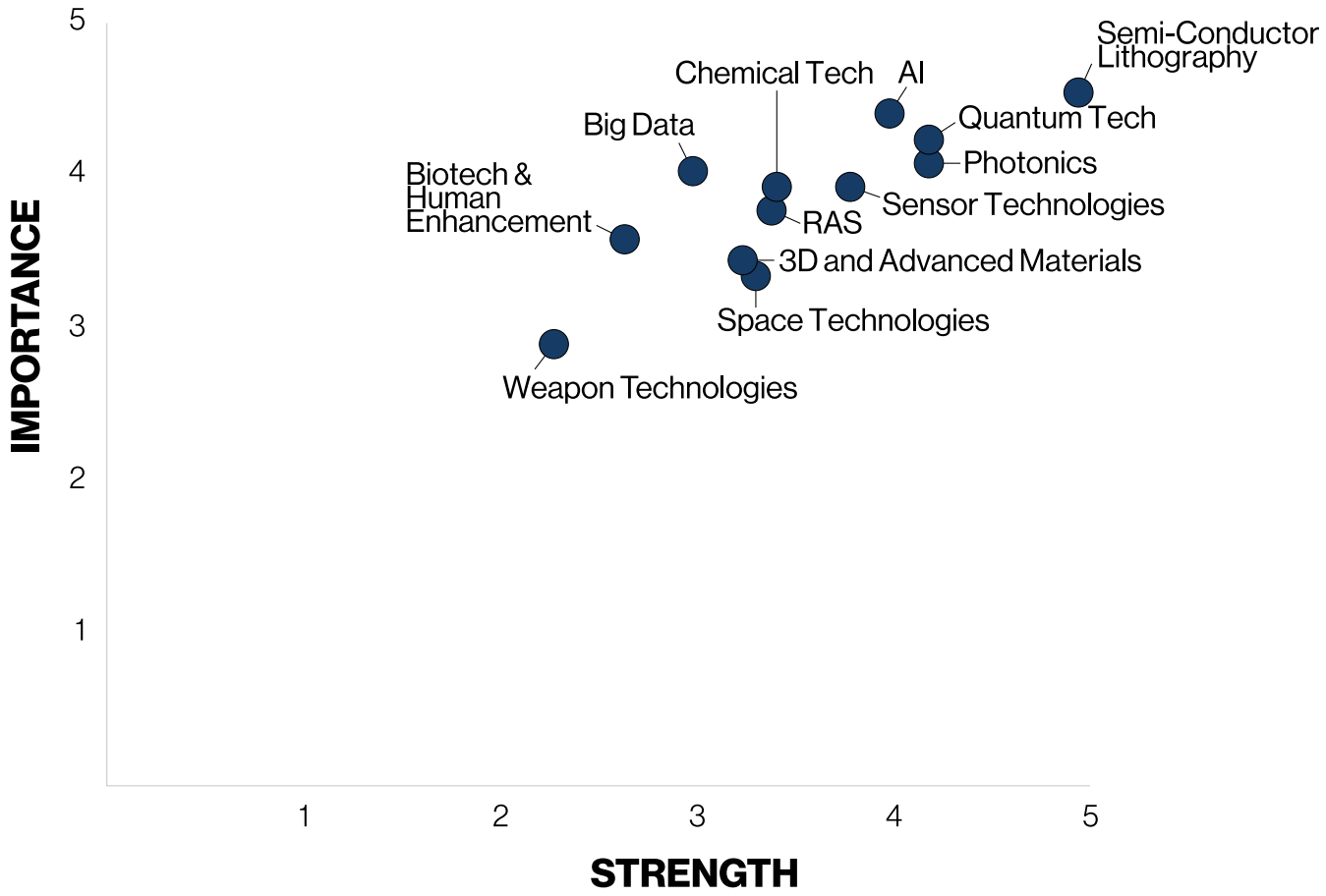

Figure 1 - Experts' appraisal of the strength and importance in sensitive technology areas for the Netherlands

Strategies of Techno-Nationalism

Recent years have seen an uptick in state engagement in techno-nationalism. Spurred on by the transformative nature of today's sensitive technologies and a renewed focus on great power competition, states have increasingly embraced the notion that their national security is linked to their technological innovation and capabilities. The US, Russia, China, and India, amongst others, have all formulated and pursued policies aimed at expanding national control over sensitive technologies in recent years (see Table 2).

Table 2 - Strategies of techno-nationalism: an overview

Measures that transfer technology and/or technological know-how	Market-based approaches	**Foreign direct investment (FDI) & acquisitions**. FDI & acquisitions offer a clear path to acquiring both technology and technological know-how.
		Patent licensing. Patent licensing is a key part of many companies' business models. Typically implemented as business to business (B2B) arrangements, the practice allows a company that has developed a technology to charge 3rd parties to use said technology in their products.
		Technology purchases. Similar to patent licensing, the acquisition of high-tech goods and services lends itself to the manifestation of negative outcomes because many of the actors which engage in techno-nationalism behave in uncompetitive ways.
	Legislative approaches	**"Lose the market" laws**. Localization barriers to trade (LBTs, or "lose the market" laws) link market access to a series of preconditions, such as intellectual property (IP) sharing or opting into technology transfers.
		"Violate the law" laws. "Violate the law" laws are laws that are designed to allow for the easy prosecution and sanctioning of companies that refuse to cooperate with efforts at facilitating technology transfers once they are already active within a country's domestic market.
		"No choice" dynamics. "No choice" dynamics are dynamics that make it difficult for foreign companies to protect themselves from technology theft within a country's borders.
	Forced	**Forced approaches** constitute the final approach type that can be employed to secure technology transfers. These include, but are not limited to, the use of espionage and the leveraging of diaspora.
Measures that make for an uneven playing field	Direct	**Direct support** includes, but is not limited to, financial support (in the form of investments, gifts, subsidies, etc.) and logistical and/or operational support (i.e.: the use of state intelligence agencies to provide companies with a 3rd party's technological know-how).
	Indirect	**Indirect support** generally takes the form of protectionist or mercantilist policies intended to reduce foreign companies' ability to compete domestically.
	Standard setting	**Standard setting** includes the strategic pursuit of long-term initiatives geared towards reducing 3rd countries' structural ability to compete. These include, but are not limited to, leveraging first-mover advantages to introduce beneficial (technical) standards through international standard-setting bodies and investing into initiatives such as the Belt and Road Initiative (BRI), which aid in fostering long-term dependence by facilitating the adoption of key technical standards.

Instruments for Countering Techno-Nationalism

Time and options still exist for putting policies and infrastructures in place to help prevent the unwanted theft of Dutch and European technologies and the erosion of Dutch and European innovation ecosystem's ability to compete internationally.

A not-insignificant share of the initiatives which might contribute to achieving these policy goals will need to be kickstarted at the EU level. The EU, due in no small part to Member States' shared interest in maintaining a level playing field, has exclusive competences over the *customs union*, *competition rules*, *monetary policy*, and *trade*. This means that the EU alone is able pass laws which impact these areas, with Member States' roles being relegated largely to enforcement and implementation. The EU has shared competences – meaning that Member States can introduce laws independently provided they do not clash with existing EU legislation and the EU has not announced its intention to introduce laws – in many policy areas of potential relevance to countering techno-nationalism, including the *single market*, *employment and social affairs*, *economic, social and territorial cohesion*, *consumer protections*, and *research and space*.

A not-insignificant share of the initiatives which might contribute to mitigating the impact of techno-nationalism will need to be kickstarted at the EU level.

Within this context, it falls upon the Netherlands to take a proactive approach to securing its innovation ecosystem from techno-nationalism. First, it can contribute to the inception of critical EU-level regulations. It can also be far-reaching in how it interprets, implements, and enforces key pieces of EU legislation – choosing to take an approach that heeds these initiatives in spirit and intention rather than in text only. Second, it can introduce national legislation provided that, in doing so, it is mindful not to infringe on existing EU legislation. EU and Member State policy options can generally be understood as being either regulatory, procurement-based, fiscal and/or monetary, or diplomatic in their scope:

- Regulatory instruments include options such as the expansion of critical infrastructure protections to sensitive technologies, something which would allow regulators to block many unwanted foreign acquisitions and FDI proactively.
- Procurement-based instruments are geared towards reducing bad-actors' access to Dutch and/or EU procurement funding on the one hand, and towards providing legitimate forms of funding and towards incentivizing the strengthening of private-sector security protocols on the other.
- Fiscal tools will see the Netherlands or the EU step up funding for sensitive technologies. This form of funding differs from the funding outlined under the previous bullet (pertaining to procurement processes) in that they are not awarded on a competitive basis. As a result, this form of funding verges on protectionism and can be associated with various pitfalls.
- Diplomatic options would consist of the Netherlands and the EU opening dialogues with the power houses such as the US and China, and/or work towards for World Trade Organization (WTO) reform.

Using this taxonomy, 27 European experts identified and ranked the *leveraging of procurement processes to incentivize improvements in private-sector cybersecurity and counterintelligence capabilities* and the *adapting and updating of existing critical infrastructure protections to cover sensitive technologies* as high impact, high feasibility policy initiatives. Other options, including the use of *subsidies and other fiscal policies to bolster local industry's ability to compete* and the introduction of targeted *import tariffs* also emerged as holding potential (Figure 2).

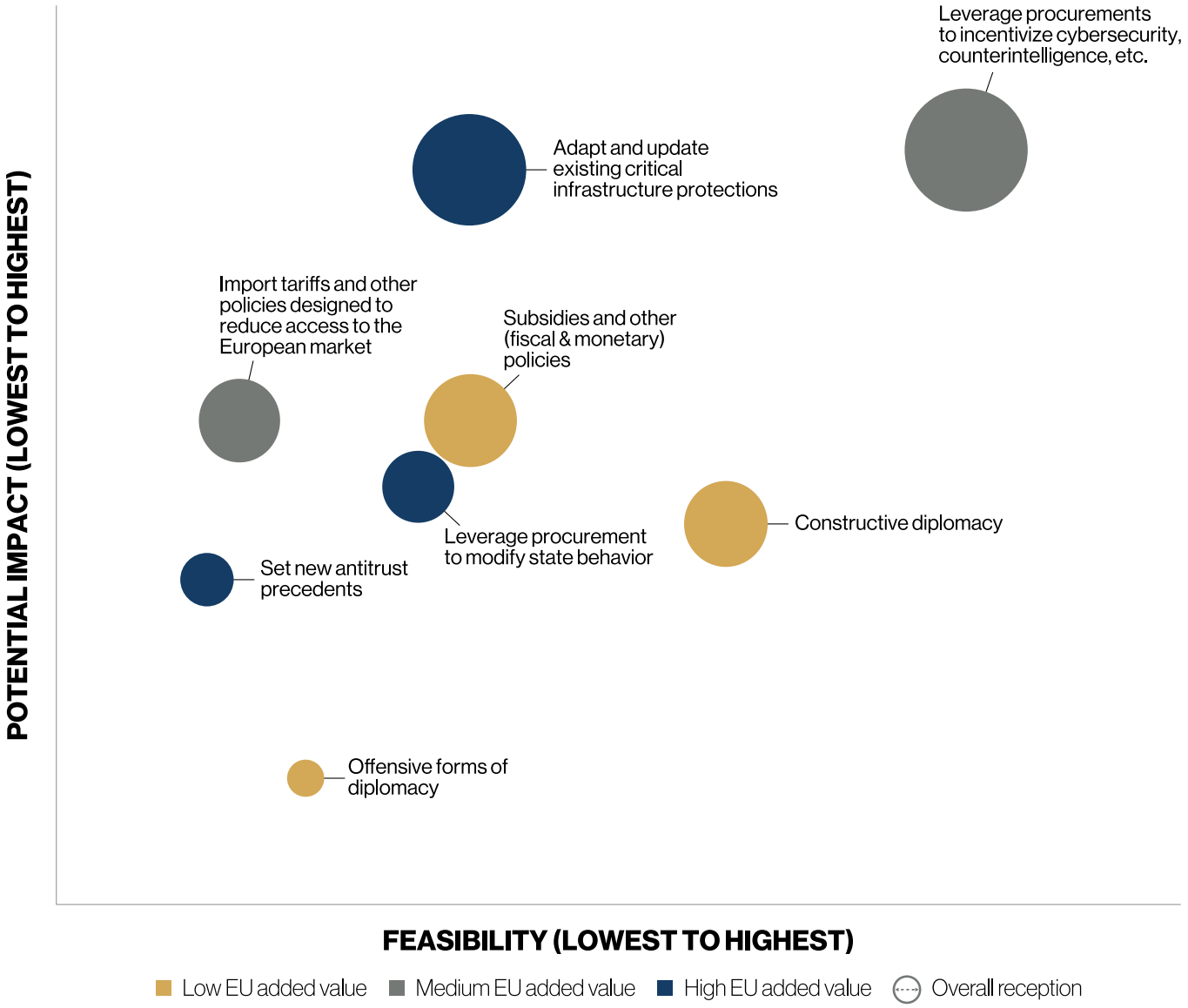

Figure 2 - Survey results: feasibility and potential impact of policy measures

A Policy Agenda for Countering Techno-Nationalism: **Recommendations**

The policy agenda detailed below outlines steps the Netherlands can take to interpret, implement, and enforce key pieces of existing EU legislation and pieces of national legislation it can introduce which do not clash with its commitments to the trading bloc. Crucially, it also – in outlining an extensive list of recommendations pertaining to EU-level initiatives – provides a clear roadmap of initiatives falling within the EU's exclusive competences which the Netherlands should work towards achieving at the EU level.

These policy recommendations contribute to putting safeguards in place to protect Dutch and European innovation ecosystems on the one hand, and to bolstering the competitiveness of the trading bloc's innovative industries on the other. They echo many of the policy

options that the Dutch Ministry of Finance (MinFin) outlines in its Brede Maatschappelijke Overweging (see Box 8 on page 78). A policy agenda for countering techno-nationalism is recommended to include the following measures:

Put Safeguards in Place

Apply critical infrastructure protections to sensitive technologies
by taking the following steps:

1. Adapt and expand the existing list of sensitive technologies and formulate a clear set of guidelines for what constitutes a sensitive technology and what does not.
2. Update the Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV's) and the Ministry of Economic Affairs and Climate's (EZK's) mandates to mirror the US Committee on Foreign Investment's (CFIUS') Final Regulations Revising Declaration Requirement for Certain Critical Technology Transactions (CCTT).
3. Formulate clear "safeguard" guidelines for the NCTV and EZK to enforce, in line with what is currently being discussed within the context of the adoption of the Bill on *Security Screening of Investments, Mergers and Acquisitions*.

Time and options still exist for putting policies and infrastructures in place to help prevent the unwanted theft of Dutch and European technologies.

Leverage procurement to improve cybersecurity and counterintelligence
by taking the following steps:

4. Identify requirements for, formulate, and develop a certification process to enforce a clear set of cybersecurity and counterespionage standards for private sector use.
5. Identify tenders and procurement processes that make funding available for work relating to sensitive technologies or which commonly attract bids from actors that conduct research into sensitive technologies.
6. Revise identified procurement processes to include adherence to cybersecurity and counterespionage standards as an exclusion criterion.

Leverage fairness principles to erect legitimate barriers to trade and to procurement
by taking the following steps:

7. Exclude Chinese companies from accessing Dutch and/or EU procurement funding until it signs onto and complies with the WTO's Agreement on Government Procurement (GPA).
8. Allow US companies to participate in Dutch and/or EU procurement funding on a case-by-case basis.
9. Develop a framework for identifying states' engagement in directly or indirectly-oriented forms of techno-nationalism. In instances of non-reciprocal trading relationships, limit countries' access to Dutch and EU procurement funding.

10. **Activate the North Atlantic Treaty Organization (NATO) to safeguard economic security**. The alliance's founding treaty outlines the need for "economic cooperation" on national security matters in its second article (Article 2). This leaves room for cooperation on (dis)allowing foreign vendors to supply sensitive technologies to critical infrastructure providers, and for formulating clear escalation ladders for responding to instances of state-sponsored economic espionage or sabotage. The introduction of such an escalation ladder would serve the purpose of deterring 3rd countries from perpetrating these activities.

It falls upon the Netherlands to take a proactive approach to securing its innovation ecosystem from techno-nationalism.

Cooperate with and strive to further the following EU-level initiatives:

11. *Advance WTO reform*. The EU should co-develop a strategy with its close partners for introducing issues relating to subsidies and state-owned enterprises (SOEs) to the WTO.
12. *Ratify the EU-China Comprehensive Agreement on Investment (CAI) and monitor China's implementation*. The EU should be ready to ratify CAI once Chinese sanctions are lifted.
13. *Adopt the foreign subsidy regulation*. The foreign subsidy regulation should be adopted. The regulation would fill an important gap in the EU's competition regime and sharpen the EU's ability to ensure fair competition in the single market which would support EU tech industry competitiveness.
14. *Aim for an ambitious EU-China Joint Roadmap for Future Science, Technology and Innovation Cooperation (STI) agreement*. The agreement should allow the EU to set clear limits on STI cooperation, while in turn deepening engagement in those sectors where common interests exist.
15. *Develop deterrence to techno-nationalist practices*. The EU must develop concrete deterrence instruments and develop an "escalation ladder" of EU action. The effectiveness of these efforts might lend themselves well to coordination within NATO.
16. *Streamline technology across EU foreign policy*. The EU should award more serious consideration to streamlining technology in foreign policies, for example as part of a revamped Global Connectivity Strategy.
17. *Refine metrics for sensitive goods and technologies*. The EU should provide guidance as to what actions are available, necessary, and proportionate for goods featured in list of "strategic dependencies".
18. *Continue EU efforts for harmonized investment screening standards*. The EU should step up efforts to harmonize investment screening standards across Member States. The current EU screening framework represents only the lowest common denominator, wielding little to no central power.
19. *Expand screening to include "economic security"*. A reform of the EU screening regulation should consider metrics measuring the competitive effect of foreign investment on strategic technology industries.
20. *Develop financial counters*. The EU needs a common financial instrument which can acquire a controlling stake in sensitive EU assets should no private, non-risky buyers be available to circumvent a foreign takeover.
21. *Continue defensive efforts for 5G infrastructure*. The EU should play a more active role in coordinating the rollout of 5G infrastructures across Member States. Member State autonomy in implementing the 5G Toolbox guidelines has resulted in substantially different approaches on limiting Huawei's role in national networks.
22. *International coordination at the Trade and Technology Council (TTC)*. The EU and US (and other close partners) must develop close coordination on issues related to economic security and technology.
23. *A multilateral agenda*. The EU should work to develop a multilateral agenda around technology and economic security. Stressing sovereignty need not preclude cooperation with other governments – especially as far as establishing new ground rules is concerned.

Bolster Competitiveness

24. **Facilitate growth in venture capital (VC) funding** by taking other actions to incentivize more robust VC for Dutch and European startups.
25. **Further step up and optimize procurement spending and other public investments** by increasing funding for Dutch and European startups and research and development (R&D) hubs, applying instruments such as the Innovation Future Fund in as focused a way as possible, and increasing the predictability of long-term funding. The goal should be to create ecosystem effects.
26. **Step-up military R&D; strive to co-develop technologies through military procurement** by increasing government investments into military R&D to meet the European Defence Agency's (EDA's) two percent norm and by participating in (military) procurement processes such as Permanent Structured Cooperation (PESCO), the European Defence Industrial Development Programme (EDPIP), the Preparatory Action on Defence Research (PADR) or NATO's Defense Planning Process.

The EU, due in no small part to Member States' shared interest in maintaining a level playing field, has exclusive competences over the customs union, competition rules, monetary policy, and trade.

Cooperate with and strive to further the following EU-level initiatives:

27. *Continue development of instruments to combat unfair competition*. The EU should redouble its efforts to put instruments for combatting unfair competition in place, even if it does not foresee requiring them in the near future.
28. *Fair competition in third countries*. The EU needs to cooperate with like-minded partners through initiatives such as the Blue Dot Network, Build Back Better World, and the EU's own Connectivity Strategy to ensure open standards for infrastructure allow for fair competition.
29. *Own financial resources*. The EU should follow-up the Recovery and Resilience Facility (RFF) with a common finance instrument capable of supporting tech industrial projects. Without its own serious financial resources, EU tech industrial policy will remain largely dependent on Member States funds.
30. *Formulate clear lists and targets*. The EU's tech industrial policy goals require clear performance targets. While a narrower list of "sensitive assets/technologies" is slowly emerging, a clear methodology remains far executing on their development remains far from obvious.
31. *Mainstream R&D funding*. While EU R&D ranks highly across the board, more efforts need to be made to focus research on bottleneck technologies and sub-sectors in critical value chains.
32. *Enlist procurement instruments*. To be able to support its most sensitive technologies, the EU needs a strong procurement instrument – or be able to coordinate national procurement instruments – to leverage scale-up of tech start-ups.
33. *Move ahead on the European Future Fund*. Before the COVID-19 pandemic, the Commission drafted plans for a €100bn sovereign wealth fund to invest (long-term equity) in strategic industries. Such firepower is critical to allow for more private finance to crowd in.
34. *A European Tech Visa*. Streamline tech visas at the EU level with the goal of attracting and retaining tech talent.
35. *International tech industrial cooperation*. Opening the Important Projects of Common European Interest (IPCEI) for 3rd country participation is an example of an initiative that could help build resilient value chains with like-minded partners.
36. *Common R&D efforts*. The EU and international partners must identify sensitive technology challenges and devise policies which incentivize international R&D cooperation. Solving the most pressing innovation challenges cannot be done in isolation, especially in a time when innovation and technological advances rely ever more heavily on international collaboration.

Lexicon

AI	Artificial Intelligence
BHET	Bio and Human Enhancement Technologies
bn	Billion
BRI	Belt and Road Initiative
B2B	Business to Business
CAI	EU-China Comprehensive Agreement on Investment
CAP	Common Agricultural Policy
CCP	Chinese Communist Party
CCTT	Final Regulations Revising Declaration Requirement for Certain Critical Technology Transactions
CFIUS	United States Committee on Foreign Investment
CMA	Competition and Markets Authority
CSRs	Corporate Structure Requirements
DARPA	Defense Advanced Research Projects Agency
DEW	Directed Energy Weapon
DMA	Digital Markets Act
DSA	Digital Services Act
EC	European Council
EDA	European Defence Agency
EDPIP	European Defence Industrial Development Programme
EIC	European Innovation Council
EO	Earth Orbit
EOTS	Electro-Optical Targeting System
EU	European Union
EUV	Extreme Ultraviolet Lithography
EZK	The Netherlands' Ministry of Economic Affairs and Climate
FDI	Foreign Direct Investment
FTTs	Financial Transaction Taxes
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GPA	Agreement on Government Procurement
GSA	Ground-based Situational Awareness
IP	Intellectual Property
IPCEI	Important Projects of Common European Interest
ISO	International Organization for Standardization
IT	Information Technology
LBTs	Localization Barriers to Trade
LEO	Low-Earth Orbit
MFF	Multiannual Financial Framework
MinFin	The Netherlands' Ministry of Finance
mn	Million
MoD	Dutch Ministry of Defense
NATO	North Atlantic Treaty Organization
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
OECD	Organization for Economic Co-operation and Development
OODA	Observe, Orient, Decide, Act
PADR	Preparatory Action on Defence Research
PESCO	Permanent Structured Cooperation
PLA	People's Liberation Army
PNT	Positioning, Navigation, Timing
R&D	Research and Development
RAS	Robotic and Autonomous Systems
RFF	Recovery and Resilience Facility
SoC	System on a Chip
SOE	State-Owned Enterprise
SSA	Space Situational Awareness
STI	EU-China Joint Roadmap for Future Science, Technology and Innovation Cooperation
tn	Trillion
TRIPS	Agreement on Trade-Related Aspects of Intellectual Property Rights
TTC	Trade and Technology Council
UK	United Kingdom
UN	United Nations
US	United States
VC	Venture Capitalism
WTO	World Trade Organization

1. Introduction

As recognition of the economic, military, and strategic relevance of access to and control over the distribution of modern technologies has grown, so, too, has the prevalence of the sentiment that a nation's technological innovation and capabilities are directly linked to its national security, economic prosperity, and social stability.

In recent years, the Netherlands and other European countries have been confronted with attempts by the United States (US) and China to force or prevent the transfer of sensitive technologies. The Netherlands, for its part, has some first-hand experience with this. ASML, the world's largest supplier of photolithography systems critical to the production of integrated circuits, works on technologies that have been designated as vital to national security by Dutch authorities. It fell victim to (allegedly) Chinese-backed corporate espionage in 2015 and was subjected to US pressure to halt its export of technologies to China in 2020.[3]

The case is emblematic of a far wider – and more worrying – trend at the global level. As recognition of the economic, military, and strategic relevance of access to and control over the distribution of modern technologies has grown, so, too, has the prevalence of the sentiment that a nation's technological innovation and capabilities are directly linked to its national security, economic prosperity, and social stability. Interchangeably referred to as "techno-nationalism," and "innovation mercantilism," this sentiment can be clearly discerned in the national security strategies of the US, Russia, China, and India, amongst others. It is creating incentives for states to treat access to sensitive technologies as a zero-sum game and to pursue policies to expand national control over and international influence through sensitive technologies. The "geopoliticization" of sensitive technologies – even those which, on first sight, appear banal and/or consumer-focused in nature – are on clear display in debates surrounding European telecom providers' use of Huawei technologies within their 5G networks, fresh discussions regarding Johnson & Johnson's purchase of Crucell,[4] and the United Kingdom's (UK's) response to NVIDIA's proposed acquisition of ARM (see Box 1).

State infatuation with technology is nothing new. France invested significant resources to (and eventually succeeded in) stealing the Jenny Spin Wheel from the UK during the Napoleonic Era.[5] The US and the Soviet Union allocated exorbitant funds to military procurement and research and development (R&D) on the assumption that doing so was key to ensuring their continued existence. Japan embraced anti-competitive trade policies to facilitate the growth of modern-day mega-corporations such as Sony and Toyota in the 1970s, harming the prospects of many European manufacturers in the process.[6] The techno-nationalism which the world is contending with today differs from past incarnations in that, as the world has seen a return to great power competition, the resurgence of techno-nationalism has prompted states to view sensitive technologies as vectors of influence peddling and control. In this context, many sensitive technologies combine a transformative impact on national industries and warfighting capacities with extremely high barriers to entry.

3 "'ASML had juist goede banden met China,'" NOS, February 28, 2015, https://nos.nl/l/2021909.

4 Crucell was a Leiden-based company which was acquired by Johnson & Johnson (J&J) in 2010. The company, now a subsidiary of J&J, has been renamed to Janssen Vaccines. It developed the Janssen SARS-CoV-2 vaccine.

5 Gregory Clark, "The British Industrial Revolution, 1760-1860," *University of California Davis*, 2005.

6 Robert E. Kelly, "Uber and Classic Asian Mercantilism," *The Diplomat*, July 25, 2014, https://thediplomat.com/2014/07/uber-and-classic-asian-mercantilism/.

Box 1 – The UK's response to ARM's acquisition by NVIDIA

When NVIDIA announced its intention to acquire ARM Limited from SoftBank in a deal valued at $40bn in 2020, many tech investors predicted that UK regulators would block the merger. Their pessimism was partially vindicated later the same year, when Daniel Zeichner – a Cambridge MP – secured a Parliamentary debate on the merger after responding to reports that neither the Chancellor nor the HM Treasury had held talks with ARM or NVIDIA. He accused the government of being "asleep at the wheel" and of failing to protect the UK's technological sovereignty. It was further vindicated in 2021, when the UK's Digital Secretary instructed the Competition and Markets Authority (CMA) to investigate the merger on national security grounds.

This regulatory scrutiny is hardly unexpected, if only for economic reasons. NVIDIA's acquisition of ARM risks more than 3,000 British jobs, a concern which NVIDIA has sought to alleviate by announcing that it will honor SoftBank's previous commitment to keeping ARM's headquarters in Cambridge for the foreseeable future. But ARM's acquisition by NVIDIA also has significant implications for the UK's ability to exert pressure on trading partners and to compete in artificial intelligence (AI) research. Though the company does not manufacture or sell system-on-a-chips (SoCs) itself, it designs and licenses an SoC architecture that is used in both Qualcomm's Snapdragon line and in Apple's iPhones (that is to say: in virtually all the world's smartphones). It is also seeing increasing success in other market segments. Apple and Microsoft have both released laptops which forego Intel and AMD-branded chips in favor of chips using an ARM-based architecture. Due in no small part to its power efficiency and optimization for performing machine learning-centric workloads, the architecture is also coming to enjoy increased market saturation within the enterprise space.

NVIDIA's acquisition would afford the US' Committee on Foreign Investment (CFIUS) the jurisdiction to unilaterally block the export of products incorporating ARM's technologies. This would transfer the strategic leverage afforded by (dis)allowing foreign countries access to ARM's architecture from Downing Street to the White House, arguably hamstringing the UK's ability to execute on its strategic vision in the process.

Against this background, national access to and control over sensitive technologies is increasingly taking on the form of a zero-sum game. States are incentivized to leverage any and all of the tools at their disposal to expand their access and control over sensitive technologies and to undermine the competitiveness of allies and adversaries alike. Policy instruments include, but are not limited to, traditional mercantilist practices such as import and export controls, the subsidization of "national champions," espionage, laws designed to force foreign companies to transfer core technologies, initiatives to revise international technical standards, and even global infrastructure development strategies such as the Belt and Road Initiative (BRI). Doing so benefits not only the competitive ability of states in the present. Because the barriers to developing and accessing sensitive technologies are exceptionally high, it also allows for the creation of long-term dependencies.

Concerns over sensitive technologies' role in fostering long-term dependencies play directly into discussions regarding the need for European strategic autonomy, within the context of which they have been interchangeable referred to as infringing on the European Union's (EU's) "digital" and "technological" sovereignty by officials. European strategic autonomy can generally be understood as a strategy for political survival. The European Council (EC) first cited some variation of the concept in relation to the EU's defense industry in 2013,

when the Obama Administration withdrew some 7,000 combat troops from Europe.[7] The sentiment that US' commitment to guaranteeing European security was wavering has been reaffirmed by its subsequent pivot to Asia, the pressures placed upon the North Atlantic Treaty Organization (NATO) alliance under the Trump Administration, and – most recently – the Biden Administration's abrupt withdrawal from Afghanistan.[8] These developments led the Foreign Affairs Council to use the phrase in 2015, as well to the EC citing it in official policy documents in 2016, 2017, 2018, 2019, 2020.[9]

The notions that power gaps between great powers are shrinking, that Europe's internal security is threatened by conflicts and tensions in the Sahel and the Eastern Mediterranean, and that the world is growing to be more transactional has gone mainstream among EU policymakers.

The notions that power gaps between great powers are shrinking, that Europe's internal security is threatened by conflicts and tensions in the Sahel and the Eastern Mediterranean, and that the world is growing to be more transactional has gone mainstream among EU policymakers. Annegret Kramp-Karrenbauer, the German Defense Minister, recently stated "only if we take our own security seriously, will America do the same."[10] Though the term has most commonly been applied within the context of the EU's military capabilities – where it refers to the notion that the EU should be able to defend its borders and act militarily in its neighborhood without relying on the US[11] – the sentiment underpinning European strategic autonomy is far broader in scope. Competition over vaccine access during COVID-19 served to highlight the fundamentally asymmetrical nature of interdependence, with science, technology, trade, data, and investments all increasingly morphing into sources and instruments of force in international politics.[12] Within this context, European strategic autonomy has increasingly grown to encapsulate not only the need for European autonomy in military operations, but, more generally, the notion that the EU and its Member States ought to be able to make decisions without being constrained by their relationships with external actors.

Recent years have seen this logic linked to sensitive technologies more explicitly. In her 2019 inauguration speech, Commission President Ursula von der Leyen outlined the need for a "geopolitical Commission" capable of putting the EU on track to "lead the way on digital".[13] Dutch and Spanish officials have argued that the EU must "become more technically and digitally sovereign,"[14] a sentiment which has since been echoed by Paris and Berlin.[15] Combined with pieces of legislation such as the Commission's recently updated industrial and digital strategies,

7 "US to Withdraw Two Europe Combat Brigades," *BBC News*, January 13, 2012, sec. US & Canada, https://www.bbc.com/news/16543456; "Obama to Recall US Troops from Europe," *Financial Times*, April 8, 2011, https://www.ft.com/content/23852314-6236-11e0-8ee4-00144feab49a.

8 Peter Baker, "Biden Plays the Long Game as He Justifies the End of the 'Forever War,'" *The New York Times*, September 1, 2021, sec. US, https://www.nytimes.com/2021/09/01/us/politics/biden-politics-afghanistan.html.

9 Josep Borrell, "Why European Strategic Autonomy Matters," Text, EEAS, 2020, https://eeas.europa.eu/headquarters/headquarters-homepage/89865/why-european-strategic-autonomy-matters_en.

10 "Speech by AKK: Presentation of the Steuben Schurz Media Award," 2020, https://www.bmvg.de/en/news/speech-akk-presentation-steuben-schurz-media-award-3856630.

11 "Strategic Autonomy for the EU? How Europe Can Better Care for Its Security," *ECFR* (blog), March 15, 2018, https://ecfr.eu/event/strategic_autonomy_for_the_eu_how_europe_can_better_care_for_its_security/.

12 Borrell, "Why European Strategic Autonomy Matters."

13 Ursula von der Leyen, "Speech in the European Parliament Plenary Session" (Strasbourg, November 27, 2019), https://ec.europa.eu/info/sites/default/files/president-elect-speech-original_en.pdf.

14 "Spain-Netherlands Non-Paper on Strategic Autonomy While Preserving an Open Economy" (Kingdom of the Netherlands, March 24, 2021), https://www.permanentrepresentations.nl/documents/publications/2021/03/24/non-paper-on-strategic-autonomy.

15 "A Franco-German Manifesto for a European Industrial Policy Fit for the 21st Century" (Bundesministerium für Wirtschaft und Energie, February 19, 2019), https://www.gouvernement.fr/sites/default/files/locale/piece-jointe/2019/02/1043_-_a_franco-german_manifesto_for_a_european_industrial_policy_fit_for_the_21st_century.pdf

the Digital Services Act (DSA),[16] the Digital Markets Act (DMA),[17] the Cybersecurity Strategy,[18] and the General Data Protection Regulation (GDPR),[19] these statements have served to institutionalize the notion that digital and technological "sovereignty" refer to the bloc's ability to maintain independent ownership over and mastery of a predefined list of key (sensitive) technologies and to ensure they are applied in ways which are consistent with EU values.[20]

Achieving a greater degree of sovereignty within the tech space will require the implementation of policies – both offensive and defensive – and oversight processes geared towards circumventing techno-nationalist initiatives. It will also require a deepening of EU-level cooperation. The Netherlands' impressive innovation infrastructure notwithstanding, it cannot realistically strive to 'go it alone' as far as securing access to sensitive technologies is concerned. It is also bound by EU law, with the trading bloc commanding exclusive competences in many of the policy areas relevant to mitigating techno-nationalism. This means that its economic prosperity and military warfighting capabilities are set to remain dependent not only on other EU Member States' ability to safeguard their (domestic) technological know-how and research infrastructures against encroaching techno-nationalism, but on the Commission's ability to introduce, and enforce the EU-wide implementation of, relevant pieces of legislation.

The Netherlands' impressive innovation infrastructure notwithstanding, it cannot realistically strive to 'go it alone' as far as securing access to sensitive technologies is concerned.

This study aims to provide Dutch policymakers with an overview of steps they might take to interpret, implement, and enforce key pieces of existing EU legislation and pieces of national legislation it can introduce which do not clash with its commitments to the trading bloc. Crucially, it also provides a clear roadmap of initiatives falling within the EU's exclusive competences which the Netherlands should work towards achieving at the EU level. It begins with an identification of technologies that are critical to Dutch national prosperity and security (hereafter referred to as **sensitive technologies**),[21] providing an appraisal of the Netherlands' R&D capacities within each of these technologies. It then provides a concise overview of the various strategies of states to achieve techno-nationalist goals. This allows for the differentiation between directly and indirectly-oriented techno-nationalists – a distinction that helps to structure recommendations and to drive home the breadth of the techno-nationalist attack surface. It then identifies policy instruments that the Netherlands and the EU can employ to safeguard their innovation ecosystems from techno-nationalism. These policy options are transposed into policy recommendations based on an expert survey and on a gap analysis existing EU and NL-level policy initiatives and instruments.

16 "The Digital Services Act Package," European Commission, 2021, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

17 "Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act)" (European Commission, December 15, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0842&from=en.

18 "Cybersecurity Strategy," European Commission, 2021, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy.

19 "Regulation (EU) 2016/679 of the European Council of 27 April 2016 on the Protection of Natural Persons with Regard to Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)," Pub. L. No. 2016/679 (2016), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=NL.

20 "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on A New Industrial Strategy for Europe" (European Commission, October 3, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0102&from=EN.

21 With the exception of instances in which 3rd parties have been quoted as doing otherwise, this report refers to "sensitive" technologies rather than to "critical," "key," "cutting edge", or "emerging" technologies. **Sensitive technologies are defined as technologies that are critical to Dutch and EU national security and economic prosperity. These technologies are already reshaping entire economies and affecting the character of war – even if the ultimate consequences of these changes are difficult to predict.** Many are "cutting edge" or "emerging" in that research into their real-world applications remains in its infancy. The "sensitive" nomenclature is maintained within the context of this report to prevent confusion vis-à-vis terminology employed in pieces of international legislation, such as the Wassenaar Agreement.

2. What Technologies are of Critical Importance to the Netherlands?

The Netherlands' position as one of the wealthiest, safest, and most peaceful countries in the world depends to a large extent on its ability to remain at the forefront of innovation and exploitation of a relatively small group of sensitive technologies.

This Chapter provides the reader with an overview of the relevance of and the Dutch capacity to develop sensitive technologies. Categories of sensitive technologies are identified on the basis of an in-depth literature review of Dutch and international strategy and research documents. Relevance (importance) and Dutch capacity are each identified through a combination of literature review, expert interviews, and a survey circulated among Dutch research and policy people.

The exercise outlined in the previous paragraph provides the reader with a high-level overview of which technologies the Netherlands has robust research capabilities which technologies it is likely to need to source from 3rd countries. These findings are intended to facilitate strategic planning. Technologies which the Dutch innovation base has a competitive advantage in are likely to face techno-nationalist advances in the near-medium term. Policymakers should formulate concrete strategies for protecting these technologies. Conversely, they will need to formulate strategies to source technologies which the Netherlands has relatively less domestic know-how in.

The Netherlands' position as one of the wealthiest, safest, and most peaceful countries in the world depends to a large extent on its ability to remain at the forefront of innovation and exploitation of a relatively small group of sensitive technologies.[22] Dutch universities do cutting-edge work in a wide range of areas such as AI, quantum technologies, photonics, and semi-conductor lithography, and they attract the best and brightest researchers from around the globe. Dutch industry works closely with these universities to foster talent and to develop world-class technologies and products. The Dutch military has access, partly through its own technological base, and partly through its memberships in NATO and close relationship with the US, to the world's finest military technology.

As a relatively small, open economy, the Netherlands is highly reliant on the international exchange of ideas, goods, and people. This is especially true for sensitive technologies. The Netherlands needs to be able to attract the best students from around the world to drive its research into quantum technology, and it needs to retain access to markets around the world so that companies such as ASML can sell its top-of-the-line extreme ultraviolet lithography (EUV) semi-conductor lithography machines.

22 US

There is a downside to the globalized economy: the openness of the Dutch economic model leaves it vulnerable to the growing threat of techno-nationalism.

Though the Netherlands benefits enormously from international trade and exchange, there is a downside to the globalized economy: the openness of the Dutch economic model leaves it vulnerable to the growing threat of techno-nationalism. In sensitive technology areas in which the Netherlands is strong, such as semi-conductor lithography, there is a strong incentive for other countries to take advantage of the country's relative openness. They do this in several ways: poaching the best technical students from Dutch universities; purchasing Dutch technology that they cannot manufacture themselves; incentivizing Dutch companies to transfer intellectual property (IP) to domestic competitors; and outright theft, via espionage.[23] There is a growing recognition that the Netherlands needs to develop new strategies for protecting, maintaining and promoting its standing as a leader in some of the most important sensitive technologies.

Of course, in areas of sensitive technology in which the Netherlands is a follower rather than a leader, it should be able to gain access to these technologies by partnering with other countries. The surge in techno-nationalism includes strong protectionist elements. Increasingly, other states are implementing measures designed to prevent the transfer of sensitive technology abroad. This means that, if the Netherlands wishes to improve its standing in sensitive technology areas in which it is weaker, it needs to develop a strategy for doing so.

The first step in drafting a strategy for protecting areas of sensitive technologies in which the Netherlands is strong, and bolstering those areas in which it is somewhat weaker, is to develop a list of the most important sensitive technologies, estimate their impact, and the approximate timing of that impact.[24] This is the goal of the following section, which evaluates sensitive technologies in the areas of international security and economic prosperity.

23 Expert interviews; Jan Fred van Wijnen, 'Alarm over braindrain in kunstmatige intelligentie', *FD.nl*, October 29, 2018.

24 In developing this list, this report consulted the following works, among others: Ministerie van Defensie, 'Strategische Kennis- en Innovatieagenda (SKIA) 2021-2025 (27 November 2020); Ministerie van Economische Zaken en and Klimaat, 'Kwantitatieve analyse van onderzoek en innovatie in sleuteltechnologieën in Nederland', June 2018; 'Science and Technology Trends, 2020-2040' (NATO, March 2020); Michael E. O'Hanlon, 'Forecasting Change in Military Technology, 2020-2040' (Brookings Institution, 11 September 2018); Kelley M. Sayler, 'AI and National Security' (Congressional Research Service, 10 November 2020); Tim Sweijs and Frans Osinga, 'Maintaining NATO's Technological Edge', *Whitehall Papers* 95, no. 1 (2 January 2019): 104–18.

Box 2 – Methodological note: sensitive technologies

This section of the study examines twelve sensitive technologies that are relevant to the Netherlands. It is important to note that this list is neither definitive, nor is it static; it may change over time depending on how these technology areas develop.

The list of technologies assessed in this report was compiled after conducting a meta-review of Dutch and international scientific and policy-oriented literature, as well as by holding in-depth interviews with 8 experts on sensitive technology areas, some from the private sector, some from the public sector. For a full list of the sources consulted, see Annex I. For each of these technologies we evaluate their impact on two areas, international security and economic prosperity. In some cases, the impact of a technology in one area is different than in the other.

The technologies have been scored in two areas; namely: **estimated impact** and **timing**. For **estimated impact**, the study uses three categories: modest, significant, and revolutionary.

- Modest indicates that the technology will lead to a limited increase of the performance of military equipment or systems or increase economic growth only by a few percent.
- Significant suggests a much larger increase in performance or growth, at a minimum in the double digits.
- Revolutionary signifies that the technology will potentially render current military equipment/systems obsolete or create entirely new economic categories or processes.

For timing, the categories are as follows:

- Now indicates that the technology currently has a substantial impact.
- Soon suggests a substantial impact by 2030.
- Long-term predicts a substantial impact after 2030.

In order to evaluate the position of the Netherlands when it comes to sensitive technologies, the HCSS conducted a survey with leading experts in Dutch industry, academia, and the public sector. We sent the survey to 60 individuals; 26 responded. 50 percent work in the public sector, 38.5 in academia, and 11.5 percent in the private sector.[25] We asked the experts to rate the Netherlands in two categories:

- The importance of each technology for international security and economic prosperity, both for the Netherlands and for the world. (See Annex II for the full results of the survey, including scores for each technology area.)
- How the Netherlands compares with the rest of the world (**strength**) in terms of its development of each technology.

The results of the survey can be found in Figure 3.[26]

25 It should also be noted that expert surveys, though useful and widely-used tools for gathering data, are not infallible. Therefore, the survey data included in this report are by no means the final word on the importance of these technologies and the Netherlands' relative strength in each technology area.

26 The first part of this section, 2.1, refers to sensitive technology areas in terms of having a revolutionary, significant, or modest impact. In 2.2, the report refers to the importance of technologies and the Netherlands relative strength in those technology areas. This discrepancy is a result of the fact these two classifications – despite referring to what is essentially the same phenomena – were sourced through diverging methods at different phases of the overall research. Impact markers (revolutionary, significant, modest) were, as previously outlined, identified through expert interviews conducted at the beginning of the research. Technologies' importance – which is expressed as the average score assigned to a technology by experts in a survey, between 1 and 5 – was collected at a later phase of the research, with the explicit goal of ranking technologies through quantitative rather than qualitative methods.

2.1 The Relevance of Sensitive Technologies

Sensitive technologies are critical to Dutch and EU national security and economic prosperity. These technologies are already reshaping entire economies and affecting the character of war – even if the ultimate consequences of these changes are difficult to predict.[27] The Netherlands needs to keep abreast of these technologies if it wishes to be able to defend itself and its allies. For instance, in the 2020 Nagorno-Karabakh war, drones – part of the technology area robotics and autonomous systems (RAS) – gave Azerbaijan a pivotal edge. They provided significant advantages in intelligence, surveillance, and reconnaissance, as well as in Azerbaijan's long-range strike capabilities.[28]

Sensitive technologies are already reshaping entire economies and affecting the character of war – even if the ultimate consequences of these changes are difficult to predict.

Other technologies will only be relevant in the future – but will require years of R&D, so the Netherlands needs to invest time and resources in them today. AI is an area in which many applications are still at the R&D stage. Nevertheless, countries such as China, Russia, and the US are investing significant sums of money into AI military applications – the US plans to spend $874mn in 2022 – and experts predict that as soon as within the next five years, AI will begin to have an impact in areas such as intelligence collection and analysis. The results can already be seen in undertakings such as Project Maven, a US Department of Defense project that interprets data from unmanned drone videos. In other instances, such as fully autonomous vehicles, it will likely take longer for the technology to reach the battlefield.[29]

The same current-future dichotomy applies to the impact of sensitive technologies on economic prosperity. In many areas, these technologies are already playing a big role in the Dutch economy. For instance, in the field of photonics, more than 20,000 people work in the industry at an estimated 290 companies, generating a profit of EUR 4.2bn.[30] In contrast, quantum technology holds considerable promise for economic development in areas such as communications, trading and finance, mining and extraction, healthcare services, energy, and ICT, but mostly in the future.[31] In 2021, the global market for quantum technology was only $9.21bn. It is expected to reach $31.6bn by 2026 and as high as $300bn by 2050.[32]

27 Justin Lynch, 'Yet Another Article about Information Technology and the Character of War', War on the Rocks, 2 September 2020, https://warontherocks.com/2020/09/yet-another-article-about-information-technology-and-the-character-of-war/.

28 'The Air and Missile War in Nagorno-Karabakh: Lessons for the Future of Strike and Defense', accessed 24 June 2021, https://www.csis.org/analysis/air-and-missile-war-nagorno-karabakh-lessons-future-strike-and-defense.

29 John Keller, 'Pentagon to Spend $874mn on AI (AI) and Machine Learning Technologies next Year', Military Aerospace, 4 June 2021, https://www.militaryaerospace.com/computers/article/14204595/artificial-intelligence-ai-dod-budget-machine-learning; Zachary Fryer-Biggs, 'In Project Maven's Wake, the Pentagon Seeks AI Tech Talent,' Wired, accessed 8 July 2021; Kelley M. Sayler, 'AI and National Security' (Congressional Research Service, 10 November 2020).

30 "National Agenda Photonics," 11-13.

31 "Economic Impact of Quantum Technologies," National Research Council, accessed May 4, 2021, https://nrc.canada.ca/en/research-development/research-collaboration/programs/economic-impact-quantum-technologies.

32 Research and Markets ltd, 'Quantum Technology Market by Computing, Communications, Imaging, Security, Sensing, Modeling and Simulation 2021 - 2026', accessed 24 June 2021, https://www.researchandmarkets.com/reports/5317365/quantum-technology-market-by-computing; Ministerie van Economische Zaken en Klimaat, 'Nationale Agenda Quantumtechnologie - Brochure - Rijksoverheid.nl', brochure (Ministerie van Algemene Zaken, 18 February 2020), https://www.rijksoverheid.nl/documenten/brochures/2020/02/17/nationale-agenda-quantumtechnologie.

2.1.1 International Security

The following section provides a brief analysis of the relevance of sensitive technology groups in international security, including their estimated impact and the timing of that impact. More detailed overviews of each technology group can be found in Annex I.

Table 3 - Sensitive technologies' impact on international security

Technology	Estimated Impact[33]	Estimated Timing[34]
AI	Revolutionary	Long Term
Big Data	Revolutionary	Soon
Bio and Human Enhancement Technologies (BHET)	Modest to Significant	Soon
Chemical Technologies	NA	NA
Photonics	Significant	Now to Soon
Quantum Technologies	Revolutionary	Soon to Long Term
RAS	Significant to Revolutionary	Soon
Semi-conductor Lithography	Significant	Now
Sensor Technologies	Modest	Long Term
Space Technologies	Modest to Significant	Soon to Long Term
Weapon Technologies	Modest (directed energy weapon – DEW) to Significant (Hypersonics)	Soon
3D printing and advanced materials	Modest to Significant	Soon to Long Term

Table 3 depicts the estimated impact on international security, and the timing of that impact, of the twelve sensitive technology areas examined in this report. Four technology areas will have a revolutionary impact: AI, big data, quantum, and possibly RAS. Three technology areas will have a significant impact: photonics, semi-conductor lithography, and weapon systems (hypersonic weapons). Three technology areas will have a modest to significant impact: biotechnology and human enhancement, space technologies, and 3D printing and advanced materials. Two technology areas will have a modest impact: sensor technologies and weapon technologies (directed energy weapons). Chemical technologies will not have a direct impact on international security.

Two technology areas will have an impact in the long term: AI and sensor technologies.

As for the expert-estimated timing depicted in Table 3, two technology areas will have an impact in the long term: AI and sensor technologies. Three technology areas will have an impact in the soon to long term: quantum technologies, space technologies, and 3D printing and advanced materials. Four technology areas will have an impact soon: big data, biotechnology and human enhancement, RAS, and weapons technologies. One technology area will have an impact now or soon: photonics. Survey data also indicates that one technology area, semi-conductor lithography, is having an impact now.

33 **Modest** indicates that the technology will lead to a limited increase of the performance of military equipment or systems or increase economic growth only by a few percent. **Significant** suggests a much larger increase in performance or growth, at a minimum in the double digits. **Revolutionary** signifies that the technology will potentially render current military equipment/systems obsolete or create entirely new economic categories or processes. See Box 3.

34 **Now** indicates that the technology currently has a substantial impact. **Soon** suggests a substantial impact by 2030. **Long-term** predicts a substantial impact after 2030. See Box 3.

2.1.2 Economic Prosperity

The following section provides a brief analysis of the relevance of sensitive technology groups relevant to economic prosperity, including their estimated impact and the timing of that impact. More detailed overviews of each technology group can be found in Annex I. These overviews are based on a review of Dutch and international literature, as well as expert interviews.

Table 4 - Sensitive technologies' impact on economic prosperity

Technology	Estimated Impact[35]	Estimated Timing[36]
AI	Revolutionary	Now
Big Data	Modest	Now
BHET	Significant	Now
Chemical Technologies	Modest to significant	Now
Photonics	Significant	Now
Quantum Technologies	Significant to Revolutionary	Soon
RAS	Significant to Revolutionary	Now
Semi-conductor Lithography	Significant to Revolutionary	Now
Sensor Technologies	Modest	Now
Space Technologies	Significant to Revolutionary	Now to Long Term
Weapon Technologies	NA	NA
3D printing and advanced materials	Significant to Revolutionary	Now

AI's impact will be revolutionary.

Table 4 depicts the estimated impact on economic prosperity, and the timing of that impact, of the twelve sensitive technology areas examined in this report. One technology, AI, will have a revolutionary impact. Five technologies will have a significant to revolutionary impact: quantum, RAS, semi-conductor lithography, space technologies, and 3D printing and advanced materials. Two technology areas, BHET and photonics, will have a significant impact. One technology area, chemical technologies, will have a modest to significant impact. Two technology areas, big data and sensor technologies, will have a modest impact. Weapon technologies will not have a direct impact on economic prosperity.

As for the estimated timing depicted in Table 4, nine technology areas are having an impact now: AI, big data, BHET, chemical technologies, photonics, RAS, semi-conductor lithography, sensor technologies, and 3D printing and advanced materials. Space technologies will have an impact between now and the long term. Quantum technologies will have an impact soon.

35 **Modest** indicates that the technology will lead to a limited increase of the performance of military equipment or systems or increase economic growth only by a few percent. **Significant** suggests a much larger increase in performance or growth, at a minimum in the double digits. **Revolutionary** signifies that the technology will potentially render current military equipment/systems obsolete or create entirely new economic categories or processes. See Box 3.

36 **Now** indicates that the technology currently has a substantial impact. **Soon** suggests a substantial impact by 2030. **Long-term** predicts a substantial impact after 2030. See Box 3.

2.2 What Sensitive Technologies Should the Netherlands Invest in?

In the previous section, as the first step in developing a strategy for protecting areas of sensitive technologies in which the Netherlands is strong, and bolstering those areas in which it is somewhat weaker, the report scored sensitive technologies in terms of estimated impact and timing.

The next step is to evaluate the Netherlands' relative strength in these areas. The Netherlands needs to know not only what is important, but also what it is good at. This is necessary to be able to craft appropriate policies, including be able to decide which technology areas to protect and which should be obtained from other states.

The Netherlands will want to protect technology areas in certain situations. For instance, ASML's EUV lithography machines are the only devices capable of producing the most advanced microchips. The company therefore has significant strategic value within the conterxt of the ongoing global chip shortage.

More specifically, many technologies are important to the Netherlands, but not all are relevant. Also, the Netherlands is not at the cutting-edge of research or development in all technologies. The Netherlands needs to take an inventory of what it is good at, so these technology areas can be protected and promoted. The Netherlands may also wish to protect technology areas in certain situations. For instance, the Dutch company ASML's EUV lithography machines are the only devices capable of producing the most advanced microchips. These microchips are essential for economic prosperity, but also have implications for national security. It is in the interest of the Netherlands to maintain control over access to EUV lithography machines to prevent them from being obtained for reasons that could run contrary to Dutch interests or values.

It is necessary to identify sensitive technology areas in which the Netherlands is less strong, so that policymakers, industry, and researchers know what to prioritize in the future or find partnerships. In particular, the Netherlands needs to consider in which areas it needs to develop and maintain domestic expertise in certain technologies, to avoid developing dangerous dependencies. AI in the international security sector represents an example of this type of technology. The Netherlands will increasingly need domestic expertise in AI to be able to understand how its military systems function.

As is outlined in Box 3, the report conducted a survey to score technologies on their importance and on the Netherland's relative strength, including in R&D, as it relates to them. The results of this survey are outlined in Figure 3.

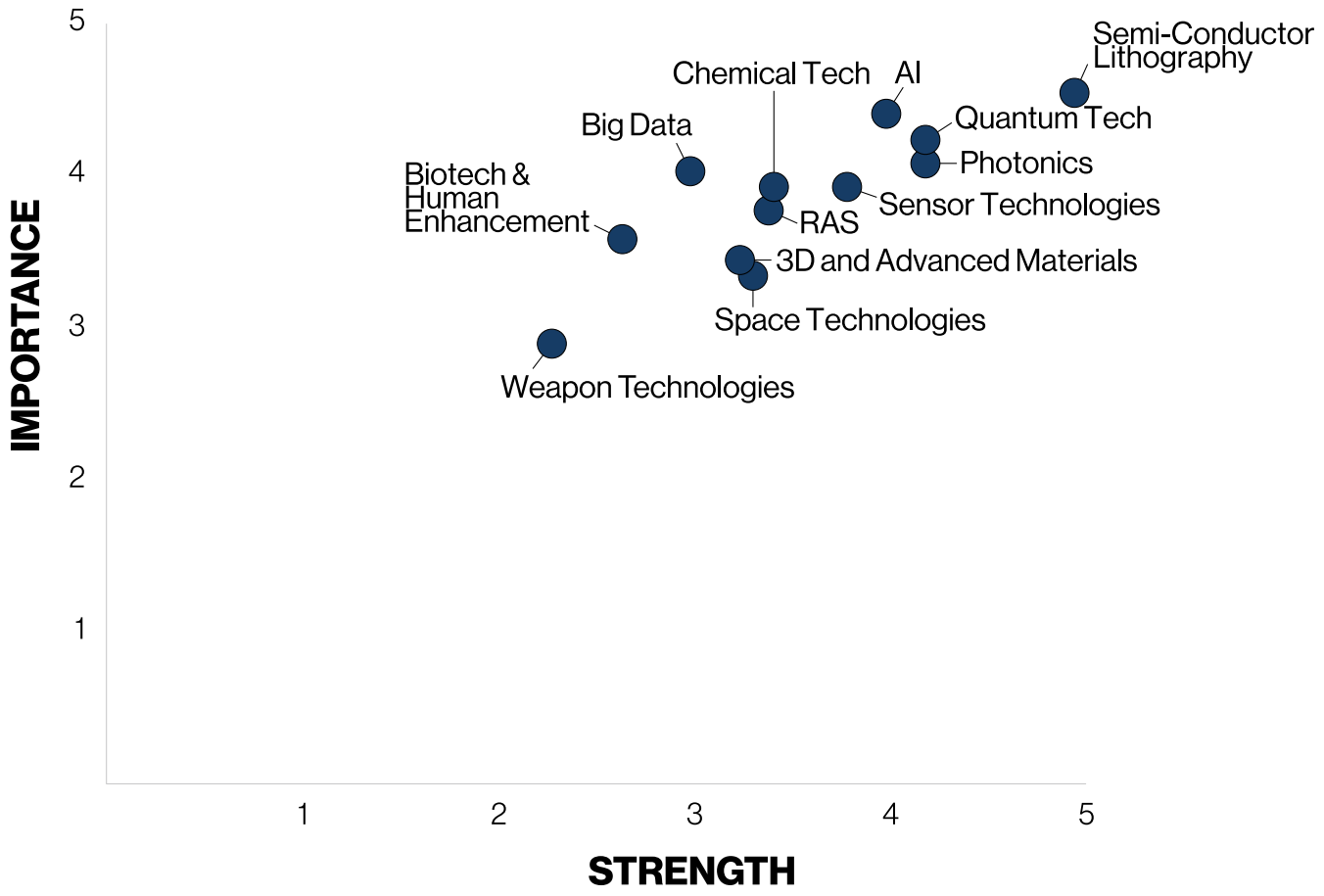

Figure 3 - Strength and importance in sensitive technology areas for the Netherlands

2.2.1 Strength and Importance in Sensitive Technology Areas for the Netherlands

Figure 3 depicts experts' appraisal of the twelve sensitive technology areas examined in this report, scored according to two factors: how strong the Netherlands is in each area, as compared to other states; and how important each technology area is to the Netherlands. For the full scores, which are based on a survey of experts on sensitive technologies, see Annex II.

The Netherlands' R&D capacities are relatively robust in most sensitive technology areas.

Overall, the results are positive for the Netherlands: it is relatively strong in most of the important technology areas. That said, within Figure 3 there are some notable differences, and several sub-categories can be identified. These sub-categories are based on the distribution of the data in the expert survey. They are intended to provide policymakers with some general guidelines for approaching the subject in an organized manner.

2.2.2 Tier One

In the first tier, standing alone, is **semi-conductor lithography**. It is the most important because it ranks first both in terms of importance and strength. The Netherlands is a world leader in this area. The Dutch company ASML is the world's largest manufacturer of photolithography systems for the semi-conductor industry.[37]

37 'How ASML Became Chipmaking's Biggest Monopoly', *The Economist*, 29 February 2020, https://www.economist.com/business/2020/02/29/how-asml-became-chipmakings-biggest-monopoly.

2.2.3 Tier Two

In the second tier, there are three technology areas in which the Netherlands is strong and which are important. First, **AI**: The Netherlands is relatively strong on the commercial side of AI. World-class research in AI is taking place at Dutch universities, and Dutch universities are good at developing collaborations with foreign companies. However, brain drain is a problem. In addition, there is concern in the field that, when compared to countries such as the US, the environment for investment is less than ideal and that there is a lack of innovation in the industrial sector, which helps to prevent the emergence of Dutch companies on the scale of Google or Apple.[38] One exception to this trend is TomTom, a successful Dutch consumer electronics and navigation company which increasingly uses AI for mapmaking.[39] Although the Netherlands does cutting-edge theoretical research on AI, it struggles to translate this work into applications that have direct relevance for international security. The Dutch government explored the possibility of holding a Dutch version of the Defense Advanced Research Projects Agency's (DARPA's) Cyber Grand Challenge but concluded that there was not sufficient expertise in the country for such an event. This lack of expertise is a problem: it forces the Netherlands to rely on foreign partners, creating dependencies. Furthermore, AI is special; without domestic expertise, the Netherlands will lack the ability to understand what its own systems are doing.[40]

The Netherlands is not one of the major players when it comes to quantum technologies.

Also in the second tier, the Netherlands is strong in the area of **quantum technologies** compared to most states. It is strong in the knowledge creation side of the field. But it lags behind the leaders, such as the US, and is weaker when it comes to exploiting potential commercial opportunities linked to quantum technologies. The Netherlands is not one of the major players when it comes to work on quantum technology with direct relevance to international security. However, TNO is doing important work on the technical side that has relevance to international security. QuSoft, a research center, is working on cryptography. At least one Netherlands-based researcher is working on a project funded by the US Department of Defense's DARPA. And cutting-edge academic work is being done at Technische Universiteit (TU) Delft and the University of Amsterdam.[41]

Finally, the Netherlands is strong compared to other countries when it comes to **photonics**. According to the International Society for Optics and Photonics, Dutch companies are among the most competitive in the field. However, their overall market share remains limited, with scope for the Netherlands to expand in this field. From 2015 to 2020, the size of the global photonics market nearly tripled, from $228bn to an estimated $614bn, an annual growth rate of more than 6.4 percent. In the Netherlands, more than 20,000 people work in the industry at an estimated 290 companies, generating a profit of EUR 4.2bn. The most notable companies include ASML, Océ-Canon, Signify, Philips Healthcare and Prysmian Group.[42] The Netherlands mostly does not focus on aspects of the field with direct international security applications.

38 Interview with expert, May 18, 2021.

39 Pierluigi Casale, 'How Does AI Improve Mapmaking? TomTom, 13 February 2020, https://www.tomtom.com/blog/maps/artificial-intelligence-map-making/.

40 Expert interview.

41 Expert interview; '$2.1M DARPA Grant Puts Lehigh Univ. Optimization Experts at Vanguard of Quantum Computing', EurekAlert!, accessed 14 June 2021, https://www.eurekalert.org/pub_releases/2020-03/lu-dg032020.php.

42 "National Agenda Photonics," 11-13.

2.2.4 Tier Three

In tier three, there are five technology areas in which the Netherlands is moderately strong when compared to other countries; these technologies are somewhat important. First, **sensor technologies**: The Netherlands is strong in a few critical areas of sensor technology, especially laser (including firms such as VTEC) and optical (where TNO does cutting edge work).[43] In the international security sphere, Nederland Radarland is a platform in which different entities collaborate to promote research and innovation in the field of radar sensors. Participants in this initiative are the Ministry of Defense (MoD), Thales Nederland, TNO, TU Delft and the Ministry of Economic Affairs and Climate (EZK), along with some small to medium-sized enterprises (SMEs). Another notable research project is "Unmanned Under Water Sensors 2035," also supported by the MoD. This program is designed to gather the knowledge and expertise required to enable the deployment, by 2035, of several underwater unmanned sensors able to perform multiple tasks independently and in coordination with one another.[44]

The Netherlands is home to several institutions at the forefront of research about chemical manufacturing technologies, including Maastricht University, Tilburg University, TU Eindhoven, Brightsite, Chemelot-InSciTe, DIFFER, and TNO.

The Netherlands is home to several institutions at the forefront of research about **chemical** manufacturing **technologies**, including Maastricht University, Tilburg University, TU Eindhoven, Brightsite, Chemelot-InSciTe, DIFFER, and TNO, which creates a favorable environment for the development of innovative chemical technologies. Additionally, the Netherlands hosts many large international firms operating in the field of chemical manufacturing, such as OW Chemical, SABIC, Air Products, Yara, OCI Nitrogen, Cosun and Shell Moerdijk. These companies are at the forefront of the effort to implement innovative green chemical technologies.[45]

In the area of **space technologies**, the Netherlands has a sophisticated space industry, with the nexus between universities (notably Delft TU) and the private sector playing an important role.[46] Dutch firms provide services such as smallsats, sensors and satellite components, thermal control systems, space vehicles, and nanosatellites, and many are well-positioned to take advantage of the substantial growth prospects in the sector.[47] The Netherlands specializes in a few key areas. One is providing for secure communications in space (laser and optical communications), based on its expertise in photonics. Cutting edge work is being done at TNO and Airbus, working with some SMEs. Another area of specialization is nanosatellites with miniaturized sensors and earth observation (EO) instruments. Dutch companies such as ISISPACE and NLR are active in this area.[48] Key priorities for the Netherlands in the coming years will be position, navigation, and timing (PNT); space situational awareness (SSA); ground-based situational awareness (GSA); secure communications; and the development of partly or wholly Dutch-owned space assets.[49] The Netherlands has no military space program and uses other countries' satellites. However, there is a desire to develop more Dutch-controlled assets and capabilities to reduce foreign dependencies. In 2021, it began

43 Expert interview.

44 "Strategische Kennis- En Innovatieagenda 2021-2025" (Ministerie van Defensie, December 2020), 48.

45 "Groene Chemie, Nieuwe Economie" (TNO, February 2021), 16.

46 Hugo van Manen, Tim Sweijs, and Patrick Bolder, "Towards a Space Security Strategy Action Points for Safeguarding Dutch Security and Prosperity in the Space Age" (The Hague Centre For Strategic Studies, March 2021), 4-5.

47 van Manen, Sweijs, and Bolder, 4.

48 Expert interview.

49 Expert interview.

launching mini satellites with partners such as Virgin Orbit, including a nanosatellite called Brik-II.[50] In addition, the MoD will soon publish a Defense Space Agenda.[51]

The Netherlands is strong in some areas of RAS, with cutting edge research being done at TU Delft and TU Eindhoven in subfields such as medical robotics and cognitive robotics, and organizations such as Holland Robotics bringing together interested parties in the private and public sectors. The Netherlands relies on foreign partners for RAS technology, as there are no Dutch companies making big investments in this area. For the most part, this is not a problem, though there is some concern about being dependent on foreign algorithms and software.[52]

The US dominates the 3D printing and advanced materials market, but Europe commands the second-largest market share, with Germany, the UK, Italy, and France leading the way.[53] The Netherlands trails these top countries, but still features some cutting-edge work in companies such as Ultimaker and the Province of North Holland's project XL-3D printers.[54] Key centers of research in this area include the industrial design faculties at TU Delft and TU Eindhoven.

The Netherlands relies on foreign partners for RAS technology, as there are no Dutch companies making big investments in this area.

2.2.5 Tier Four

There are two technology areas that are important for the Netherlands, but in which it is relatively weak when compared to other states. The Netherlands is strong on the commercial side of BHET, with several large biotech firms present in the region. It also has the building blocks for substantial further growth in the sector, with excellent universities and transport infrastructure. One report predicts additional annual gross domestic product (GDP) of €7bn and the creation of 100,000 additional jobs by 2030.[55] The Netherlands is not a world leader when it comes to research into biotechnology and human enhancement technologies with direct international security applications. However, as with some of the other technology areas, research institutes and universities such as TU Delft (with its Interactive Intelligence Group) and TNO (research groups include Human Performance, Perceptual and Cognitive Systems) do cutting-edge work that has numerous theoretical and indirect links to international security.

When it comes to big data, the Netherlands is relatively strong on the commercial side. Dutch companies such as ING and Booking.com make extensive use of the technology.

50 Kees de Waal, 'The Netherlands Launches Its First Military Nanosatellite - NLR News', Royal Netherlands Aerospace Centre, 26 January 2021, https://www.nlr.org/news/the-netherlands-launches-its-first-military-nanosatellite/; 'Virgin Orbit Aims to Launch Multiple Satellites in June', AP NEWS, 6 May 2021, https://apnews.com/article/business-f71b8e00cca1d7d60031af93df7c5000.

51 Expert interview; https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2021/05/20/beantwoording-kamervragen-over-hcssclingendael-publicatie/beantwoording-kamervragen-over-hcssclingendael-publicatie.pdf

52 Expert interview.

53 "Additive Manufacturing Around the World: What Is the State of 3D Printing Adoption in North America and Europe?," AMFG Autonomous Manufacturing, November 7, 2019, https://amfg.ai/2019/11/07/additive-manufacturing-around-the-world-what-is-the-state-of-3d-printing-adoption-in-north-america-and-europe/.

54 "Additive Manufacturing Around the World;" "Sustainable Building Design for the Masses with XL-3D Printers from Amsterdam-Projects," European Commission, accessed May 12, 2021, https://ec.europa.eu/regional_policy/en/projects/Netherlands/sustainable-building-design-for-the-masses-with-xl-3d-printers-from-amsterdam.

55 "Scaling Innovation: How Benelux Could Become Europes Leading Biotech Hub" (McKinsey, March 2020), https://www.mckinsey.com/~/media/mckinsey/industries/pharmaceuticals%20and%20medical%20products/our%20insights/biotech%20in%20europe%20a%20strong%20foundation%20for%20growth%20and%20innovation/scaling-innovation-how-benelux-could-become-europes-leading-biotech-hub-march%202020.pdf.

Booking com even has a blog dedicated to data science and machine learning.[56] However, the Netherlands lags behind other states when it comes to the use of big data in applications with direct international security implications.

The Netherlands also emerges as being fairly weak on weapon technologies, including directed-energy weapons and hypersonic weapons. However, the experts in the survey conducted for this report believe it to be of relatively low importance for the Netherlands.

56 Juan Monge, "How ING Engages Customers with Big Data and the Internet of Things," Internet of Business, January 13, 2017, https://internetofbusiness.com/ing-customers-big-data-iot/; 'How Booking.Com Leverages Its Online Data to Get Grip on the Customer Service Workload Forecast', MIcompany, accessed 8 July 2021, https://micompany.nl/inspiration/how-booking-com-leverages-its-online-data-to-get-grip-on-the-customer-service-workload-forecast/; 'Booking.Com Data Science', Booking.com Data Science, accessed 8 July 2021, https://booking.ai/.

2.3 Key Takeaways

- Sensitive technologies are crucial to Dutch and EU national security and economic prosperity. Some of these technologies are already having a big impact; others will only play a major role in the future, but in order for the Netherlands to be able to harness these technologies, significant planning and investment needs to take place now.
- Four technology areas could revolutionize international security: AI, big data, quantum technologies and (partially) RAS.
- Five technology areas will have a significant impact on international security: BHET, photonics, semi-conductor lithography, space technologies, weapon technologies (hypersonic weapons), and 3D printing and advanced materials.
- One technology – sensors – will have a modest impact on international security, and one – directed energy weapons – a partially modest impact.
- Six technology areas could have a revolutionary impact on economic prosperity: AI, quantum technologies, RAS, semi-conductor lithography, space technologies, and 3D printing and advanced materials.
- One technology area will have a significant impact on economic prosperity: BHET.
- Two technology areas will have a modest impact on economic prosperity: big data and sensor technologies.
- The Netherlands is strong, to one degree or another, in many of the most important technology areas: notably semi-conductor lithography, AI, quantum technologies, and photonics.
- The Netherlands is less strong in two areas that are relatively important: BHET, and big data.

3. An Overview of Techno-Nationalism

This Chapter provides the reader with a high-level overview of the measures and approaches states employ in the pursuit of techno-nationalism. It is intended to be generic; it describes patterns of behavior that can be used either to transfer technology from a 3rd state or to erode a 3rd state's ability to compete with domestic industry.

This results in the presentation of a conceptualization of techno-nationalism which is relatively far broader than many "competing" concepts, with practices such as cybercrime, espionage, and the (abuse of) open market dynamics (among others) all being identified as possible tools for undermining the Netherlands' security interests.

For a quick overview of the measures this study subsumed within techno-nationalism, please refer to Annex IV: Taxonomy of Techno-Nationalism; an Overview.

Techno-nationalism stems from the notion that a state's technological innovation and capabilities are directly linked to its national security.

Techno-nationalism stems from the notion that a state's technological innovation and capabilities are directly linked to its national security. This creates incentives for states – and great powers in particular – to treat access to sensitive technologies as a zero-sum game at the global level. It is playing an increasingly central role in international competition. The US, Russia, China, and India have all formulated and pursued policies geared towards expanding national control over (and, in the case of the US and China, international influence through) sensitive technologies in recent years. Even the EU has taken overt and covert steps to implement techno-nationalist strains of thinking into its foreign policy. Policies such as the European Commission's proposed 2021 AI Act,[57] as well as Ursula von der Leyen's[58] identification of technology as one of the Commission's top priorities for the next five years, speak to the bloc's recognition of modern technologies' potentially disruptive nature.[59]

The global scramble to secure access to sensitive technology and to expand state influence through its export has played out in several times in recent years. Recent controversies surrounding European Member States' (un)willingness to utilize Huawei technology within their national 5G infrastructures provide a good example of this dynamic. Financial incentives created by Beijing's subsidization of Huawei have complicated this discussion considerably. Deutsche Telekom AG, a German cellphone operator, claimed in 2019 that rolling out 5G without Huawei would delay its network by at least two years and increase the costs of its

57 "Regulation of the European Parliament and of the Council: Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts," April 21, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

58 Ursula von der Leyen has been President of the European Commission since 1 December 2019.

59 Von der Leyen went was far as to proclaim that "we must have mastery and ownership of key technologies in Europe" in her 2019 ascension speech, something which speaks to her recognition of sensitive technologies as a vector for foreign influences. See Tyson Barker, "Europe Can't Win Its War for Technology Sovereignty," *Foreign Policy*, January 16, 2020, https://foreignpolicy.com/2020/01/16/europe-technology-sovereignty-von-der-leyen/.

construction by billions.[60] A Wall Street Journal investigation conducted in the same year found that Huawei received as much as $75bn in state support in the run-up to 2020,[61] something which likely contributed to the company's ability to offer 5G hardware at significantly lower costs than rivals such as Ericsson and Nokia Oyj.[62]

Two arguments have been leveraged against the prospect of integrating Huawei into the EU's 5G "core". The first – and one which has been afforded significant credence in the wake of recent headlines – posits that an overreliance on Huawei's technologies opens the door to privacy infringements and espionage.[63] European Member States remain split on whether and how to utilize Huawei's technologies in the introduction of their 5G networks. Spain and Hungary have both expressed their intent to use Huawei equipment in their 5G "cores." Romania, Poland, the Czech Republic, Latvia, and Estonia have all pledged not to do business with companies that are subject to state interference.[64]

Techno-nationalism creates incentives for states – and great powers in particular – to treat access to sensitive technologies as a zero-sum game at the global level.

The second, tellingly, emphasizes the (negative) strategic implications of opting into dependence on Chinese manufacturers to maintain critical infrastructures.[65] This criticism – that an action or choice risks erosion of one actor's autonomy by increasing its dependence on another – is one which Huawei's push to provide European Member States with components to integrate into their 5G "cores" shares with NVIDIA's acquisition of ARM (previously outlined). Given the fact that Huawei's initiative arguably poses a far greater risk to European technological sovereignty than does NVIDIA's acquisition of ARM, this is unintuitive. NVIDIA is an independent US-based entity; Huawei is a China-based entity with strong ties to the Chinese Communist Party (CCP). NVIDIA's acquisition is being driven, first and foremost, by the company's motivation to gain a competitive edge by securing access to ARM's employee and patent base; Huawei's foray into the EU's 5G "core" would see the at-scale delivery of proprietary physical components to the bloc's telecom giants. This allows for a broad distinction between two different types of techno-nationalists; namely: states which pursue techno-nationalist policies through direct government interaction with private sector actors, and states which pursue them through indirect means (Table 5).

Table 5 - Directly vs. indirectly oriented techno-nationalists

Direct	Indirect
The state views private sector actors as a direct extension of itself and plays a direct role in facilitating beneficial technology transfers from foreign countries and companies. Private sector actors have relatively little autonomy, but receive a bevy of direct (whether formalized or not) advantages over international competitors through state policy.	The state views private sector actors as an indirect extension of itself. The state seeks to facilitate beneficial technology transfers by creating a regulatory environment that empowers private sector actors to act aggressively or uncompetitively. Private sector actors enjoy a high degree of autonomy and enjoy various forms of indirect protection from prosecution.

60 "Huawei Is a Paralyzing Dilemma for the West," *Bloomberg.Com*, November 23, 2019, https://www.bloomberg.com/opinion/articles/2019-11-23/huawei-s-5g-networks-are-a-paralyzing-dilemma-for-the-west.

61 State support came in the form of tax breaks, financing, and cheap resources. See Chuin-Wei Yap, "State Support Helped Fuel Huawei's Global Rise," *Wall Street Journal*, December 25, 2019, sec. Tech, https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736.

62 "Huawei Is a Paralyzing Dilemma for the West," Bloomberg.com, November 23, 2019, https://www.bloomberg.com/opinion/articles/2019-11-23/huawei-s-5g-networks-are-a-paralyzing-dilemma-for-the-west.

63 Huib Modderkolk, "Huawei kon alle gesprekken van mobiele KPN-klanten afluisteren, inclusief die van de premier," de Volkskrant, April 17, 2021, https://www.volkskrant.nl/gs-bd1aece1.

64 Patrick Wintour, "Europe Divided on Huawei as US Pressure to Drop Company Grows," *The Guardian*, July 13, 2020, sec. Technology, https://www.theguardian.com/technology/2020/jul/13/europe-divided-on-huawei-as-us-pressure-to-drop-company-grows.

65 "Europe's 5G Plans in Limbo after Latest Salvo against Huawei," *POLITICO*, August 23, 2020, https://www.politico.eu/article/europe-5g-plans-in-limbo-after-latest-salvo-against-huawei/.

3.1 Measure Types

Though the context surrounding these examples differs significantly, the cases of Huawei's foray into the EU's 5G infrastructure and of NVIDIA's ARM acquisition are both cases of actors leveraging the EU's open market – and circumventing existing safeguards – in ways that potentially undermine the trading bloc's technological sovereignty. From the Dutch perspective (and the European perspective more broadly), techno-nationalist measures can, broadly speaking, be divided into two high-level categories; namely: **measures that transfer technology and/or technological know-how** and **measures that make for an uneven playing field**.

3.1.1 Measures that Transfer Technology and/or Technological Know-How

Securing access to sensitive technologies is key motivator for techno-nationalists.

In 2007, Chinese hackers stole technical documents related to the development of the F-35 from Lockheed Martin. As recently as 2017, Chinese hackers went after Australian F-35 contractors, securing even more technical information on the cutting-edge fighter in the process.[66] Come 2019, images emerged of the People Liberation Army's (PLA's) J-20 stealth fighter sporting a sensor system that bore an uncanny resemblance to Lockheed Martin's Electro-Optical Targeting System (EOTS).[67]

Securing access to sensitive technologies is key motivator for techno-nationalists. Leapfrogging or gaining an edge over an adversary's technological advantage helps to level the playing field between great powers, something which has strengthened the incentive for the US and China to do so as they have inched closer to technological parity over time. These transfers can be achieved – as can be observed in the F-35 example – through espionage, but they can also be achieved through open market-based and legislative toolkits (Table 6).

Table 6 - Approach typology; measures that transfer technology and/or technological know-how

Approach type	Approach description
Market-based	The use of open-market mechanisms (i.e.: free flow of goods and services, right to invest in 3rd parties, etc.) to facilitate the unwanted transfer of technology or technological know-how from a foreign state. Within the context of sensitive technologies, this approach is made viable – at least in part – by sensitive technology's tendency to outpace regulatory efforts.
Legislative	The use of domestic legislative frameworks to erode foreign companies' ability to protect their IP. These laws can range from localization barriers to trade (LBTs – hereafter referred to as "lose the market" laws) laws to "violate the law" or "no choice" dynamics. These approaches to securing access to sensitive technology are typically grounded in recognition of the fact that accessing the implementing country's domestic market constitutes a key (or even non-omissible) component of foreign companies' growth strategies.
Forced	The use of coercive, bad-faith, or criminal instruments to secure access to (whether in the form of blueprints, algorithms, or other) the sensitive technologies developed by 3rd parties.

These activities infringe on Dutch and/or EU-level technological sovereignty in several ways. In instances where the transfer of a European technology does not result in the transfer

66 Task and Purpose, "Hacked: How China Stole US Technology for Its J-20 Stealth Fighter," Text, The National Interest (The Center for the National Interest, July 10, 2019), https://nationalinterest.org/blog/buzz/hacked-how-china-stole-us-technology-its-j-20-stealth-fighter-66231.

67 Purpose.

of corresponding technological know-how or of R&D or manufacturing capabilities, they erode affected parties' competitive advantage. Technology transfers facilitated through (for example) espionage or through "lose the market" laws allow 3rd parties to forego the R&D costs associated with developing them, meaning that these suppliers do not need to subsidize these costs through product sales. This effect is amplified when technologies are transferred through measures that also transfer R&D or manufacturing capabilities (read: personnel). These transactions provide the receiving party with access to human resources and infrastructure which have, in many cases, cost the country from which they are being transferred many years and millions (if not tens or hundreds of millions) of Euros to foster. These types of transfers allow the receiving state to leverage the technology and technological know-how gained to foster dependence because the state from which it has received them has a.) been deprived of its access to said technology, and b.) will need to invest significant time and funding into rebuilding its capacity to develop it independently. They also erode technological sovereignty by removing control over how the transferred technology should be used (and which actors should have access to it) from the state which has developed it. In some instances, it also bolsters the technological know-how of adversarial states.

A key consideration is that techno-nationalism erodes Dutch firms' competitive advantage. This reduces their ability to invest in R&D and to contribute to maintaining the Netherlands' technological sovereignty in the long term.

3.1.1.1 Market-Based Approaches to Transferring Technology and/or Technological Know-How

Market-based approaches exploit open market mechanisms to facilitate the unwanted transfer of technology or technological know-how. Within the context of sensitive technologies, these approaches derive their viability from legislative systems' inability to "keep up" with developments in sensitive technologies, deficits in many states' ability or willingness to take a strategic approach to regulating their internal markets, and to continued (often non-reciprocal) reverence for free trade principles. These approaches include the purchase of foreign companies, other forms of foreign direct investment (FDI), patent licensing, or the purchase of high-tech goods and services.

FDI & Acquisitions

FDI & acquisitions offer a clear path to acquiring both technology and technological know-how. NVIDIA's acquisition of ARM (previously discussed in-depth) offers a clear case study of how corporate acquisitions can facilitate technology transfer,[68] but it is important to note that other forms of FDI can also be associated with negative side-effects. Within the context of sensitive technologies, this dynamic is particularly pronounced in investments that come with conditionality clauses attached or which afford groups or individuals positions on the boards of publicly-traded companies. These types of arrangements risk resulting in outcomes that are suboptimal either a.) from an innovation perspective, because they result in companies investing less in R&D; or b.) because they create internal pressure to take business decisions which result in unwanted technology transfers, or to greenlight technology transfers outright.

Patent Licensing

Patent licensing is a key part of many companies' business models. The 2021 market for patent licensing was estimated at $48.9bn in the US alone.[69] Typically implemented as busi-

68 Another clear example can be observed in Apple's acquisition of companies (both domestic and international) with the express intention of integrating their technologies within its product line or of making their workforce's technological know-how available to its own project. Apple acquires a new company once every 3-4 weeks. See Sean Hollister, "Apple Buys Companies at the Same Rate You Buy Groceries," The Verge, May 6, 2019, https://www.theverge.com/2019/5/6/18531570/apple-company-purchases-startups-tim-cook-buy-rate.

69 IBISWorld, "Intellectual Property Licencing in the US: Market Size 2002-2027," March 22, 2021, https://www.ibisworld.com/default.aspx.

ness to business (B2B) arrangements, the practice allows a company that has developed a technology to charge 3rd parties to use said technology in their products. The practice is not intrinsically negative, even when applied within the context of sensitive technologies. A company that develops and patents a technology can transfer that technology without losing access to said technology itself, meaning that patent licensing is a form of technology transfer that does not take the form of a zero-sum game. This notwithstanding, the practice has the potential of facilitating the manifestation of several suboptimal scenarios. First, patent licensing potentially provides adversaries with relatively easy access to the technologies encoded in the patent. Adversaries can license the technology outright or, in the case of actors operating in countries that protect them from prosecution for IP infringement, they can simply replicate it based on products that are already in circulation. Second, patent holders find themselves undercut by licensers – a scenario that is particularly thinkable within the context of technologies being licensed by monopolists or by actors which receive state support. Third, the attack surface for accessing and replicating patents increases as they are more widely used. It is not far-fetched to envision a scenario in which a 3rd party can access and replicate a technology by targeting an entity which has licensed a patent rather than the one which developed or owns it. Finally, and perhaps most importantly, the regulation of patent licensing markets allows states to grant or deny access to patents out of strategic considerations. When applied within the context of sensitive technologies, this affords significant leverage to technology holders.

Patent licensing potentially provides adversaries with relatively easy access to the technologies encoded in the patent.

The Purchase of High-Tech Goods and Services

Similar to patent licensing, the acquisition of high-tech goods and services lends itself to the manifestation of negative outcomes because many of the actors which engage in techno-nationalism behave in uncompetitive ways. Once brought to market, products containing sensitive technologies can be procured, replicated, and reintroduced at reduced prices by firms prepared to engage in unfair competition.

Market-based approaches to transferring technology and/or technological know-how pose a unique challenge because, unlike the approaches associated with legislative and forced approach types, they are perpetrated almost exclusively by non-state actors. Though this ultimately does little to change the outcome of these activities, it does blur the line between instances of market-based approaches which are being employed for nefarious (techno-nationalist) purposes and market-based approaches which are being employed without malevolent intent.

This differentiation problem is further exacerbated by the fact that a private sector organization's ability to employ market-based approaches in ways that lend themselves well to transferring technology and/or technological know-how is at least partially a product of policies implemented by their states of origin. China has placed a strong emphasis on building "national champions" within its tech sector, something which has manifested in (among others) significant state funding for said organizations, robust state support for said companies' initiatives to cooperate with foreign corporations or to employ other market-based approaches, and domestic protection against international prosecution. The US, though it is generally less overtly engaged in steering its private sector's actions than is China, has also taken several steps to facilitate the emergence of quasi-monopolistic tech giants. Loose regulations allow corporations to pursue relatively more profitable business models than their European counterparts. Corporate tax burdens are lower and labor groups are less well organized. This has enabled American tech giants to achieve breathtaking scale and to offer lucrative financial incentives to high-skilled workers the world over. Significant investments into (military) R&D – and close support for companies that contribute to it – incentivizes an

aggressive approach to acquiring foreign innovation capacity. Relatively weak support for foreign companies' IP rights provides large American companies with a strong incentive to leverage their monopolistic market positions to exploit foreign business partners.[70]

Whether state policies that enable corporations to behave in uncompetitive and/or techno-nationalist manners – and whether the US' hands-off approach to steering its private sector's actions in this regard rises to the same threat level as does China's – is, ultimately, a political decision. This notwithstanding, recognizing that market-based approaches can be readily understood as constituting a product of state-level policymaking (and of techno-nationalism by extension) is key to putting a framework for mitigating the negative impact of market-based approaches in place.

Market-based approaches to transferring technology and/or technological know-how pose a unique challenge because they are perpetrated almost exclusively by non-state actors - often with their host state's implicit blessing, encouragement, or support.

3.1.1.2 Legislative Approaches to Transferring Technology and/or Technological Know-How

Several states leverage the size of their domestic markets to facilitate the transfer of sensitive technologies. These countries introduce laws or maintain dynamics that require foreign companies to take actions, forfeit rights, or accept risks to access their domestic markets. These can generally be split into three distinct categories; namely: "lose the market" laws, "violate the law" laws, and "no choice" dynamics (Table 7).

Table 7 - Lose the market, violate the law, and no choice dynamics

Law type	Description
"Lose the market" laws (LBTs)	"Lose the market" laws link market access to a series of preconditions. While not always overtly geared towards facilitating the transfer of technologies – see for example laws which require companies to store Chinese consumer data domestically – many combine with other aspects of these countries' regulatory landscapes (ability to defend patents in court, corruption, etc.) to make willingness to accept technology theft a de-facto requirement.
"Violate the law" laws	Unlike "lose the market" laws – which clearly outline conditions that companies must comply with to access a market – "violate the law" laws are laws that are designed to allow for the easy prosecution and sanctioning of companies that refuse to cooperate with efforts at facilitating technology transfers once they are already active within a country's domestic market. "Violate the law" laws are not as structurally ingrained in countries' techno-nationalist strategies as are "lose the market" laws, but offer governments an ad-hoc tool for pressuring foreign companies.
"No choice" dynamics	"No choice" dynamics are dynamics that make it difficult for foreign companies to protect themselves from technology theft within a country's borders. These range from corruption to local courts' tendency not to protect foreign companies' IP rights within a country's borders. These dynamics exacerbate the negative impact of "lose the market" and "violate the law" laws. They can also make for hostile environments in countries where neither of these law types is applicable.

"Lose the market" laws

Of these three categories of laws and dynamics, "lose the market" laws arguably pose the largest challenge to European industry. Formulating and enforcing "lose the market" laws constitutes a significant strategic and logistical undertaking. This means that countries in which "lose the market" laws exist can be understood as being a.) highly competent, and b.)

70 See for example Amazon's replication products which sell well on its platform: Dana Mattioli, "Amazon Scooped Up Data From Its Own Sellers to Launch Competing Products," *Wall Street Journal*, April 24, 2020, sec. Tech, https://www.wsj.com/articles/amazon-scooped-up-data-from-its-own-sellers-to-launch-competing-products-11587650015. See also Johannes Drooghaag's discussion of the US' double standards on IP: Johannes Drooghaag, "US' Double Standards on Intellectual Property," August 10, 2020, https://news.cgtn.com/news/2020-08-10/U-S-double-standards-on-intellectual-property-SPWr9yleqs/index.html.

actors who place significant stock in techno-nationalism as a tenant of national security. The countries in which "lose the market" laws are present are also some of the world's most important economies. Large consumer bases, quickly growing middle classes, access to cheap labor, and the presence of education systems capable of producing high-skilled workers, all contribute to making the accessing of these countries' domestic markets key to securing long-term growth and competitiveness. Taken together, these dynamics limit the scope of viable diplomatic solutions. Given these laws' perceived contributions to national security and the leverage afforded to them by their economic relevance, states which introduce "lose the market" laws have little incentive to do away with them. The interconnected nature of the modern-day international economy, particularly when combined with private sector actors' vested interest in doing business within their borders, undermines the viability of most pressure campaigns that aim to do away with these laws.

The interconnected nature of the modern-day international economy, particularly when combined with private sector actors' vested interest in accessing US, Chinese, and Indian (among others) markets, undermines the viability of most pressure campaigns that aim to do away with "lose the market" laws.

"Lose the market" laws can take several forms, including (but not limited to):[71]

1. Local content requirements, i.e., requirements to purchase domestically manufactured goods or domestically-supplied services, to store consumer data within a country's borders, secure a joint venture (JV) with a local company, or meet corporate structure requirements (CSRs) before being granted market access;
2. Subsidies or other preferences that are only received if producers use local goods, locally owned service providers, or domestically owned or developed IP, or IP that is first registered in that country;
3. Requirements to provide services using local facilities or infrastructure;
4. The outright requirement that a company greenlight the transfer of technology or IP as a precondition for market access;
5. Requirements to comply with country- or region-specific or design-based standards that create unnecessary obstacles to trade, and;
6. Unjustified requirements to conduct or carry out duplicative conformity assessment procedures in-country.

While all these LBTs facilitate the transfer of technology in one way or another, local content requirements have emerged as particularly popular tools for techno-nationalists in recent years. This is partially because they clash less blatantly with World Trade Organization (WTO) rules than do their counterparts, and partially because the states that implement them can, when critiqued for doing so, point towards similar policies implemented by their detractors.[72] Local content requirements have, in recent years, been most prominently employed by China and by India. Lockheed Martin and Boeing – which recently secured contracts to supply India with F-16 fighter jets and with AH-64 Apache attack helicopters respectively – won their bids to do so by agreeing to partner with Tata Advanced Systems to produce key components, such as wings and fuselages.[73] Though Narendra Modi's government has since cast doubt over India's willingness to purchase additional F-16's – opting instead to purchase additional

71 **Several of these LBTs are, on paper, applied by the EU as well. It is important to note that, within the EU context, they are generally not employed with in as blatantly a techno-nationalist manner as they are in, say, China**. See Office of the United States Trade Representative, "Localization Barriers to Trade," n.d., https://ustr.gov/trade-topics/localization-barriers.

72 These arguments are generally made in bad faith. The EU's requirement that European consumer data be stored within its borders – despite mirroring China's own laws – exists for completely different practical reasons. Whereas the EU's version of this law is geared towards protecting European consumer privacy, China's laws are geared – at least partially – towards facilitating domestic surveillance.

73 "Tata, Lockheed Martin to Build F-16 Wings in India," September 4, 2018, https://www.tata.com/newsroom/tata-lockheed-martin-build-f16-wings-in-india.

units of the Indian-made Tejas – Tata's partnerships with Lockheed and Boeing was one of the first examples of the Modi government's "Make in India" initiative being put into action.[74]

China, for its part, has also not shied away from enforcing local content requirements. Apple's concession to the CCP – which saw the company build a data center to store Chinese consumer data in the country in 2016[75] – made international headlines.[76] But, while it highlights the leverage Beijing derives from China's economic value, it is far from the only example of the local content requirements imposed by the country. China also notoriously requires foreign companies to secure JVs with Chinese companies when entering the Chinese market, requires them to establish Chinese subsidiaries, and – through CSRs – places a percentage cap on foreign ownership of Chinese subsidiaries. While this framework does not explicitly facilitate technology transfers, China's economic structure – which all-but ensures that major equity holders are state-affiliated – ensures that it does provide CCP officials with a behind-the-scenes perspective on foreign companies' activities within the country. Chinese investment partners also oftentimes leverage these requirements to secure technology transfers indirectly.[77] Companies seeking entry into the Chinese market often complain that they are played off against one another when negotiating with potential JV partners for entry into the Chinese market. The crux of these negotiations is often that, to secure a business opportunity and to mitigate the risk of said opportunity being awarded to a competitor, these companies must capitulate to technology transfer agreements.[78]

China, for its part, has also not shied away from enforcing local content requirements. Apple's concession to the CCP – which saw the company build a data center to store Chinese consumer data in the country in 2016 – made international headlines.

China and India are not the only two countries to introduce localized content requirements and/or LBTs more generally. Russia, Argentina, and Indonesia have all fielded criticism for the introduction of similar measures in recent years.[79]

"Violate the law" laws

"Violate the law" laws are laws that are designed to allow for the easy prosecution and sanctioning of companies that refuse to cooperate with efforts at facilitating technology transfers once they are already active within a country's domestic market. In most cases, these laws pertain to subjects such as national security, cybersecurity, or environmental protections. These laws make use of ambiguous language. This makes them effective tools for facilitating technology transfers because governments are empowered to bypass the rule of law and to prosecute corporations or mete out punishments as they see fit.

A topical example can be observed in Shell's withdrawal from its Sakhalin Island natural gas project in 2006. In that case, Russian authorities nullified Shell's permit to develop the $20bn Sakhalin-2 energy project citing concerns over the wellbeing of the region's Pacific grey whales. While environmental groups were quick to laud the Kremlin's actions as environmentally focused, the move was widely viewed as being geared towards wresting back control of

74 David Axe, "Maybe India Will Get Its Super F-16, After All," *Forbes*, May 18, 2020, sec. Aerospace & Defense, https://www.forbes.com/sites/davidaxe/2020/05/18/maybe-india-will-get-its-super-f-16-after-all/.

75 "中华人民共和国网络安全法 'Cybersecurity Law of the People's Republic of China,'" November 7, 2016, http://www.gov.cn/xinwen/2016-11/07/content_5129723.htm.

76 Jack Nicas, Raymond Zhong, and Daisuke Wakabayashi, "Censorship, Surveillance and Profits: A Hard Bargain for Apple in China," *The New York Times*, May 17, 2021, sec. Technology, https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html.

77 Alan O Sykes, "The Law and Economics of 'Forced' Technology Transfer and Its Implications for Trade and Investment Policy (and the US–China Trade War)," *Journal of Legal Analysis* 13, no. 1 (January 1, 2021): 127–71, https://doi.org/10.1093/jla/laaa007.

78 See for example Michael Fitzpatrick, "Did China Steal Japan's High-Speed Train?," *Fortune*, April 15, 2013, https://fortune.com/2013/04/15/did-china-steal-japans-high-speed-train/.

79 World Trade Organization, "Local Content Measures Scrutinized by WTO Members in Investment Committee," June 6, 2019, https://www.wto.org/english/news_e/news19_e/trim_06jun19_e.htm.

Russia's natural resources from western oil companies. Gazprom had previously pushed Shell to sell it its 25 percent stake in Sakhalin-2 in exchange for Siberian assets, something which lends credence to the notion that the project's halting on environmental grounds was, at least in part, motivated by geopolitical interests.[80]

A similar dynamic exists in China. Business groups representing companies active within the Chinese market have previously cited concerns that Chinese companies leverage the corporate ties that companies are required to forge with them upon entry to pressure them into giving up trade secrets. This pressure is oftentimes actualized through these companies' close connections with the CCP, and through the CCP's ability to prosecute foreign entities under existing security laws by extension.[81] In 2016, Beijing leveraged consumer protection laws to subject the products sold by Apple and other big foreign companies to scrutiny.

Business groups representing companies active within the Chinese market have previously cited concerns that Chinese companies leverage the corporate ties that companies are required to forge with them upon entry to pressure them into giving up trade secrets.

"No choice" dynamics

"No choice" dynamics make it difficult for foreign companies to protect themselves from prosecution or to defend their IP within a country's borders. Though these dynamics complement "lose the market" laws and "no choice" laws in the countries where they exist by further eroding defendants' legal recourses for dispute settlement, they are nonetheless worth exploring individually. This is first and foremost because "no choice" dynamics pose a threat to the integrity of Dutch and/or EU innovation ecosystems and technological competitiveness. Many countries which do not feature prominent "lose the market" laws or "violate the law" laws do feature "no choice" dynamics.

"No choice" dynamics can be encountered in diffuse forms. In many autocratic countries, they routinely manifest in phenomena such as corruption or in state-controlled courts – both dynamics which undermine foreign actors' ability to seek legal recourse if such a recourse exists on paper in the first place. In others – and in the US most prominently – they take the form of judicial systems in which require defendants to devote significant funds to mount a defense. This system is significantly easier for large companies to navigate than it is for SMEs, meaning that it provides US-based corporations with an incentive structure to engage in shady practices, such as IP theft.[82]

3.1.1.3 Forced Approaches to Transferring Technology and/or Technological Know-How

Forced approaches constitute the final approach type that can be employed to secure technology transfers. These include, but are not limited to, the use of espionage and the leveraging of diaspora.

Espionage has grown in popularity in recent years. "Traditional" forms of the practice have grown to be increasingly supplemented with (or, in some cases, even replaced by) cyber-based initiatives, something which arguably increases espionage's negative impact on Dutch and European technological sovereignty significantly. Espionage can be conducted by both state and nonstate or corporate actors, with both incarnations being of potential relevance to Dutch and/or European technological sovereignty. In the case of state-sponsored espionage, this is because the practice potentially allows for the extraction of technological know-how which would not ordinarily have been accessible through market-based and legislative

80 Terry Macalister, "Environmentalists Back Putin over Shell's Energy Permit," the Guardian, September 25, 2006, http://www.theguardian.com/business/2006/sep/25/russia.oilandpetrol.

81 Keith Bradsher, "How China Obtains American Trade Secrets," *The New York Times*, January 15, 2020, sec. Business, https://www.nytimes.com/2020/01/15/business/china-technology-transfer.html.

82 See Drooghaag, "US' Double Standards on Intellectual Property."

approaches to securing technology transfers. State-sponsored espionage typically targets technologies that are either a.) highly classified, or b.) in active development. Because many of the institutions (defense contractors, universities, etc.) which are engaged in the development of these technologies are protected from foreign investments by stringent government regulations and because they are unlikely to actively seek to secure access to foreign consumers, states are generally only able to access these technologies by employing forced approaches.

Recent years have seen an increasing shift towards the concentration of R&D capacity and throughput in public-sector actors. Combined with the fact that many sensitive technologies are dual-use in nature, this makes corporate espionage an increasingly relevant problem to address as far as safeguarding Dutch and European technological sovereignty is concerned. Although the nature of the technologies they work on is oftentimes no less fundamental and/or disruptive than those being developed by military contractors,[83] corporate actors are generally less well-hardened against espionage than are their state-affiliated counterparts. Corporations have wide attack surfaces (both within cyberspace and the real world), and therefore need to be increasingly aware that anyone – from a disgruntled employee to a supplier – can potentially provide competitors or foreign governments with access to trade secrets, client information, financial information, or marketing information.[84] Each of these types of information can be leveraged to inflict significant harm. Client, financial, and marketing information provides competitors with a leg-up, allowing them to quickly respond to marketing campaigns and providing them with the information they need to steal consumers, win bids, and even poach employees. Trade secrets provide perpetrators with insights into products that already exist or which are in development, meaning that gaining access to them results in technology transfer. G4S estimated in 2019 that corporate espionage is costing companies as much as $1.1 trillion annually.[85]

Recent years have seen an increasing shift towards the concentration of R&D capacity and throughput in public-sector actors. Combined with the fact that many sensitive technologies are dual-use in nature, this makes corporate espionage an increasingly relevant problem to address.

A final strategy worth touching on within the context of forced approaches to transferring technology and/or technological know-how is the leveraging of overseas diaspora, and the exploitation of students in particular. This practice is most commonly associated with China, which has actively supported Chinese students' aspirations to pursue studies at Western universities and since the 1970s and – with the introduction of the CCP's "two bases" strategy in the early 2000s – to use their positions in foreign companies to help Beijing stay abreast of technological developments.[86]

3.1.2 Measures That Make for an Uneven Playing Field

The second category of measures to consider within the techno-nationalism space concerns itself with measures designed to make for an uneven playing field. These measures can be implemented through a wide range of instruments, from overt (direct) state support for domestically based companies to protectionist measures and strategic initiatives to leverage

83 An example of a dual use technology is AI which has been trained on facial data. Google has previously applied this technology within the context of commercial products such as (among others) Google Photos and to Pixel phones, but it has also offered them to military contractors. Project Maven – a Pentagon AI project which Google was ultimately forced to walk away from – saw the company apply facial recognition to drone footage. See Adam Frisk, "What Is Project Maven? The Pentagon AI Project Google Employees Want out Of," Global News, April 5, 2018, https://globalnews.ca/news/4125382/google-pentagon-ai-project-maven/.

84 Betsy Atkins, "Learning From Apple's Spying Incidents - How To Protect Your Company From Corporate Espionage," Forbes, February 12, 2019, https://www.forbes.com/sites/betsyatkins/2019/02/12/learning-from-apples-spying-incidents-how-to-protect-your-company-from-corporate-espionage/.

85 Atkins.

86 Remco Zwetsloot, "The US Needs Multilateral Initiatives to Counter Chinese Tech Transfer," *Brookings* (blog), June 11, 2020, https://www.brookings.edu/techstream/the-u-s-needs-multilateral-initiatives-to-counter-chinese-tech-transfer/.

obscure venues – such as international standard-setting bodies – to secure beneficial arrangements (Table 8).

Table 8 - Approach typology; measures that make for an uneven playing field

Approach type	Approach description
Direct	When pursuing direct approaches, governments provide domestic corporations with forms of support that have a direct positive effect on their ability to compete both domestically and internationally. These forms of support include, but are not limited to, financial support (in the form of investments, gifts, subsidies, etc.) and logistical and/or operational support (i.e.: the use of state intelligence agencies to provide companies with a 3rd party's technological know-how).
Indirect	When pursuing indirect approaches, governments provide domestic corporations with forms of support that indirectly improve their ability to compete both domestically and internationally. These generally take the form of protectionist or mercantilist policies intended to reduce foreign companies' ability to compete domestically. In the case of countries that preside over sizeable domestic markets (see for example China, the US, India, and the EU) this also reduces foreign companies' ability to compete internationally.
Standard-setting	The strategic pursuit of long-term initiatives geared towards reducing 3rd countries' structural ability to compete. These include, but are not limited to, leveraging first-mover advantages to introduce beneficial (technical) standards through international standard-setting bodies and investing into initiatives such as the BRI, which aid in fostering long-term dependence.

Achieving some degree of technological sovereignty is at least partially contingent on the emergence of a competitive innovation base.

From a techno-nationalist perspective, the incentives underpinning state efforts to create playing fields that disadvantage their peers center around several principles. First, achieving some degree of technological sovereignty is at least partially contingent on the emergence of a competitive innovation base. Because innovation bases are oftentimes comprised of private-sector actors, this provides states with an incentive to shield domestic industries from competition and to provide them with conditions that are conducive to rapid growth. Second, maximizing the strategic benefit of presiding over a well-developed innovation base means transposing it not only into economic competitiveness, military capacity, and reduced dependence on 3rd states but also into influence abroad. Succeeding at this objective is contingent on 3rd countries' innovation bases being unable to compete with the domestic innovation base, meaning that states have a strong incentive to take steps to not only strengthen their innovative capacities but to degrade those of other states as well.

These measures can take several forms, including the provision of state support for "national champions," the implementation of protectionist policies, or through larger geopolitical initiatives such as China's BRI. Not directly covered within the context of this publication are vertical integration strategies linking the functionality of physical systems to the user opting into a long-term, ongoing relationship with the technology provider. These "mode 5" revenue models are designed to lock users into ecosystems (also commonly referred to as "walled gardens").[87] They undermine competition by introducing friction, with users having to invest time, energy, and having to weather significant disruptions in service quality when switching from one ecosystem to another.[88] Ongoing discussions regarding the right to repair – a concept which has been cited within the context of (among others) Apple's treatment of 3rd party repair shops and software-based built into John Deere's tractors – contribute to similar

87 Dieter Bohn, "Apple Isn't Just a Walled Garden, It's a Carrier," The Verge, June 7, 2021, https://www.theverge.com/2021/6/7/22521476/apple-walled-garden-carrier-app-store-innovation.

88 A quintessential example of this dynamic can be observed in the barriers users face when switching between Apple's iOS to Google's Android operating systems, and vice-versa. The two ecosystems require users (through, among others, their respective app stores) to "buy" into them, with purchases not being transferrable between ecosystems. Both also optimize services to the user by harvesting personal information, allowing for the provision of personalized in-app experiences which are also non-transferrable across ecosystems.

dynamics.[89] "Mode 5" service (revenue) models are not explicitly tackled within this section because they can, by and large, be understood as a byproduct of bad-faith exploitation of open market mechanisms (previously outlined). Their negative impact on competition can be directly and indirectly addressed through several of the policy options outlined in Chapter 4.3, with efforts at establishing robust EU-level antitrust precedents constituting the most obvious path forward.

The prevalence of techno-nationalist sentiments has driven many states to view technological know-how as a vector for securing spheres of influence abroad. Sensitive technologies are difficult to replicate and extremely expensive to procure and integrate into national infrastructures.

3.1.2.1 Direct and Indirect Approaches to Making for an Uneven Playing Field

Many governments opt to provide domestic industries with forms of direct or indirect support which allow them to outperform international competitors. On the direct side, this generally takes the form of financial or operational support. On the indirect, it manifests in a wide range of policies, including currency manipulation, import or export controls, or in the form of tariffs. Many legislative approaches to transferring technology and/or technological know-how arguably have some overlap with indirect approaches in that they reduce foreign companies' ability to compete – see for example "violate the law" and "lose the market" laws.

These policies are almost universally geared towards protecting domestic industry from external competition and (in the case of larger countries) towards reducing foreign companies' ability to compete internationally by hamstringing their access to the domestic market.

3.1.2.2 Standard Setting

The prevalence of techno-nationalist sentiments has driven many states to view technological know-how as a vector for securing spheres of influence abroad. Sensitive technologies are difficult to replicate and extremely expensive to procure and integrate into national infrastructures. Increasingly, they are also vital to ensuring economic welfare and military capacity. States capable of supplying them to their peers hold significant sway not only because they hold the power to cut them off, but also because dependent states have little incentive to switch to a competing state's "flavor" of the same technology. Direct and indirect measures will go a long way towards protecting a country's innovation base from competition and towards bolstering its technological capabilities, but they do little to transpose a well-developed innovation base into high adoption rates (and, by extension, into influence) abroad.

Signs point towards the US and China being increasingly aware of this fact. The countries have both been vocal on issues about Huawei's entry into the EU's 5G infrastructure, a behavior that can be at least partially explained by their association of the transaction with their capability to exert influence over the trading bloc. This competition is likely to intensify in coming years. The US and China both have a vested interest in fostering technological dependencies and, more generally, in locking partners and adversaries alike into tech "ecosystems" which they control. As competition within the technology space begins to take on this characteristic more and more, standard-setting is set to grow in relevance.

Standards prescribe the behavior or characteristics of people or inanimate objects, often in technical terms. CEN CENELAC distinguishes between four major types of standards;[90] namely: fundamental standards, test methods and analysis standards, specification standards, and organization standards. These are outlined in further detail below:

89 "FTC Pledges to Fight Unlawful Right to Repair Restrictions - The Verge," accessed September 8, 2021, https://www.theverge.com/2021/7/21/22587331/right-to-repair-apple-iphone-ftc-lina-khan-open-meeting.

90 "Types of Standards," CEN-CENELEC, 2020, https://www.cencenelec.eu/research/innovation/standard-stypes/Pages/default.aspx.

- **Fundamental standards** concern terminology, conventions, signs, and symbols. These standards do little in the way of standardizing technologies or methodologies but facilitate interoperability of communication. A fundamental standard might encourage corporations working within the transport sector to adhere to a system in which red is associated with danger and green is associated with safety. Equally, it might strive to ensure that all producers of corrosive acids use the same iconography in their packaging.
- **Test methods and analysis standards** strive to create uniformity in measurement types, ensuring (within the EU context) that EU-funded projects yield easily comparable results.
- **Specification standards** define the characteristics of a product (product standards) or service (service standards). They also define performance thresholds such as fitness for use, interface and interoperability, health and safety, environmental protection, etc. USB-C, a port found on many consumer electronics, is an example of a specification standard that has enjoyed widespread adoption in recent years. In the case of USB-C, the standard dictates the port size and composition, allowing manufacturers to produce cables and peripherals which can utilize it to interface with 3rd devices.
- **Organization standards** describe the functions and relationships of a company, as well as elements such as quality management and assurance, maintenance, value analysis, logistics, project or system management, production management, etc. Organization standards regulate intra and inter-organizational behaviors and practices, meaning that they play a role in (among others) the protection of workers' rights.

Standards create predictability, reduce barriers to interoperability, and level the playing field between actors affected by them - but they also create long-term lock-in.

Standards differ from government regulations in several ways. Perhaps most importantly, they tend to be targeted to regulating facets of modern life which are not typically regulated by governments. This has a lot to do with the fact that, unlike government regulations, most standards exist, first and foremost, to produce value to parties that comply with them.[91] Though they generally achieve this by creating predictability, reducing barriers to interoperability, and by leveling the playing field between actors they affect, not all standards necessarily serve the interests of a wide group of stakeholders. In many cases, they are explicitly geared towards locking industries into licensing specific IP rights or technologies – an extremely lucrative dynamic for developer of said patent or technology. For example, Apple's Lightning Connector represents something of a "soft" technical standard. It allows Apple to tightly control which manufacturers can and cannot produce devices that interface with its iPhones and to collect revenues through licensing fees.[92] In this case, Apple's large market share has allowed it to opt out of adopting the USB-C standard and to develop and maintain one of its own, a move that is arguably unfriendly to consumers and to the environment alike.[93]

Once adopted, standards create network externalities capable of producing economic incentives. Once a standard – and a specification standard (hereafter referred to as **technical** standards) in particular – is widely adopted, it becomes sticky. The Qi wireless charging standard, developed by the Wireless Charging Consortium, provides a clear example of this dynamic. The standard describes a form of power transfer in which coils in a charging peripheral transmit power to coils in a battery-powered device, among other things. Because the Qi standard incorporates specific transmitter specifications, devices that do not adhere to the Qi standard are unable to interface with Qi-certified devices. Qi is almost ubiquitous in 2020.

91 Tim Büthe and Walter Mattli, "International Standards and Standard Setting Bodies," in *The Oxford Handbook of Business and Government* (Oxford: Oxford University Press, 2010), 444.

92 Theo Priestley, "Apple Ditching The Headphone Jack Is Less About Music, More About Royalties," Forbes, 2016, https://www.forbes.com/sites/theopriestley/2016/01/11/apple-ditching-the-headphone-jack-is-less-about-music-more-about-royalties/.

93 Cameron Faulkner, "Apple Is Gearing up to Fight the EU over the Lightning Connector," The Verge, January 17, 2020, https://www.theverge.com/2020/1/17/21070848/eu-apple-european-commission-common-charger-lightning-cable-port.

From a consumer perspective, this increases confidence that buying a phone which advertises wireless charging capabilities will work with a previously purchased wireless charger, or vice-versa.[94] The Qi standard also clearly showcases standards' utility as a facilitator for market access. The standard's ubiquity means not only that all consumers are "locked-in" to Qi-enabled devices; it also incentivizes other producers to develop and introduce devices that make use of the standard, reducing the space for a competing technology to emerge.

Once a standard is widely adopted, it becomes sticky. Firms make significant investments into developing facilities capable of manufacturing goods which adhere to it. In many cases , they also suspend R&D into alternative technologies or solutions.

Standard-setting initiatives exist at both the national and international levels and may be spearheaded by public sector actors, private sector actors, or by a combination thereof. The standard's salience is defined by its adoption rate. A standard that fails the adoption test is unlikely to enjoy the benefits of having an ecosystem of enforcement mechanisms develop around it and is therefore unlikely to be sticky or to provide strategic or economic benefits to the parties which supported its development. Technical standards may emerge through several different processes. USB-C and Qi are institutionalized standards that were introduced by the USB Implementor's Forum and Wireless Charging Consortium respectively. Their chances of adoption are enforced by the fact that they were developed by a group of stakeholders which intend on using them, and who have a vested (shared) interest in doing so. By contrast, Apple's Lightning connector – though it shares many specifications and underlying technologies with USB-C – was developed and introduced by Apple individually. It succeeded largely due to Apple's well-established foothold within the global smartphone market.

Both institutional (i.e.: Qi, USB-C) and unilateral (i.e.: Lightning) forms of standard-setting benefit early movers. In the case of institutional standard-setting, early movers (read: actors who have developed sensitive technologies) can shape the contours of the standard-setting process at an early phase due to knowledge asymmetries. In the case of unilateral standard-setting initiatives, actors who preside over sensitive technologies which their peers do not can establish their preferred iteration of said technology as a de-facto standard simply by encouraging their peers to buy into it. The US and China benefit from this dynamic disproportionately. Huawei's attempts at selling EU Member States on 5G can be readily understood as an attempt to lock the EU into China's preferred technical standard for 5G radios. The F-35 is highly dependent on American infrastructure to function and can be similarly understood as a trojan horse for locking European militaries into structural relationships with US arms manufacturers, and with the US by extension.[95] The introduction of "trojan horse" standards are central to regional initiatives such as the BRI, which champions Chinese norms and rules globally.[96]

94 Thuy Ong, "Qi Reigns as the Standard for Wireless Charging after Powermat Joins WPC," The Verge, January 8, 2018, https://www.theverge.com/2018/1/8/16862244/powermat-wireless-power-consortium-qi-charging.

95 Paul Verhagen, Esther Chavannes, and Frank Bekkers, "Flow Security in the Information Age" (The Hague Centre For Strategic Studies, December 7, 2020), https://hcss.nl/report/flow-security-in-the-information-age/.

96 China has explicitly outlined its view that the BRI holds the potential of contributing to its standard setting initiatives. See European Union Chamber of Commerce in China, "The Road Less Travelled: European Involvement in China's Belt and Road Initiative," 2020, 22, https://www.europeanchamber.com.cn/en/publications-belt-and-road-initiative.

- The Netherlands must contend with two different types of innovation mercantilists. **Directly** oriented actors – such as China – take a direct role in facilitating technologies from foreign countries and companies. **Indirectly** oriented actors – such as the US – create conditions (both domestically and internationally) that empower their private sectors to achieve techno-nationalist goals without direct government involvement.

- Techno-nationalists are motivated by two high-level goals. The first is to transfer technology and technological know-how from 3rd countries, partially to ensure they can keep pace with or leapfrog adversaries and partially because it allows them to produce dependencies and to strengthen spheres of influence. The second is to erode foreign countries' competitiveness. Both of these goals infringe on the Netherlands' independence and technological sovereignty.

- Each of these goals can be achieved through a wide range of different tools. In the case of technology transfers, open market-based, legislative, and forced (coercive) approaches are all commonly applied. The erosion of 3rd countries' ability to compete is achieved mostly through unfair forms of (direct or indirect) state aid, with "locking in" strategies – such as standard-setting or the BRI – also being of relevance.

»The Netherlands must contend with a wide (and varied) gamut of techno-nationalist approach types.«

4. Mitigating the Impact of Techno-Nationalism

Reducing techno-nationalist policies' impact on the Dutch innovation ecosystem is contingent, in no small part, on EU-level action.

This Chapter provides an overview of the instruments states have at their disposal for countering the approaches outlined in the previous Chapter. It does so by identifying structural factors which make Europe and the Netherlands vulnerable to techno-nationalist approaches, arguing that – with some exceptions – these will need to be addressed to mitigate techno-nationalism's impact on the internal market's innovation ecosystem. The instruments identified within this Chapter are derived from an in-depth literature review of other countries' responses to relevant (similar) occurrences and dynamics. They serve as the basis of the expert survey which has been conducted as part of the final Chapter, and thus underlie and structure the report's overall policy recommendations.

Many actors have taken concrete steps towards implementing policies geared towards reducing techno-nationalism's negative impact on their current and future access to sensitive technologies. This Chapter draws upon a broad review of existing literature to outline these steps, and to organize and translate them in a way that makes sense within the Dutch and/or European context.

Doing so requires understanding of three variables. First, within what legislative context is the Netherlands operating? A not-insignificant share of the initiatives which might contribute to achieving these policy goals will, due to the EU holding exclusive competences in key policy areas, need to be kickstarted at the EU level. This has a significant impact on the role the Netherlands can play in protecting its innovation ecosystem from techno-nationalism, with the interpretation, implementation, and enforcing of key pieces of existing EU legislation, as well as participation the EU legislative process, arguably superseding the relevance of domestic reforms.

Second, what factors (hereafter referred to as facilitating factors) help to explain – even despite the introduction of instruments such as the EU's newly minted FDI screening mechanism[97] – Dutch and/or EU innovation bases' vulnerability to each of the techno-nationalist approaches outlined in the previous Chapter? Understanding these facilitating factors is key to formulating and expanding on (EU-level) responses to US and Chinese efforts at forcing unwanted technology transfers or at undermining EU industries' ability to compete.

Finally, how have other countries or regions responded to techno-nationalism and to what degree can (and should) these practices be exercised at the EU level? An in-depth literature review shows that responses to techno-nationalism can generally be understood as being **regulatory**, **procurement-based**, **fiscal**, or **diplomatic** in nature, with an expert survey identifying **procurement-based** measures as holding the greatest potential to safeguard EU innovative capacity while preserving key values.

97 "EU Foreign Investment Screening Mechanism Becomes Fully Operational," Text, European Commission, September 10, 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1867.

4.1 Within What Legislative Context is the Netherlands Operating?

Reducing techno-nationalist policies' impact on the Dutch innovation ecosystem is contingent, in no small part, on EU-level action. Charged with maintaining a level playing field within its internal market, the EU has exclusive competences over the *customs union*, *competition rules*, *monetary policy*, and *trade*. This means that the EU alone is able pass laws which impact these areas, with Member States' roles being relegated to enforcement and implementation. The EU has shared competences in several policy areas of potential relevance to countering techno-nationalism, including the *single market*, *employment and social affairs*, *economic, social and territorial cohesion*, *consumer protections*, and *research and space*. This means that Member States can introduce laws independently provided they do not clash with existing EU legislation and the EU has not announced its intention to introduce laws.

The EU has exclusive competences over the customs union, competition rules, monetary policy, and trade. This has a significant impact on the steps the Netherlands can realistically take if it wishes to take a proactive approach to safeguarding its innovation ecosystem.

The division between EU and Member State competences in these key policy areas does not mean that Member States have no say over the policies they are compelled to enforce within their own borders. It also does not mean that Member States are at risk of being left to defend their innovation ecosystems from techno-nationalist approaches without legal recourse necessary for doing so. The EC plays an important role in setting the bloc's legislative agenda, defines its foreign and security policy, and is involved in negotiating the multiannual financial framework (MFF). These processes allow the heads of the EU's 27 Member States to shape EU institutions' responses to techno-nationalism relatively directly. This ensures that Member States need not be hamstrung by a lack of EU action in their efforts to mitigate techno-nationalism's impact on technological sovereignty.

What it *does* mean is that the lens through which the Netherlands needs to look at tackling the threat posed by techno-nationalism differs slightly from the lens through which it might approach other national security problems. The EU's exclusive competences over the *customs union*, *competition rules*, *monetary policy*, and *trade* – all of which are policy areas that are key to addressing the threat posed by techno-nationalism – has a significant impact on the steps the Netherlands can realistically take if it wishes to take a proactive approach to safeguarding its innovation ecosystem. Specifically, it shifts the Netherlands' role in taking a proactive approach from safeguarding its innovation ecosystem away from formulating, passing, and enforcing independent legislation. A proactive approach instead starts to take on the contours of one in which the Netherlands interprets (to whatever degree possible), is quick to implement, and excels at enforcing key pieces of existing EU legislation on the one hand, and actively participates in the EU legislative process on the other. Space exists to make minor modifications to domestic procurement processes (see Chapter 6), but these are unlikely to have the far-reaching impact could be achieved through EU-level reforms.

The EU has been quick to introduce initiatives which address some of its most egregious vulnerabilities. This is likely due, in no small part, to increased policymaker awareness of the threat that US and Chinese activities pose to the trading bloc's technological sovereignty. In response to Beijing acquiring a controlling stake in or taking over several European high-tech firms, an FDI screening mechanism was introduced in the wake of 2016/2017.[98] In an update to the EU Industrial Strategy, the Commission highlighted 137 products in six sectors as risky and in need of diversification. A wide swathe of regulations within the digital space – including

98 "EU Foreign Investment Screening Mechanism Becomes Fully Operational."

(among others) the DSA,[99] the DMA,[100] the Cybersecurity Strategy,[101] and the GDPR[102] – serve to protect EU consumers, to erode the monopolistic market power of US corporations, and to incentivize the emergence and growth of EU-based competitors. The EU's commitment to pursuing these goals is also evident in its renewed push to prosecute American tech giants for antitrust violations under Margrethe Vestager,[103] who is currently serving as Executive Vice President of the European Commission for A Europe Fit for the Digital Age. These are all initiatives that the Netherlands, as a Member State without the competences to introduce domestic legislation of its own, needs to be participating in and contributing to.[104]

The EU has been quick to introduce initiatives which address some of its most egregious vulnerabilities. It has taken steps to erode the monopolistic market power of US corporations and to incentivize the emergence and growth of EU-based competitors.

It is important to note that, in addition to being largely unable to take meaningful action in the absence of EU-level consent, it would not be in the Netherlands' best interest to do so even if it were possible. As showcased in Chapter 2 (Figure 3), the Netherlands – though it hosts a robust innovation ecosystem – is not, and will likely never be, self-sufficient as far as accessing sensitive technologies is concerned. Safeguarding robust EU innovation ecosystem, one which (by and large) succeeds at safeguarding EU-level technological sovereignty and at allowing the Netherlands to meet its technological needs by leveraging the trading bloc's internal market, is in the Dutch national interest.

4.2 Facilitating Factors – What Makes the Netherlands and the EU Vulnerable to Techno-Nationalist Practices?

The open market, legislative, forced, and direct & indirect approaches and standard-setting are all venues or approaches through which states can pursue techno-nationalist agendas. Within the Dutch and EU contexts, the exploitation of these venues is made possible by a set of structural factors that – though the EU has taken extensive action (Chapter 5) – increase the bloc's innovation ecosystem's vulnerability to them. Reducing techno-nationalism's negative impact on Dutch and/or EU security is contingent on the implementation of policies geared towards addressing these facilitating factors.

4.2.1 Market-Based Approaches

The viability of market-based approaches to extracting technological know-how from the EU's internal market can be summarized as being facilitated by three high-level factors; namely: 1.) regulatory lag, 2.) ideological asymmetries, and 3.) exploitative behavior on the part of bad-faith actors.

99 "The Digital Services Act Package."

100 "Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act)."

101 "Cybersecurity Strategy."

102 Regulation (EU) 2016/679 of the European Council of 27 April 2016 on the protection of natural persons with regard to processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

103 Simon van Dorpe, "Google Is Back — under EU Competition Scrutiny," POLITICO, June 22, 2021, https://www.politico.eu/article/google-ads-european-union-competition-scrutiny-margrethe-vestage/.

104 For a full overview of EU-level initiatives, see Chapter 5. For a concrete list of policy recommendations, see Chapter 6.

Within the context of market-based approaches, regulatory lag refers to the notion that regulations applied to the Dutch and/or EU innovation ecosystems fail to correct for the market failures associated with (and brought on by) techno-nationalist behaviors. This can be attributed to the rate at which innovation drives the emergence and transformation of sensitive technologies. Exponential gains in (among others) efficiency and manufacturing capacity have, in the case of many sensitive technologies, unlocked a host of transformative and potentially destabilizing use cases. In the AI and big data spaces, this dynamic came to a head between 2016 and 2020. Widespread attention for the spread of misinformation on platforms such as Facebook and YouTube kickstarted political debates (and drew attention to) algorithms' contribution to the fomentation of political unrest,[105] resulting in the introduction of pieces of legislation such as the GDPR.[106] The regulation arguably came too late, with microcosms of this phenomenon having been perpetrated by social media platforms years prior. In the wake of the COVID-19 pandemic, it is worth noting that a similar dynamic exists within the synthetic biology space. As early as 2011, Dutch researchers succeeded in modifying H5N1 – a disease with a 60 percent mortality rate – into one which could be transmitted through the air.[107] The research, which drew widespread condemnation, was conducted in a highly controlled environment by individuals with years of training. Advancements in the accessibility of gene editing tools mean that, very soon, it could be replicated by any individual with access to the internet.[108] Current regulation has yet to address this challenge in any meaningful way, opening the door to a dilapidating (manmade) pandemic in the not-so-distant future.

As early as 2011, Dutch researchers succeeded in modifying H5N1 – a disease with a 60 percent mortality rate – into one which could be transmitted through the air. In 2020, technologies such as CRISPR have yet to be effectively regulated.

Advances such as these also change the incentives states associate with having access to these technologies. A general lack of policymaker awareness around a.) how sensitive technologies can be used to impact society, and b.) the incentives this creates from a state perspective means that existing regulation often fails to address the most pressing market failures associated with sensitive technologies.

A similar dynamic can be associated with ideological asymmetries. The US and China have each pursued strategies to facilitate the emergence of huge companies within the tech space, something which has allowed them to perpetrate market-based approaches within the EU by leveraging the sheer scale of their private sectors. The EU has generally failed to produce comparable entities. At the macro level, this can be attributed to a combination of regulatory restraints, EU-level fragmentation in procurement and R&D, and differences in fiscal policy. Whereas the US and China view securing access to sensitive technologies as a policy objective, the EU and its Member States do not. Companies such as Google or Huawei drive innovation forward not only through internal R&D; they are also key parts of why US and Chinese universities have more money for cutting-edge research and why the startup ecosystem in those countries is more vibrant. Of course, ideational differences and regulatory lag do not create the market failures that characterize market-based approaches in a vacuum. Perpetrating states cite concepts such as national sovereignty and the invisible hand of the market, problematizing an open discussion of techno-nationalism's negative impact and reducing the space for finding bilateral solutions to the aforementioned market failures.

105 Nilay Patel, "Nick Clegg Doesn't Think Facebook Is Polarizing," The Verge, March 31, 2021, https://www.theverge.com/2021/3/31/22359026/facebook-nick-clegg-newsfeed-medium-decoder.

106 Karen Kornbluh, "Could Europe's New Data Protection Regulation Curb Online Disinformation?," Council on Foreign Relations, February 20, 2018, https://www.cfr.org/blog/could-europes-new-data-protection-regulation-curb-online-disinformation.

107 Steve Connor, "Alarm as Dutch Lab Creates Highly Contagious Killer Flu," The Independent, December 21, 2011, https://www.independent.co.uk/news/science/alarm-dutch-lab-creates-highly-contagious-killer-flu-6279474.html.

108 Sam Harris and Rob Reid, *Special Episode: Engineering the Apocalypse by Rob Reid and Sam Harris*, accessed June 29, 2021, https://www.youtube.com/watch?v=UaRfbJE1qZ4&ab_channel=SamHarris.

4.2.2 Legislative Approaches

Legislative approaches to extracting technological know-how from the EU's internal market are made viable by perverse incentive structures on the one hand, and (similarly to what is the case with market-based approaches) by exploitative behavior on the part of bad-faith actors on the other.

These two factors can, by and large, be understood as being mutually enforcing. "Lose the market" laws, "violate the law" laws, and "no choice" dynamics emerge as a result of calculated policy considerations on the part of legislators, with the motivations underpinning their introduction ultimately being open to interpretation. As showcased through case studies such as China and India, the viability of these approaches correlates at least partially with market size – a reality that the EU has arguably recognized and leveraged as well. Dutch and/or European companies are incentivized to accept the risk associated with entering these markets because securing access to these markets (whether American, Chinese, Indian, or other) is key to securing growth and competitiveness in the short term.

Forced approaches are difficult to mitigate insofar that actors have little agency over whether they are affected by them or not.

The aforementioned mismatch between state-level national security objectives and private sector welfare is also central to the notion that legislative approaches are perpetrated by bad-faith actors. In many countries, these policies are explained away as measures intended to bolster national security. They weaponize concepts such as national sovereignty in bad faith to achieve objectives that conflict with implementing states' obligations to the WTO, preying upon foreign companies' need to secure growth and often drawing false parallels between their domestic policies and those implemented by their detractors.

While it is unclear to what degree these factors can be addressed by changes in public policy or through diplomacy, it is worth exploring whether (and to what degree) national and regional initiatives can contribute to addressing the market failures that facilitate and are brought on by legislative approaches.

4.2.3 Forced Approaches

Forced approaches are difficult to mitigate insofar that actors have little agency over whether they are affected by them or not. This notwithstanding, two factors – namely: 1.) a general lack of awareness, and 2.) exploitative behavior on the part of bad-faith actors – combine to increase the EU internal market's vulnerability to them.

EU Member States' vulnerability to forced approaches can be summarized as stemming, first and foremost, from a lack of awareness of forced approaches, how they are perpetrated, and what their implications are. A large number of SMEs remain largely unaware of the threat that corporate and state-backed espionage poses to their core businesses.[109] Awareness that state intelligence agencies might employ a wide range of coercive measures – from cyberattacks to employee intimidation – to access trade secrets, let alone that they might do so with the explicit intent of disseminating them among domestic partners within the private sector to allow them to outcompete their European counterparts, is lacking among European SMEs.

Even more pronounced is these entities' general inability to implement measures designed to mitigate the impact of these types of espionage. Studies conducted by, among others, Tilburg

109 Bill Priestap and Holden Triplett, "Beyond Economic Espionage," Lawfare, March 3, 2021, https://www.lawfareblog.com/beyond-economic-espionage.

University and the European Commission found that a whopping 20 percent of European businesses suffered breaches from within cyberspace between 2015 and 2017.[110]

Shortcomings in private-sector awareness of SMEs' roles in bolstering the EU's innovation ecosystem and in developing sensitive technologies compound the challenges posed by awareness deficits among policymakers. Unlike what is the case for many military contractors, European regulators do not provide the trading bloc's SMEs with incentives (whether positive or negative) to invest in hardening their organizations against espionage.

Public and private-sector awareness deficits are a boon for states and agencies which perpetrate espionage. Faced with a relatively soft target, their efforts to extract technological know-how are met with little resistance, a dynamic they are all too happy to exploit.

The EU maintains an internal market in which private-sector actors are not driven to compete as fiercely as they are in the US, and not provided with as much state support as they are in China.

4.2.4 Direct & Indirect Approaches

Much as is the case with forced approaches, affected actors have little agency over whether or how they are impacted by direct and indirect approaches. Often, these approaches manifest in policies implemented by bad-faith actors, meaning that they are facilitated (at least in part) by exploitative behaviors. Their viability can also be attributed to ideological asymmetries between the EU and the US and the EU and China.

Much as is also the case with the factors that facilitate forced and legislative approaches, those that facilitate direct & indirect approaches are mutually enforcing. The EU maintains an internal market in which private-sector actors are a.) not driven to compete as fiercely as they are in the US, and b.) not provided with as much state support as they are in China. As outlined in previous Chapters and sections, this contributes to putting European industry at a significant disadvantage. European companies – whether because competition does not incentivize them to "move fast and break things," because they do not have access to the same type of state funding, or otherwise – generally do not grow to the scale of their US and Chinese counterparts. This disadvantages them in everything from being able to acquire innovative startups to holding onto and attracting exceptional employees.

As is also the case with forced approaches, many of the policies that put European companies at a disadvantage are implemented in bad faith and with the explicit intention of undermining competition. This is particularly the case in countries such as (among others) China and India, where tariffs on foreign goods and services mean they face barriers as far as securing domestic market share is concerned.[111]

4.2.5 Standard Setting

Standard setting's viability as a tool for techno-nationalism can be explained almost fully by ideological asymmetries between the EU and China, with the US (arguably) being less of a disruptive factor within this space.

110 European Commission. Directorate General for Internal Market, Industry, Entrepreneurship and SMEs. and PwC., *The Scale and Impact of Industrial Espionage and Theft of Trade Secrets through Cyber.* (LU: Publications Office, 2018), https://data.europa.eu/doi/10.2873/48055.

111 See for example the price of iPhones in India; Ians, "Apple IPhones Get Costly in India after Import Duty Hike," *The Hindu*, March 2, 2020, sec. Gadgets, https://www.thehindu.com/sci-tech/technology/gadgets/apple-iphones-get-costly-in-india-after-import-duty-hike/article30961563.ece.

This asymmetry is observed in differences between the EU and China's approach to the practice. China centralizes its standard-setting process, both domestically and internationally. On the domestic level, the country's standard-setting is highly hierarchical. National standards make up the top rung of China's standard hierarchy. These are followed by sector (industry) standards, local standards, association standards, and (finally) enterprise standards. The high degree of vertical integration means that Beijing enjoys a relatively high degree of autonomy as far as introducing domestic standards is concerned. The country's economic scale, its subsidization of domestic industry, and initiatives such as the BRI mean that these standards also have a leg-up as far as being adopted internationally (whether de-facto or through an organization such as the International Organization for Standardization – ISO) is concerned.

Beijing has made a consecrated push to transform China into a standard setter within the context of its goal to transform the country's economy by 2050, something which has manifested in increased attention for standard-setting within ISO.

The country's standard-setting initiatives also have several other characteristics which potentially afford them an outsized capacity to formulate standards that go on to be widely adopted.[112] China's non-market-driven approach to developing and technologies means it can prioritize the pursuit of its strategic objectives over profitability.[113] This positions it well to introduce international standards. Beijing has made a consecrated push to transform China into a standard setter within the context of its goal to transform the country's economy by 2050, something which (at least in the short term) has manifested in increased attention for standard-setting within ISO.[114] Chinese organizations which participate in standard-setting within the organization differ from competing members in several ways. First and foremost, their participation is incentivized by significantly different factors than that of their competitors. The government's willingness to support and expand Chinese corporations' efforts to access resources abroad, means that they are not incentivized by their wish of protecting their market share, but rather by realizing China's strategic objectives. These factors also combine to ensure that Chinese standard setters have access to disproportionately more information than many of their peers, something which has previously been shown to further an actor's standard-setting capacity within the ISO significantly.

In contrast, the Netherlands and the EU do not engage in any form of centralized standard-setting initiatives. The process is generally spearheaded by consortia of private-sector actors, with regional or international bodies (see CEN-CENELAC or ISO respectively; NEN in the Netherlands) facilitating negotiations and lending credence to the process. Government actors are tangentially included within the process as contributing stakeholders. Technical standards developed within this context may, in some instances, be transposed into national law, but the process is nonetheless a far cry from Beijing's centralized approach to introducing de-facto and institutionalized technical standards.

112 Björn Fägersten and Tim Rühlig, "China's Standard Power and Its Geopolitical Implications for Europe" (Swedish Institute of International Affairs, 2019), 3, https://www.ui.se/globalassets/ui.se-eng/publications/ui-publications/2019/ui-brief-no.-2-2019.pdf.

113 Polina Klossek, Jakob Kullik, and Karl Gerald van den Boogaart, "A Systemic Approach to the Problems of the Rare Earth Market," *Resources Policy* 50 (December 1, 2016): 134, https://doi.org/10.1016/j.resourpol.2016.09.005; Aiping Han, Jianping Ge, and Yalin Lei, "Vertical vs. Horizontal Integration: Game Analysis for the Rare Earth Industrial Integration in China," *Resources Policy* 50 (December 2016): 158, https://doi.org/10.1016/j.resourpol.2016.09.006.

114 Fägersten and Rühlig, "China's Standard Power and Its Geopolitical Implications for Europe," 3.

4.3 Policy Options

Though the facilitating factors outlined in the previous section put the Netherlands – and the EU at large – at a disadvantage as far as defending techno-nationalism is concerned, the trading bloc's continued vulnerability to these approaches is far from inevitable. This section outlines – based on a thorough review of steps taken by other states and/or regional actors – a series of policy options for mitigating techno-nationalism's impact on Dutch and/or European prosperity and security.

CFIUS' mandate was also expanded to explicitly cover sensitive technologies with 2020's Final Regulations Revising Declaration Requirement for Certain Critical Technology Transactions, which applies to transactions involving US businesses that produce, design, test, manufacture, fabricate, or develop one or more sensitive technologies.

Though these are not labeled as such in the text, it is worth noting that these can generally be conceptualized as requiring policymakers to embark on two distinct initiatives. The first is to take steps to reduce the Dutch or EU internal market's vulnerability to techno-nationalist policies geared towards facilitating technology theft and eroding domestic companies' ability to compete internationally. These steps – hereafter referred to as steps intended to **harden Dutch and/or EU innovation ecosystems** – are intended to mitigate techno-nationalist practices' negative impact on Dutch and/or EU security by putting regulatory, procurement-based, and fiscal infrastructures in place. The second – hereafter referred to as measures intended to **deter bad-faith actors** – leverages regulatory, procurement-based, and diplomatic measures to reduce the likelihood that 3rd parties will pursue these practices in the first place.

As previously alluded to, this section clusters policy options by instrument type. **Regulatory**, **procurement-based**, **fiscal**, and **diplomatic** are explored individually, with synergies between the various policy options being touched on throughout the main text and summarized at the end of the Chapter.

It is worth noting that the procurement-based, fiscal, and diplomatic instrument types outlined in this section are not comprehensive. Governments also have access to a wide range of ad-hoc, difficult-to-implement (and even more difficult to scale) options for addressing specific facilitating factors. As an example, one way of improving the European private sector's resilience to espionage which is not touched on in this section, is to offer courses in cybersecurity and counterintelligence. Another is to take concrete steps to increase security services' scrutiny of the day-to-day operations of affected firms.[115] Though undoubtedly of relevance to mitigating techno-nationalism's impact on Dutch and EU security, these measures are not outlined in-depth – mainly because formulating recommendations detailed enough to facilitate their implementation falls without the scope of this research.

4.3.1 Regulatory

Regulatory instruments offer the Netherlands and the EU a wide range of pathways to reducing techno-nationalism's negative impacts on their internal markets, with much of the infrastructure needed for implementing regulatory changes already being present. Changes to Dutch and/or EU regulatory frameworks are key not only to hardening the bloc's innovation ecosystem; they also serve as a limited deterrent. Combined with the value of its internal market, they can potentially be leveraged as a bargaining chip.

Within this context, the first regulatory measure worth touching upon emphasizes the potential utility of adapting and expanding Dutch and/or EU regulatory regimes to treat sensitive

115 Bill Priestap and Holden Triplett, "The Transformation of Business in an Age of Espionage," Lawfare, October 20, 2020, https://www.lawfareblog.com/transformation-business-age-espionage.

technologies similarly to critical infrastructure. Under such a regime, sensitive technologies, patents that utilize them, and the companies involved in developing and manufacturing them would be subject to regulations or to proactive government measures designed to preclude their acquisition by foreign companies and to limit their opportunities to transfer technology to foreign entities through patent licensing or technology sales. Regulatory regimes such as these are uncommon, but they are not unheard of. The US' CFIUS saw its mandate expanded significantly when the Foreign Investment Risk Review Modernization Act (FIRRMA) came into effect in 2018. The law adds several types of transactions to CFIUS' purview; namely: (1) a purchase, lease, or concession by or to a foreign person of real estate located in proximity to sensitive government facilities;[116] (2) "other investments" in certain US businesses that afford a foreign person access to material nonpublic technical information in the possession of the US business, membership on the board of directors, or other decision-making rights, other than through voting of shares;[117] (3) any change in a foreign investor's rights resulting in foreign control of a US business or an "other investment" in certain US businesses;[118] and (4) any other transaction, transfer, agreement, or arrangement designed to circumvent CFIUS jurisdiction.[119] CFIUS' mandate was also expanded to explicitly cover sensitive technologies with 2020's Final Regulations Revising Declaration Requirement for Certain Critical Technology Transactions (CCTT), which applies to transactions involving US businesses that produce, design, test, manufacture, fabricate, or develop one or more sensitive technologies. Importantly, the CCTT requires transacting parties to evaluate not only whether US regulatory authorization is required for international exports, but also whether it is required for transactions between US-based companies, a rule which applies only when the acquiring party has foreign investors holding more than 25 percent of its voting rights.[120] The US, famously, has previously also leveraged infrastructure such as its Entity List and the Bureau of Industry and Service's (BIS') presumption of denial to actively block tech transfers.[121]

While the EU has, for its part, taken steps to block foreign takeovers by working towards improved information sharing between Member States, the bloc's regulatory infrastructures lags far behind CFIUS' sweeping power to block transactions.

While the EU has, for its part, taken steps to block foreign takeovers by (among others) working towards improved information sharing between Member States,[122] the bloc's regulatory infrastructures lags far behind CFIUS' sweeping power to block transactions. It also, unsurprisingly, lags far behind that of China. Beijing met the CCTT's introduction in 2020 with its own Export Control Law, which aims to protect China's national security by regulating the export of sensitive materials and technologies that appear on a control list. It would apply to all companies in China, including foreign-invested ones.[123] Providing a clear indication that Chinese lawmakers perceive regulations such as the Export Control Law as tools for waging international competition and for influence peddling, the official Daily Legend reported

116 "Summary of the Foreign Investment Risk Review Modernization Act of 2018," 2021, https://www.treasury.gov/resource-center/international/Documents/Summary-of-FIRRMA.pdf.

117 "Summary of the Foreign Investment Risk Review Modernization Act of 2018."

118 "Summary of the Foreign Investment Risk Review Modernization Act of 2018."

119 "Summary of the Foreign Investment Risk Review Modernization Act of 2018."

120 US

121 See Angela E. Giancarlo et al., "US Government Restricts Certain Exports to Huawei and Affiliates by Adding It to Entity List While Permitting Temporary Narrow Exceptions | Perspectives & Events | Mayer Brown," Mayer Brown, May 22, 2019, https://www.mayerbrown.com/en/perspectives-events/publications/2019/05/us-government-restricts-certain-exports-to-huawei-and-affiliates-by-adding-it-to-entity-list-while-permitting-temporary-narrow-exceptions. See also Bureau of Industry and Security, "Bureau of Industry and Security (BIS) Amendment to the Export Administration Regulations (EAR)," May 16, 2019, https://www.bis.doc.gov/index.php/all-articles/17-regulations.

122 Éanna Kelly, "Technology Sovereignty: New EU Rules to Block Foreign Takeovers," Science|Business, October 13, 2013, https://sciencebusiness.net/technology-strategy-board/news/technology-sovereignty-new-eu-rules-block-foreign-takeovers.

123 Bloomberg News, "China Set to Pass Law Protecting Vital Tech From US," *Bloomberg*, October 15, 2020, https://www.bloomberg.com/news/articles/2020-10-15/china-moves-to-shield-its-own-advanced-tech-in-fight-with-u-s.

that legislators had pondered adding source codes, algorithms, and technical documents as controlled items. It also reported that policymakers discussed whether China should restrict the export of technologies on which Beijing has a competitive edge – such as 5G and quantum communications.[124]

Proactive, stringent, and comprehensive regulatory regimes are not the only regulatory tools available to governments looking to reduce foreign actors' freedom to engage in techno-nationalism. More conservative options, such as limiting what share of a company's stock can be controlled by foreign individuals would constitute a welcome first step in this regard.

It is worth noting that proactive, stringent, and comprehensive regulatory regimes – potentially competition-stifling as they are – are not the only regulatory tools available to governments looking to reduce foreign actors' freedom to engage in techno-nationalism. More conservative options, such as limiting what share of a company's stock can be controlled by foreign individuals would constitute a welcome first step in this regard. CFIUS' definition of what constitutes a sensitive technology; namely: any technology that is "essential for maintaining or increasing the technological advantage over countries of special concern with respect to national defense, intelligence, or other areas of national security, or gaining such an advantage over such countries in areas where such an advantage may not currently exist"[125] may offer a useful guideline for Dutch and/or EU policymakers looking to implement such policies, if only because it highlights the legal framework applied within the US context.

Another (arguably less heavy-handed) option for expanding EU-level regulatory regimes is to actively pursue the setting of new antitrust precedents. While unlikely to go a long way as far as addressing the problems of technology transfers through patent licensing and the purchase of goods and services are concerned, establishing antitrust precedents offers several benefits. First and foremost, it offers a pathway to establishing regulatory norms, rules, and best practices without the need for consensus building at the Member State and EU levels. Antitrust cases can be tried and can establish precedents under existing European laws, meaning that any precedents which may (or may not) emerge through this process are unlikely to carry significant political stigma. They also have the benefit of having some efficacy as far as deterring bad-faith corporate actors is concerned. Whereas updates to Dutch and/or EU-level regulatory rules and procedures will go a long way to improving regulators' ability to respond to bad behaviors, they will do little to deter the actors which perpetrate them. Under Margrethe Vestager, the European Commission has sought to introduce antitrust cases against the likes of Google and Apple, though the focus of these cases has (up-till now) been on how these companies manage their platforms rather than on their acquisition of European startups.

4.3.2 Procurement-Based

The value at stake in public sector procurement is massive, with public-sector organizations around the world purchasing more than $9.5tn of goods and services annually.[126] EU Member States spend more than €1.9tn annually, a value that amounts to approximately 14 percent of the trading bloc's GDP.[127] Though the majority of these investments cannot be directly linked to sensitive technologies, the strategic management of these kinds of expenditures provides the Netherlands (and the EU more generally) with an effective carrot for modifying

124 " _ ," October 15, 2020, http://www.npc.gov.cn/npc/c30834/202010/0998a6a07d6e44b9be1d2ca48335f493.shtml.

125 Suire Parron Boggs, "Proposed CFIUS Law WIll Impose New Export Controls on US Businesses," 2018, https://www.squirepattonboggs.com/~/media/files/insights/publications/2018/02/proposed-cfius-law-will-impose-new-export-controls-on-businesses/29559--proposed-cfius-law--new-us-export-controls-client-alert.pdf.

126 Terra Allas et al., "How Smarter Purchasing Can Improve Public-Sector Performance" (McKinsey, March 29, 2018), https://www.mckinsey.com/industries/public-and-social-sector/our-insights/how-smarter-purchasing-can-improve-public-sector-performance#.

127 Allas et al.

the behavior of states and non-state actors alike. This potentially makes them an effective tool for addressing awareness deficits and perverse incentive structures in private-sector actors. Because a large share of EU procurement funding goes to foreign companies – some estimates put the bloc's foreign procurement spending at as high as €50bn – it also makes them a potentially useful tool for mitigating the impact of exploitative behaviors propagated by bad-faith actors.[128]

A large share of EU procurement funding (± €50bn) goes to foreign companies. This may make procurement-based policies a useful tool for mitigating the impact of exploitative behaviors propagated by bad-faith actors.

Procurement-based initiatives can contribute to addressing awareness deficits and perverse incentive structures in several ways. Tendering processes can be used to incentivize tendering parties to meet a predefined set of conditions. Within the context of mitigating the impact of techno-nationalism, this creates several avenues worth exploring; namely: 1.) the use of tendering processes to improve the quality (and awareness) of security protocols within the European innovation ecosystem, and 2.) the use of tendering processes to disincentivize EU companies from selling sensitive technologies to foreign actors. Given the fact that both practices are commonplace within military procurement, there is reason to believe that these types of measures hold some potential. Including requirements pertaining to a firm's cybersecurity practices constitutes particularly low-hanging fruit, especially considering the relatively low cost (and, by extension, popularity) of engaging in cyber-based espionage. The use of tendering processes to disincentivize EU companies from selling sensitive technologies to foreign actors is likely to be a harder sell. Requirements such as these work well within the context of military procurement because the funding made available through such contracts is significant (and reliable) enough to offset the increased operating costs they incur. However, they may create adverse effects if applied within the context of wider sensitive technology-related procurement and/or R&D funding initiatives. Specifically, they may result in many SMEs choosing to participate in tendering processes, something which would constrain their access to public funding, and their capacity to invest in R&D activities by extension.

Procurement-based initiatives' utility within the context of mitigating the impact of exploitative behaviors propagated by bad-faith actors centers almost entirely around the fact that foreign companies participate in and benefit from EU procurement funding. As an example, the EU's Horizon 2020 research program, which was at least partially geared towards facilitating research into sensitive technologies, actively encouraged US and Chinese participation, with several calls and topics having been specifically targeted towards Chinese enterprises.[129] Procurement processes such as these offer would-be competitors' access to EU funding and research networks. They also offer EU Member States access to information about sensitive technologies which domestic industries do not have a competitive advantage in. While this makes them mutually beneficial to a certain degree, foreign actors arguably receive the better deal. EU procurement agencies could feasibly threaten to preclude techno-nationalist countries from participating in research programs. They could also introduce behavioral requirements intended to punish actors (state and non-state alike) which engage in techno-nationalist practices.

128 Lucian Cernat and Zornitsa Kutlina-Dimitrova, "How Open Is the European Union to US Firms and Beyond?," *CEPS Policy Insights*, March 2020, 10.

129 European Commission, "List of Calls Targeting China in Horizon 2020 Work Programme for 2014 and 2015," 2021, https://ec.europa.eu/programmes/horizon2020/sites/default/files/List%20of%20calls%20targeting%20China%20in%20Horizon%202020%20work%20programme%20for%202014%20and%202015_2.pdf.

4.3.3 Fiscal Policy

Another effective and commonly applied tool within most state's toolkits is the use of fiscal and monetary policies. Depending on how aggressively (and within which sectors) they are applied, these policies amount to direct & indirect approaches, meaning that they are intended to bolster domestic industry by insulating it from international competition. Within the European context, their introduction would likely see them mimic the common agricultural policy (CAP) in structure, with subsidies being provided to organizations involved in the development of sensitive technologies and tariff barriers being introduced to reduce foreign industries' ability to compete with domestic producers. The implementation of such a policy would likely be contingent on the successful EU-level formulation of a European equivalent of the US' control list, which features a clear definition of what constitutes a sensitive technology.

Within the European context, the introduction of fiscal policies would likely mimic the common agricultural policy in structure, with subsidies being provided to organizations involved in the development of sensitive technologies and tariff barriers being introduced to reduce foreign industries' ability to compete with domestic producers.

Fiscal & monetary policies have received in-depth coverage throughout this report's previous sections, and are, therefore not covered in-depth here. It is important to note that the kinds of fiscal policies implemented by 3rd countries are (by and large) not compatible with the EU's norms, values, or with WTO rules. It is nonetheless thinkable for the Netherlands to implement them through the oft-cited reciprocity principle, something which has allowed for the implementation of similarly targeted policies in the past.

4.3.4 Diplomatic

Diplomacy, whether by bilateral or multilateral means, offers the Netherlands and the EU another pathway to mitigating the impact of techno-nationalism. The introduction of sanctions, the forging of new bilateral partnerships such as the US and EU's proposed tech alliance,[130] the introduction of new (international) behavioral norms, and the formulation of binding international agreements within the techno-nationalist space. Diplomatic instruments have the potential of helping to address exploitative behavior and of reducing the space for bad-faith actors, though their efficacy is likely to be defined by the specific contours of eventual agreements and (in the case of sanctions) on the circumstances under which they are implemented (messaging, targeted entities, sanction weight, etc.).

4.4 Relevance and Potential Impact

This section provides a high-level overview of results derived from a survey which sought to identify the **feasibility** and **potential impact** of the policy options outlined in the previous section. The goal of this survey is twofold. First, by asking experts to assign policy options scores for **feasibility** and **potential impact**, it sets out to provide the reader with a high-level overview of how the policy options outlined in the previous section compare to one-another from an expert perspective. Second, it sets out – by inviting experts to provide in-depth feedback – to identify a series of high-level policy objectives, with the intention being the facilitation of a seamless clustering of policy recommendations in the following Chapters. They (Figure 4) represent the opinions of 27 European experts working on issues pertaining to economic security, national security, and technological sovereignty (Box 3).

130 Mark Scott and Jacopo Barigazzi, "US and Europe to Forge Tech Alliance amid China's Rise," *POLITICO*, June 9, 2021, https://www.politico.eu/article/eu-us-trade-tech-council-joe-biden-china/.

Box 3 – Methodological overview, feasibility and potential impact survey

The survey was conducted in accordance with the methodology outlined in Annex V: Expert Survey – Feasibility and Potential Impact. The eight (8) policy options tested for **feasibility** and **potential impact** were identified and described in Chapter 4.3. EU added value classifications (high, medium, low) were based on expert responses to the survey's open-form questions. These are intended to capture the degree to which EU-level cooperation (whether in the form of Commission Directives, Member State agreements, or otherwise) are likely to improve on a policy option's impact when compared to a scenario in which it is implemented at the Member State (NL) level exclusively.

EU added value classifications are qualitative, and base themselves on the sentiments experts expressed through open-form questions. They can be understood as follows:

- **Low EU-added value**. Experts either explicitly expressed that the EU has no role in implementing this policy option or made no mention of the EU's added value in their open-form responses.
- **Medium EU-added value**. Experts opinions on whether EU involvement improves the feasibility or potential impact of this policy option were mixed. Experts expressed sentiment which indicated that the feasibility of introducing this policy option at the EU-level was relatively low, but the need for EU-level cooperation was reiterated by several experts.
- **High EU-added value**. Expert responses to open-form questions indicate that the feasibility of implementing this policy at the EU level is high and that the potential impact of doing so is significant. The need for EU cooperation was reiterated by several experts, and concrete examples of initiatives which are already underway were outlined by at least one expert.

Figure 4 also features an "overall reception" metric. This reflects the sum of each policy option's aggregate **feasibility** and **potential impact scores** across respondents. It is included to provide policymakers with an alternative way of understanding the overall **feasibility** and **potential impact** of each policy option.

The survey was sent out to 73 leading experts in Dutch and international industry, academia, and the public sector. Respondents were invited to disseminate the survey to colleagues and/or relevant contacts. The research team collected 27 responses, the results of which are outlined in Figure 4 below.

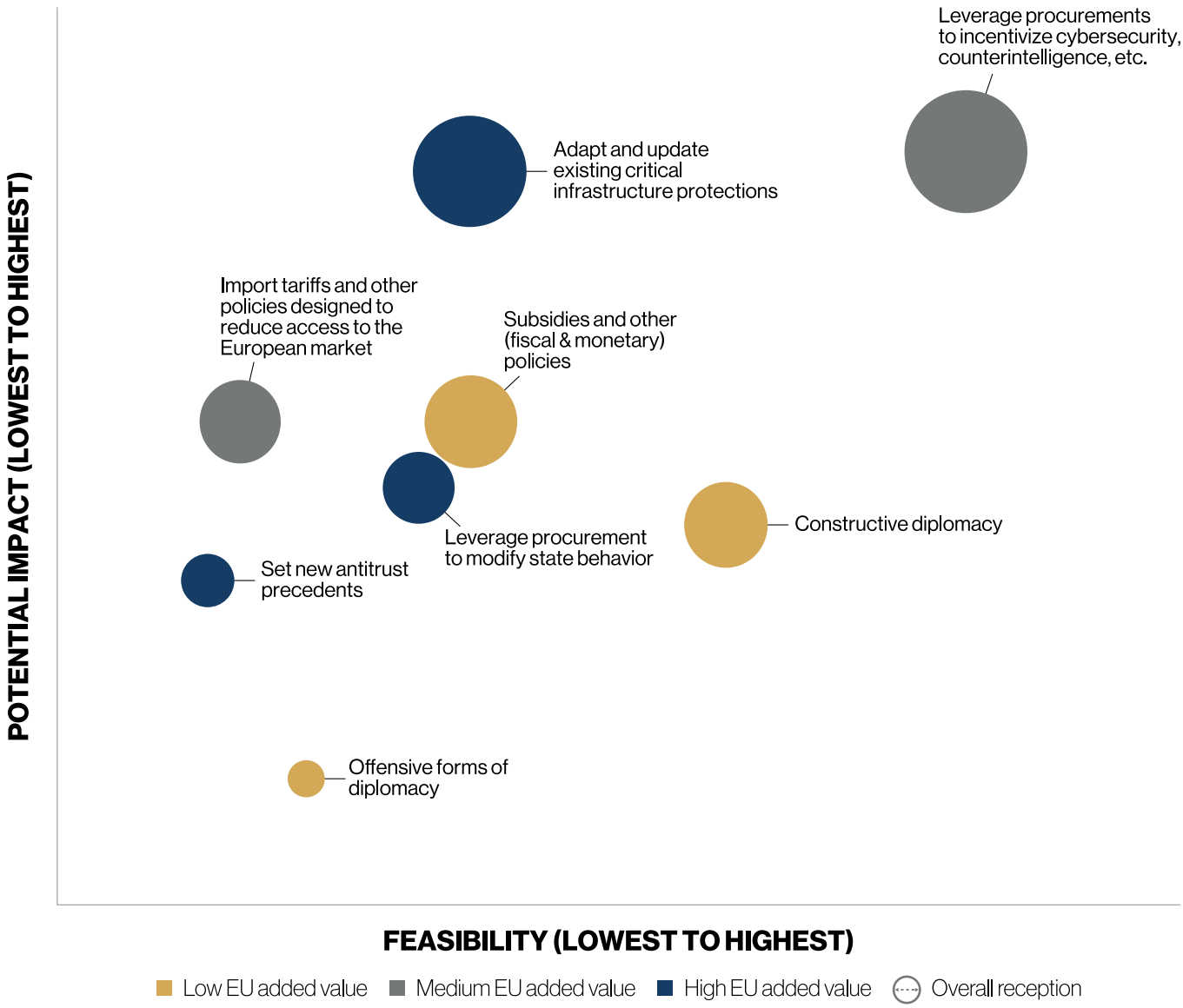

Figure 4 - Survey results, feasibility and potential impact

The adaptation and updating of existing critical infrastructure protections and the conducting of constructive diplomacy are widely perceived as being the next most feasible policy options.

Survey results point to leveraging procurements to incentivize company-level changes to procurement and counterintelligence practices as holding both the highest potential impact and as being the most feasible of all the policy options identified. Experts also perceive the EU as having high added value as far as implementing this policy option is concerned, an appraisal which is only shared with the option of introducing import tariffs, the introduction of other policies designed to reduce access to the European internal market, and with the leveraging of procurement-based instruments to modify state behavior. The leveraging of procurement-based instruments to incentivize company-level changes to procurement and counterintelligence practices scores significantly more positively than the leveraging of these instruments to modify state behavior, something which several experts indicate is because large countries – such as the US or China – preside over enough resources to be able to ignore this form of behavioral conditioning.

The adaptation and updating of existing critical infrastructure protections and the conducting of constructive diplomacy are widely perceived as being the next most feasible policy options, though the former (adaptation of existing infrastructure protections) scores slightly lower on feasibility and the latter (constructive diplomacy) scores relatively lower on potential impact.

Subsidies and other (fiscal and monetary) policies also perform well, though several experts warn that it is imperative that the Netherlands and the EU not respond to techno-nationalism by engaging in a protectionist race to the bottom. The setting of new antitrust precedents and offensive forms of diplomacy receive relatively low scores for similar reasons: experts stress the need for the Netherlands and the EU to leverage their existing policy instruments in ways which are a.) in-line with WTO rules, and b.) do not erode their ability to contribute to norm-setting going forward.

A key takeaway to be derived from experts' in-depth responses to survey questions is that the Netherlands and the EU lag behind their competition in terms of venture capitalism funding.

A key takeaway to be derived from experts' in-depth responses to survey questions is that the Netherlands and the EU lag behind their competition in terms of venture capitalism funding.

An analysis of in-depth expert comments furthermore allows for the identification of two (2) high-level goals; namely: 1.) put safeguards in place to circumvent bad actors' efforts at engaging in techno-nationalism, and 2.) bolster EU firms' global competitiveness. **Regulatory**, **procurement-based**, **fiscal**, and **diplomatic** policy recommendations for achieving these goals are outlined in the following Chapters.

131 Georgios Petropoulos and Guntram B. Wolff, "What Can the EU Do to Keep Its Firms Globally Relevant?," *Bruegel* (blog), February 15, 2019, https://www.bruegel.org/2019/02/what-can-the-eu-do-to-keep-its-firms-globally-relevant/.

132 Isabella Pojuner and Freya Pratty, "The Data: European vs US VCs," Sifted, May 3, 2021, https://sifted.eu/articles/europe-us-vc/.

133 Isabella Pojuner and Freya Pratty, "The Data: European vs US VCs," Sifted, May 3, 2021, https://sifted.eu/articles/europe-us-vc/.

4.5 Key Takeaways

- The Netherlands' (and the EU's by extension) vulnerability to techno-nationalist policies is increased by several structural factors; namely: regulatory lag, ideological asymmetries, exploitative behaviors on the part of bad-faith actors, perverse incentive structures, and awareness deficits. Hardening the Dutch and/or innovation ecosystems against techno-nationalism will mean implementing policies to address these.

- Broadly speaking, the Netherlands and the EU can look towards regulatory, procurement-based, fiscal, and diplomatic instruments as potential tools for addressing the vulnerabilities encoded in the aforementioned structural factors. Regulatory instruments include options such as the expansion of critical infrastructure protections to sensitive technologies, something which would allow Dutch regulators to block many unwanted foreign acquisitions and FDI proactively. Procurement-based instruments are geared towards reducing bad-actors' incentives to engage in techno-nationalism by limiting their access to Dutch and/or EU procurement funding on the one hand, and towards providing legitimate forms of funding and towards incentivizing the strengthening of private-sector security protocols on the other. Fiscal tools would see the Netherlands or the EU step up funding for sensitive technologies, something which approaches the introduction of "soft" protectionist policies. Diplomatic options would see the Netherlands and the EU open dialogues with the likes of the US and China, or lobby for WTO reform.

- Experts identify regulatory and procurement-based options as the highest opportunity instruments to employ, with leverage procurement-based instruments to incentivize cybersecurity and counterintelligence and adapt and update existing critical infrastructure protections being the preferred configurations for these policy instruments' implementation.

- Experts identify two high-level goals for Dutch and EU policy initiatives geared towards addressing techno-nationalism going forward; namely: 1.) providing (EU) industry with the tools and conditions to grow large enough to compete with their US and Chinese counterparts, and 2.) implementing measures designed to reduce the negative impact of techno-nationalist practices intended to facilitate the transfer of technologies or of technological know-how.

5. EU State of Play

This Chapter, which was commissioned by HCSS and developed by the Egmont Institute's Tobias Gehrke, builds upon the previous Chapter by shortly outlining what the EU has done 1.) to implement measures designed to reduce the negative impact of techno-nationalist practices, and 2.) to provide EU industry with the tools and conditions to grow large enough to compete with their US and Chinese counterparts. The Chapter summarizes EU initiatives unfolding in each of these areas and offers reflections on whether current policy goes far enough and/or succeeds at protecting the EU's innovation ecosystem from techno-nationalism.

The Chapter expands on the aforementioned two-pronged taxonomy by including a section which reflects on the EU's efforts as far as unilaterally introducing de-facto rules and standards is concerned. Though these efforts can (depending on reading) be understood as contributing to EU industry's ability to compete, this Chapter explores them individually for two reasons. First, pieces of legislation such as the GDPR diverge significantly from the policies which are "traditionally" implemented to level or circumvent competition (i.e.: tariffs, complex review processes, etc.). They are geared more towards forcing external companies to modify their modus operandi's within the European single market in ways which protect competition than they are towards preventing them from participating altogether. Second, these initiatives are – for all intents and purposes – unique to the EU. The trading bloc is uniquely positioned to introduce and leverage these types of policies within the context of pushing back against techno-nationalism due (in no small part) to its value system and the size of its internal market.

The recommendations outlined in this section should be viewed as recommendations to EU policymakers. Several of them have been integrated into the conclusions and recommendations outlined in Chapter 6, which outlines policy recommendations for the Netherlands specifically.

When Moscow demonstrated Sputnik in 1957, the Soviet innovative breakthrough led to US fears that it was losing its technological superiority.

5.1 European Technological Sovereignty

When Moscow demonstrated Sputnik in 1957, the Soviet innovative breakthrough led to US fears that it was losing its technological superiority. To bridge the perceived gap, consecutive US governments adopted a mission mindset allowing private entrepreneurs and public institutions to transform America's innovation economy.[134] This would spark an innovation panic. The eventual commercialization of breakthrough technologies in electronics, information technology (IT), and computing would cement American tech leadership for years to come.

Around the same time, Chinese dependence on Soviet military technologies fostered concern among its leaders. Mao's 1958 'Two Bombs, One Satellite' project was the first of many tech industrial projects Beijing's political elite would nurture, driven by a set of ideas about the relationship between the state, technology, and national power.

Tobias Gehrke

134 Mariana Mazzucato, *Mission Economy: A Moonshot Guide to Changing Capitalism* (London, 2021).

Ever since, technology has been "a strategic question touching China's very destiny as a great power."[135] The strategic idea of controlling national technological capacity – and the absence of foreign dependence – still prevails today.

Europe was not exempt from these dynamics. The late 1960s saw popular authors and policymakers warn about the grave risks associated with a widening technological gap with the US. "For industrialized countries, it is perhaps on the field of science and technology that their future independence will be decided upon," Jean-Jacques Salomon of the Organization for Economic Co-Operation and Development (OECD) cautioned in 1967.[136] If the tech gap was not closed, leading politicians from British Prime Minister Harold Wilson to German Minister of Finance Franz Josef Strauß urged, European sovereignty would be at risk. Italian foreign Minister Amintore Fanfani even urged NATO allies (read: Washington) to establish a "technological Marshall Plan" to close the gap.[137]

The fear of becoming a taker rather than remaining a maker is taking center stage in Europe. The bloc must "lead the way on digital – or face having to follow the way of others, who are setting these standards for us," President von der Leyen warned in 2019.

More than five decades on, the intimacy between technology and sovereignty is once more gripping the continent. Sensing another imminent technological revolution in the shadow of great power competition, the fear of becoming a taker rather than remaining a maker is taking center stage. Europe must "lead the way on digital – or face having to follow the way of others, who are setting these standards for us," President von der Leyen warned in her 2019 inauguration speech.[138] The EU must "become more digital and digitally sovereign" and address its "dependence on foreign technologies and digital solutions," Madrid and Den Haag urged.[139] Paris and Berlin meanwhile warned in a joint manifesto that "we will only succeed if we are the ones creating, developing and producing new technologies."[140] French President Emmanuel Macron repeatedly warns that "the battle we're fighting is one of sovereignty [...]. If we don't build our own champions in all areas—digital, AI —our choices will be dictated by others."[141]

Technological sovereignty has become the catch-all buzzword across much of the continent to capture both risks and opportunities Europe faces in this "technological war," as Commissioner Breton called it. Under its banner, the EU has been in the business of adjusting its stance in this battle: 1.) better protect its existing tech capacities, 2.) boost its emerging tech capacity and competitiveness, and 3.) leverage its rules and standards. This chapter takes stock of these three clusters of action by identifying which capacities and instruments the EU has been developing, which tech nationalist issues they address, and what actions are still needed.

135 Evan Feigenbaum, *China's Techno-Warriors: National Security and Strategic Competition from the Nuclear to the Information Age* (Stanford: Stanford University Press, 2003).

136 Jean-Jacques Sorel, "Le Retard Technologique de l'Europe," *Esprit (1940-)*, no. 365 (11) (1967): 755–75.

137 Bryce Nelson, "Hornig Committee: Beginning of A Technological Marshall Plan?," *Science* 154, no. 3754 (December 9, 1966): 1307–9, https://doi.org/10.1126/science.154.3754.1307.

138 von der Leyen, "Speech in the European Parliament Plenary Session."

139 "Spain-Netherlands Non-Paper on Strategic Autonomy While Preserving an Open Economy."

140 "A Franco-German Manifesto for a European Industrial Policy Fit for the 21st Century" (Bundesministerium für Wirtschaft und Energie, February 19, 2019), https://www.gouvernement.fr/sites/default/files/locale/piece-jointe/2019/02/1043_-_a_franco-german_manifesto_for_a_european_industrial_policy_fit_for_the_21st_century.pdf

141 Kenneth Propp, "Waving the Flag of Digital Sovereignty," *Atlantic Council* (blog), December 11, 2019, https://www.atlanticcouncil.org/blogs/new-atlanticist/waving-the-flag-of-digital-sovereignty/.

5.2 Protecting Europe's Innovation Ecosystem

5.2.1 Levelling Competition

"We cannot tolerate that EU companies have to give away valuable technology as a price to pay for investing in China," former Commissioner for Trade Cecilia Malmström admonished in 2018, when the EU challenged China at WTO against its practices to force such transfers.[142] The case, which is still under consultation, signaled Brussels' willingness to combat China's systematic and multi-pronged strategy to acquire technologies through legislative and forced approaches. EU businesses have increasingly begun sounding the alarm bells: forced technology transfers and other LBTs (e.g., rules banning certain data transfers across China's borders) place European firms at a growing disadvantage. In response, the EU Commission placed its bets, as it has for three decades, on the WTO: "This is a matter that can and should be solved within the international, multilateral framework," Malmström has stated.

Leveraging international trade rules to ensure fair economic competition with China remains the EU policymakers' preferred method of mitigating the negative impact of its techno-nationalist practices to this day.

Leveraging international trade rules to ensure fair economic competition with China remains the EU policymakers' preferred method of mitigating the negative impact of its techno-nationalist practices to this day. For example, the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) (of which China is a member) imposes disciplines on IP and trade secret protection.[143] China also committed to "eliminate and cease to enforce" measures such as tying market access to technology transfers in its WTO Protocol of Accession.[144]

But clarifying and enforcing these rules has proven challenging, not least because a proper functioning and modern rulebook of the WTO are absent. The bloc will need to put its weight behind the development of new WTO rules and behind the unblocking of its enforcement function. The so-called Trilateral Meeting between US, Japanese, and EU officials is one promising venue to develop new and updated WTO rules and procedures, including on state subsidies and forced technology transfers.[145] On e-commerce, multilateral WTO negotiations are advancing slowly but are still advancing. Finding agreement on these issues with like-minded countries first could strengthen their negotiation leverage when bringing more WTO countries along (including China, eventually).

The WTO, important as it is to the global economy, is of course not the only international institution to expand global rules. Venues such as the OECD, G7/20 or at the United Nations (UN) have demonstrated their importance in the past: new economic security challenges, including on making supply chains more resilient, inevitably require a broad approach which tests different multilateral platforms – though the WTO's broad reach potential for strong enforcement make its reform the most pressing in the short run.

142 "EU Steps up WTO Action against China's Forced Technology Transfers," Trade - European Commission, December 20, 2018, https://trade.ec.europa.eu/doclib/press/index.cfm?id=1963.

143 Trade and Agriculture Directorate, "International Technology Transfer Policies" (OECD, January 14, 2019), https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2018)8/%20FINAL&docLanguage=En.

144 "Accession of the People's Republic of China" (WTO, November 23, 2001), https://www.worldtradelaw.net/misc/ChinaAccessionProtocol.pdf.download#:~:text=Upon%20accession%2C%20China%20shall%20eliminate,conformity%20with%20the%20WTO%20Agreement.

145 "Joint Statement on the Trilateral Meeting of the Trade Ministers of Japan, the United States and the European Union," January 14, 2020, https://trade.ec.europa.eu/doclib/docs/2020/january/tradoc_158567.pdf.

Bilateral tools can also support these goals. For example, the recently concluded EU-Japan Economic Partnership Agreement introduced new provisions to strengthen IP protections and to prohibit forced technology transfers. Though China is not party to this deal, the regulatory power of such large trade areas can co-opt third countries into a regulatory consensus that may enable eventual WTO reforms.

Close coordination with the US is even more important. The newly minted EU-US Trade and Technology Council (TTC),[146] formalized during President Biden's first visit to Europe, is of great importance to many of the issues discussed in this Chapter. One of its most valuable deliverables could include a transatlantic strategy of combating Chinese techno-nationalist practices by committing more diplomatic resources to advance WTO reform and plurilateral agreements. The transatlantic gap remains wide on these issues. But there are hardly better diplomatic venues for finding common ground.

Unfair Chinese practices also need to be addressed with Beijing directly. The EU-China Comprehensive Agreement on Investment tries to move the needle forward in this regard.

Unfair Chinese practices also need to be addressed with Beijing directly. The EU-China Comprehensive Agreement on Investment (CAI),[147] the ratification of which is uncertain as a result of China introducing sanctions on EU parliamentarians and researchers, tries to move the needle forward in this regard. It includes new rules on subsidies, state-owned enterprises (SOEs), financial transaction taxes (FTTs), domestic regulation and transparency, all of which relate to China's unfair trade practices. While CAI's rules, if implemented, are unlikely to provide EU companies with full protection from Beijing's distortive practices, their introduction would allow for the negotiation of a more robust set of rules through venues such as the WTO or the Trilateral Meeting.

Addressing science and research cooperation with Beijing is another critical field of action as far as combatting techno-nationalism is concerned. Chinese know-how transfers through espionage,[148] R&D centers, academic institutions, researchers, and students have grown in prevalence in recent years.[149] In the ongoing negotiation for an EU-China Joint Roadmap for Future Science, Technology and Innovation Cooperation (STI),[150] the EU demands clear commitments on IP protection, access to R&D funds, research data accessibility, and researcher mobility as a condition to continue deep STI engagement. Drawing and sticking to such red lines is critical to facilitating continued mutually beneficial cooperation.

Of course, no single agreement will transform China's complex techno-nationalist structures. For example, even though China's 2019 Foreign Investment Law formally prohibits FTTs as a precondition for investment,[151] "forced technology transfer practices continue to be a systemic problem in China [and] put foreign operators – particularly in high-tech sectors

146 "EU-Japan Economic Partnership Agreement" (European Commission, 2019), https://trade.ec.europa.eu/doclib/docs/2017/july/tradoc_155724.pdf.

147 "EU – China Comprehensive Agreement on Investment (CAI): List of Sections," European Commission, January 22, 2021, https://trade.ec.europa.eu/doclib/press/index.cfm?id=2237.

148 William C. Hannas and Didi Kirsten Tatlow, *China's Quest for Foreign Technology: Beyond Espionage* (Milton Park, Abingdon, Oxon ; New York, NY, 2020).

149 Hannas and Tatlow.

150 "EU-China High Level Dialogue on Research and Innovation," European Commission, January 25, 2021, https://ec.europa.eu/info/news/eu-china-high-level-dialogue-research-and-innovation-2021-jan-25_en.

151 Weihuan Zhou and Huiqin Jiang, "Technology Transfer Under China's Foreign Investment Regime: Does the WTO Provide a Solution?," *Journal of World Trade* 54, no. 3 (June 1, 2020), https://kluwerlawonline.com/journalarticle/Journal+of+World+Trade/54.3/TRAD2020021.

– at risk of losing their competitive advantage."[152] Other informal (indirect) barriers, such as domestic favoritism in public procurement, slow license delivery, or domestic standards inhibiting foreign investor have proven particularly difficult to identify and address.[153]

The EU has, albeit slowly, been drawing the right conclusions. It has increasingly moved to negotiate international rules for fair competition, while also preparing unilateral back-ups to be used as failsafes. For example, the International Procurement Instrument (IPI),[154] recently agreed upon by the Council, will allow the EU to limit or exclude foreign bidders from EU procurement contracts if their home country restricts equal access to EU businesses. Its drafters hope that the threat of EU market closure will increase the bloc's leverage to access the Chinese (and other 3rd countries') market. Should that not materialize, the EU can at least ensure reciprocity – a level playing field.

The EU has been drawing the right conclusions. It has increasingly moved to negotiate international rules for fair competition, while also preparing unilateral back-ups.

The Commission proposal for a Regulation on Foreign Subsidies could also be a critical instrument for ensuring fair competition within the single market.[155] China's national champions are highly insulated within their home market, something which allows them to scale to mega-companies before going global and undercutting EU firms in Europe and elsewhere.[156] Companies like Huawei are reported to have received various forms of state subsidies which gives them unfair advantage over EU competitors when bidding for procurement contracts,[157] acquisitions, and other operations. The regulation would provide the Commission with important powers to referee fair competition in the single market, to the benefit of EU firms.

In STI policy, the EU promises to "more assertively promote a level playing field [...], protect the use of IP rights, ensure the security of supply, and encourage fair innovation ecosystems not distorted by undue rules or foreign subsidies."[158] While the primary channels for achieving these goals remain international rules and institutions and bilateral agreements, the EU has also readied itself to act unilaterally if necessary. Third-country participation in Horizon Europe, the Union's €95bn flagship research program, could in the future be limited to "safeguard the EU's strategic assets, interests, autonomy, or security."[159] While the proposal has yet to be adopted (and while the criteria for exclusion are yet to be formulated), it promises

152 See "Business Confidence Survey 2021," European Chamber, 2021, https://www.europeanchamber.com.cn/en/publications-business-confidence-survey. See also "Report on the Protection and Enforcement of Intellectual Property Rights in Third Countries" (Brussels: European Commission, April 27, 2021), https://trade.ec.europa.eu/doclib/docs/2021/april/tradoc_159553.pdf.

153 Agatha Kratz and Janka Oertel, "Home Advantage: How China's Protected Market Threatens Europe's Economic Power," Policy Brief (Brussels: European Council on Foreign Relations, April 2021), https://ecfr.eu/wp-content/uploads/Home-advantage-How-Chinas-protected-market-threatens-Europes-economic-power.pdf.

154 "Trade: Council Agrees Its Negotiating Mandate on the International Procurement Instrument," European Council, June 2, 2021, https://www.consilium.europa.eu/en/press/press-releases/2021/06/02/trade-council-agrees-its-negotiating-mandate-on-the-international-procurement-instrument/.

155 "Proposal for a Regulation of the European Parliament and of the Council on Foreign Subsidies Distorting the Internal Market" (European Commission, May 5, 2021), https://ec.europa.eu/competition/international/overview/proposal_for_regulation.pdf.

156 Kratz and Oertel, "Home Advantage: How China's Protected Market Threatens Europe's Economic Power."

157 Chuin-Wei Yap, "State Support Helped Fuel Huawei's Global Rise," *Wall Street Journal*, December 25, 2019, sec. Tech, https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736.

158 "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Global Approach to Research and Innovation" (European Commission, May 18, 2021), https://ec.europa.eu/info/sites/default/files/research_and_innovation/strategy_on_research_and_innovation/documents/ec_rtd_com2021-252.pdf.

159 Cristina Gallardo, "Commission Seeks to Block China from Sensitive Joint Science Projects," POLITICO, March 30, 2021, https://www.politico.eu/article/commission-plans-to-limit-research-tie-ups-with-china/.

to offer an important tool for ensuring fair STI cooperation. Horizon's budget earmarked €500mn for joint EU-China research projects during 2016-2020.[160]

To better protect EU companies from IP theft and espionage, the Commission also promised in the 2020 IP Action Plan to more assertively employ "the restrictive measures available to counter private and government-sponsored cyber espionage aimed at acquiring cutting-edge European IP assets."[161] Such countermeasures could follow from the Union's new cyber sanction tool.[162] At the same time, the Commission also began to raise awareness among institutions, governments, universities, research organizations and businesses to prevent, react to, and recover from foreign IP and know how transfer.[163] It will release (non-binding) guidelines to that effect next year.[164]

The EU has also invested into ring-fencing access to and control of certain technologies and strengthening the resilience of its supply chains, infrastructures, and networks.

5.2.2 Protecting the Crown Jewels

While fair competition is one guarantor for EU tech capacities, the EU has also invested into ringfencing access to and control of certain technologies and strengthening the resilience of its supply chains, infrastructures, and networks. This debate was kickstarted by a China's strategic investment spree in 2016/2017, which saw its SOEs (and private companies) acquire controlling stakes in and take over European high-tech firms. Within just 14 months, the EU managed to adopt an investment screening regulation (in force since 2020) with the aim of allowing governments to intervene in FDI they deem too risky.[165]

The regulation was a first compromise. While the Commission has no central powers to block FDI, a minimum threshold for Member States to implement national FDI screening mechanisms was agreed upon, and an information sharing process established. But so far, only 18 capitals have adopted national screening laws,[166] many of which differ significantly in their scope and design.[167] Some, like Germany, the Netherlands, and France, have adopted tech-specific screening targets. Others have been far less specific. Such inconsistencies can weaken the overall protection in the single market.

Another ringfencing tool – export controls – was revived as a blunt American instrument for hamstringing Huawei during the Trump administration. Ringfencing can play a critical role in protecting existing technological advantages and in deterring the illiberal and dangerous use of technologies, but (as the US has demonstrated) its effective application is difficult. Europe's vulnerability to growing export controls helped unlock a year of negotiating a reform of the

160 "EU-China Co-Funding Mechanism," *China Innovation Funding* (blog), accessed August 9, 2021, http://chinainnovationfunding.eu/eu-china-co-funding/.

161 "Making the Most of the EU's Innovative Potential: An Intellectual Property Action Plan to Support the EU's Recovery and Resilience" (European Commission, November 25, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0760&from=EN.

162 "Council Decision (CFSP) 2020/1127 of 30 July 2020 Amending Decision (CFSP) 2019/797 Concerning Restrictive Measures against Cyber-Attacks Threatening the Union or Its Member States," Pub. L. No. 32020D1127, 246 OJ L (2020), http://data.europa.eu/eli/dec/2020/1127/oj/eng.

163 "Concept Note on Tackling Foreign Interference in Higher Education Institutions and Research Organizations" (European Commission, February 2020), https://s3.eu-central-1.amazonaws.com/euobs-media/3ef6dc3d60ee27a2df16f62d47e93fdc.pdf.

164 "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Global Approach to Research and Innovation."

165 "EU Foreign Investment Screening Mechanism Becomes Fully Operational."

166 "List of Screening Mechanisms Notified by Member State" (European Commission, July 14, 2021), https://trade.ec.europa.eu/doclib/docs/2019/june/tradoc_157946.pdf.

167 "EU Framework for FDI Screening" (European Parliament, 2019), https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/614667/EPRS_BRI(2018)614667_EN.pdf.

bloc's own export control regime in 2021.[168] The export of cyber surveillance technologies, which may be used to violate human rights, were particularly concerning the negotiators (especially the European Parliament). While the reformed regime offers novel ways of harmonizing export controls enacted in one member state across the Union, the EU was unable to define Europe technological advantages – its technological frontier – and how export controls can support these, for example.

Indeed, the key question for the EU's protective tech agenda canter around the question: what are Europe's tech crown jewels which may require ringfencing in the first place? 5G telecom infrastructure dominated this question in the past two years, after Huawei's role as a supplier emerged as an international concern. To safeguard its ability to protect the bloc's critical digital infrastructure, the EU agreed to a 5G Toolbox in early 2020.[169] Similar to the investment screening regulation, the Toolbox constitutes a compromise: it formulates minimum common standards, information sharing, and technical support for Member States when they tender suppliers. But varying national interpretations of the Toolbox have resulted in a patchwork of approaches to 5G security, especially as they relate to Huawei.

The Commission has more recently broadened its protective lens to strategic dependencies on others "for things we need the most: critical materials and technologies, food, infrastructure, security and other strategic areas."

Next to digital infrastructures, the Commission has more recently broadened its protective lens to strategic dependencies on others "for things we need the most: critical materials and technologies, food, infrastructure, security and other strategic areas."[170] In an update to the EU Industrial Strategy, the Commission highlighted those goods and supplies as critical which are necessary to develop and innovate technologies enabling the green and digital transition. 137 products in six sectors were identified as risky: raw materials, batteries, active pharmaceutical ingredients, hydrogen, semiconductors, and cloud & edge technologies. Other sectors, including renewables, energy storage, and cybersecurity, are expected to be subjected to similar reviews.[171]

The Commission rightly determines that economic security in these sectors requires a multi-track strategy, one which combines protective measures (e.g., investment screening; stockpiling, export control) with promotive measures (e.g., supply diversification, domestic production). In a first example – critical raw materials – the Commission identified 83 materials necessary to the development of nine strategic technologies, the supply of 30 of which was identified as risky due to concentration or scarcity.[172] The subsequent EU Action Plan on Critical Raw Materials suggests a range of actions to strengthen domestic capacity, trade diversification, international financial support, R&D efforts, and international partnerships.[173] A first Strategic Partnership on Raw Materials was inked with Canada in June.[174]

168 "Commission Welcomes Agreement on the Modernisation of EU Export Controls," European Commission, September 11, 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2045.

169 "Secure 5G Networks: Commission Endorses EU Toolbox and Sets out next Steps," European Commission, January 29, 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_123.

170 "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on A New Industrial Strategy for Europe."

171 "European Industrial Strategy," European Commission, 2021, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-industrial-strategy_en.

172 S. Bobba et al., "Critical Raw Materials for Strategic Technologies and Sectors in the EU—A Foresight Study" (European Comission, 2020), https://rmis.jrc.ec.europa.eu/uploads/CRMs_for_Strategic_Technologies_and_Sectors_in_the_EU_2020.pdf.

173 "Critical Raw Materials Resilience: Charting a Path Towards Greater Security and Sustainability" (European Commission, March 9, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0474&from=EN.

174 "EIT Raw Materials Summit," Text, European Commission, June 17, 2021, https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/eit-raw-materials-summit_en.

Tobias Gehrke

A similar, complementary effort is now developing for sensitive technologies. A first list of 22 sensitive technologies across six industries was identified to "help to decide which technologies are important for technological sovereignty [and] where support from different EU programs and instruments can address such challenges," the Commission notes.[175] To this end, an EU Observatory of Critical Technologies will be established to monitor and analyze sensitive technologies, their potential applications, value chains, needed research and testing infrastructure, desired level of EU control over them, and existing gaps and dependencies for the defense, space and related civil industries. It is unclear how well the Commission is equipped to carry out such assessments, but these efforts present necessary steps in targeting a limit set of sensitive technologies for both protective and promotive measures.

A first list of 22 sensitive technologies across six industries was identified to "help to decide which technologies are important for technological sovereignty [and] where support from different EU programs and instruments can address such challenges."

5.2.3 Policy Recommendations

5.2.3.1 Levelling Competition

1. **Advance WTO reform**. A Trilateral Meeting communiqué from January 2020 detailed the necessary reform to existing WTO rules, especially on subsidies and SOEs. But the agenda has since been dormant. The EU should co-develop a strategy with its close partners how these issues can be introduced at the WTO and how other countries can be brought along. E-commerce and services trade negotiations at the WTO are equally important and require more efforts to create common intersections with partners.
2. **Ratify the CAI and monitor China's implementation**. There are obvious red lines for the EU on ratifying this deal – lines which are currently seriously breached. But if Chinese sanctions were lifted, the EU should be ready to ratify CAI as one building block in advancing a fairer economic environment. Monitoring closely the implementation of China's commitments and quickly disputing shortcoming would need to become a key task.
3. **Continue development of instruments to combat unfair competition**. While the EU has made great progress in advancing its unilateral toolkit, some policies remain to be finalized and adopted. The EU must ensure to quickly get its instruments in place, even if it will not require their use.
4. **Adopt the foreign subsidy regulation**. The regulation would fill an important gap in the EU's competition regime and sharpen the EU's ability to ensure fair competition in the single market which would support EU tech industry competitiveness. The Commission will have to be granted sufficient resources to carry out this work effectively.
5. **Fair competition in third countries**. Ensuring a level playing field outside the single market is significantly more difficult, especially along the BRI and Digital Silk Road where fair competition is undermined. The EU needs to cooperate with like-minded partners through such initiatives as the Blue Dot Network, Build Back Better World, and the EU's own Connectivity Strategy to ensure open standards for infrastructure allow for fair competition.
6. **Aim for an ambitious EU-China STI agreement**. The agreement should allow the EU to set clear limits on STI cooperation, while in turn deepening engagement in those sectors where common interests exist.
7. **Leverage access to Horizon and EDF projects**. The EU should make use of its public procurement participation leverage for strong and enforceable commitments and reciprocity in the STI agreement. But as innovation and technological advances rely ever more

175 "Action Plan on Synergies: Between Civil, Defence and Space Industries" (European Commission, February 22, 2021), https://ec.europa.eu/info/sites/default/files/action_plan_on_synergies_en_1.pdf.

heavily on international collaboration, the EU must ensure that like-minded innovation partners retain full access.

8. **Develop deterrence to techno-nationalist practices**. The EU must develop concrete instruments – such as financial or trade sanctions, freezing of assets, or waiving of IP protections – to deter the transfer of sensitive know how and technologies. This will require developing an "escalation ladder" (common principles of action) for the Union. in the economic and tech space. The effectiveness of these efforts might lend themselves well to coordination within NATO.
9. **Streamline technology across EU foreign policy**. A reference to "Science Diplomacy" in the Global Approach is a good start, but should receive more serious considerations, for example as part of a revamped Global Connectivity Strategy. Ultimately, a comprehensive EU tech strategy will be required.

5.2.3.2 Protecting the Crown Jewels

1. **Refine metrics for sensitive goods and technologies**. The Commission's focus on "strategic dependencies" is a good start and allows to quantify some risks. However, there is still little guidance as to what actions are available, necessary, and proportionate for such goods. Ongoing work on the Critical Tech Observatory should seek to introduce more transparent metrics and methodologies which can action.
2. **Continue EU efforts for harmonized investment screening standards**. The EU screening framework represents only the lowest common denominator with little to no central powers. Deeper integration, moving towards FDI screening uniformity, is necessary, for investment screening of global supply chains is only as strong as its weakest link.
3. **Expand screening to include "economic security"**. Economic security considerations are of growing importance. A reform of the EU screening regulation should consider metrics measuring the competitive effect of foreign investment on strategic technology industries (and thus complement other EU competition tools).
4. **Develop financial counters**. If a foreign investor is barred from acquiring a sensitive company or asset, finding alternative funding is paramount. State banks have on occasion stepped up, but not all Member States can count on deep state coffers for acquisitions worth billions. The EU needs a common financial instrument (e.g., equipping the EIB with an explicit mandate) which can take controlling stakes of sensitive EU assets should no private, non-risky buyers be found.
5. **Continue defensive efforts for 5G infrastructure**. Member State autonomy in implementing the 5G Toolbox guidelines has resulted in substantially different approaches on limiting Huawei's role in national networks. Even after national network security laws are implemented, defensive efforts must continue including by training qualified staff, sharing of R&D in network security, and exchanging best practices with allies (e.g., in NATO).
6. **International coordination at the TTC**. The EU and US (and other close partners) must develop close coordination on issues related to economic security and technology, including developing best practices for export controls, common standards for investment screening, and other controls. The TTC is uniquely positioned to foster transatlantic coordination, though it should be open to other partners (Canada, Japan, South Korea, Taiwan).
7. **A multilateral agenda**. Technology and economic security are national concerns with global implications and spill-over effects. Stressing sovereignty does not have to be averse to working with other governments to establish new ground rules. International coordination even with non-allies, whether at the UN or the G20, is paramount.

5.3 Boosting European Tech Capacity

The second pillar of the EU response to the techno-nationalist challenge has been more offensive: to boost EU tech capacity by preserving and supporting an industrial base and long-term innovation capacity. In other words, Europe needs to ensure it can run at least as fast as its competitors in the innovation and development of sensitive technologies. A renaissance of tech industrial policies – long considered an inefficient tool of government intervention – is emerging across the continent in the service of this goal.

The Commission has been busy with sketching the contours of an EU industrial strategy. In its most recent update, the Commission wants to target climate neutrality, COVID-19 recovery, resilience of critical supply chains, and reduction of foreign dependencies.

A 2019 Franco-German Manifesto on European Industrial Policy made critical inroads on this issue. The Union's sovereignty and independence "will only succeed if we are the ones creating, developing and producing new technologies,"[176] Berlin and Paris cautioned. To stay ahead of the curve, the partners promised to "massively invest in innovation" through high-risk funding instruments, industrial consortia, and deeper capital market integration, among other things. Ambitious tech industrial plans are also booming at the national[177] and regional[178] levels across the continent where governments outline ambitious targets, from digital connectivity, AI, green energy, cloud services, and quantum computing.

In Brussels, the Commission has been busy with sketching the contours of an EU industrial strategy. In its most recent update,[179] the Commission wants it to target climate neutrality, COVID-19 recovery, resilience of critical supply chains, and reduction of foreign dependencies. Among its most important objectives is deeper integration in the single market, but strategic investments in hard and soft infrastructure and R&D are of critical importance too. For example, in the Digital Decade strategy, the Commission estimated a necessary €125bn investment in ICT and skills per year to close the gap with the US and China.[180] While the lion's share of these investments is expected to come from private markets, an increasing consensus is emerging in Europe that targeted public spending can lay a crucial foundation for breakthrough technologies, which can advance the deployment and dispersion of innovation. "There is a need for more favorable conditions supporting the emergence and growth of companies and investments in strategic and R&D intensive sectors of economic and social interest," the Commission argues.[181] It also promises to help collect data about emerging needs (such as critical raw materials)[182] and possible bottlenecks for technological breakthroughs.[183]

But public money is sparse in the EU, which has comparatively few resources or competencies it can leverage (such as tax policy). While the new seven-year budget (MFF) has

176 "A Franco-German Manifesto for a European Industrial Policy Fit for the 21st Century."

177 "Made in Germany: Industrial Strategy 2030," Federal Ministry for Economic Affairs and Energy, 2021, https://www.bmwi.de/Redaktion/EN/Dossier/industrial-strategy-2030.html.

178 "Flanders Future Techfund: Vlaamse regering maakt 75 miljoen euro vrij voor nieuw technologiefonds," Departement EWI, April 1, 2019, https://www.ewi-vlaanderen.be/nieuws/flanders-future-techfund-vlaamse-regering-maakt-75-miljoen-euro-vrij-voor-nieuw.

179 "Updating the 2020 New Industrial Strategy: Building a Stronger Single Market for Europe's Recovery" (European Commission, May 5, 2021), https://ec.europa.eu/info/sites/default/files/communication-industrial-strategy-update-2020_en.pdf.

180 "2030 Digital Compass: The European Way for the Digital Decade" (European Commission, September 2, 2021), https://eur-lex.europa.eu/resource.html?uri=cellar:12e835e2-81af-11eb-9ac9-01aa75ed71a1.0001.02/DOC_1&format=PDF.

181 "Strategic Dependencies and Capacities," Commission staff working documents (Brussels: European Commission, May 5, 2021), https://ec.europa.eu/info/sites/default/files/strategic-dependencies-capacities.pdf.

182 "Critical Raw Materials Resilience: Charting a Path Towards Greater Security and Sustainability."

183 "Strategic Dependencies and Capacities."

significantly increased the heading on research and innovation to about €150bn, many of the Commission's proposals were significantly downsized.[184] For that reason, tech industrial policies remain largely in the hands of Member States. The Commission is trying to tie together national efforts in Important Projects of Common European Interest (IPCEI), a mechanism which grants private-public partnerships in multi-country projects more lax rules on state aid (for subsidies).[185] IPCEI projects so far only include one for microelectronics (since 2018) and one for the battery value chain (since 2019), with the Commission urging Member States to develop more projects and offering prospects for co-financing from the EU budget. Horizon projects seek to support these industrial efforts with R&D partnerships, such as the European Processor Initiative with a budget of €80mn. A new Innovation Fund, funded from the revenues of the EU's Emission Trading System (ETS), looks to make €20bn available this decade for low-carbon technologies, for example.[186]

The Commission is trying to tie together national efforts in Important Projects of Common European Interest, a mechanism which grants private-public partnerships in multi-country projects more lax rules on state aid (for subsidies).

But how the Commission wants to commit public and private investments of "€20bn to €30bn" to a European alliance on microelectronics for example, as Commissioner Breton promised, remains unclear. Despite 22 Member States signing a Declaration on A European Initiative on Processors and semiconductor technologies in which they support the spending of €145bn of the RFF (20 percent digital share) to invest in semiconductor research, design and production capability,[187] public subsidies to microchips under the IPCEI has so far only amounted to €1.7bn.[188] With these sums, Europe will hardly be able to compete with commitments made in Washington (with a $52bn semiconductor fund), Beijing ($170bn spending plans between 2017 and 2024), or even Seoul (pledge of $451bn of public and private investments).

Still, even with a limited budget, the EU has been trying to direct its resources to better address the techno-nationalist challenges. For example, the new Horizon Europe research framework is committing ever more R&D resources to strategic tech areas, such as raw materials, batteries, quantum technologies.[189] Additionally, as part of Horizon Europe, a €10bn strong European Innovation Council (EIC) fund was launched. It provides grants and takes equity in European start-ups in the riskiest R&D and scaleup stages.[190] This is a promising vehicle, but its size and scope remain limited. The short supply of private risk capital (venture funds) severely limits the commercialization of tech in Europe and the EIC has reportedly been unable to support start-ups in finding private investors.[191]

A major push to the EU's tech industrial policy came at the heels of the COVID-19 crisis, when the EU reached agreement on the €672.5bn Recovery and Resilience Facility (RFF), which

184 "2021-2027 Multiannual Financial Framework and New Own Resources: Analysis of the Commission's Proposal," Epthinktank, July 26, 2018, https://epthinktank.eu/2018/07/26/2021-2027-multiannual-financial-framework-and-new-own-resources-analysis-of-the-commissions-proposal/.

185 "State Aid: Commission Invites Stakeholders to Provide Comments on Revised State Aid Rules on Important Projects of Common European Interest," European Commission, February 23, 2021, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_689.

186 "Innovation Fund," European Commission, February 12, 2019, https://ec.europa.eu/clima/policies/innovation-fund_en.

187 "Joint Declaration on Processors and Semiconductor Technologies," European Commission, March 6, 2021, https://digital-strategy.ec.europa.eu/en/library/joint-declaration-processors-and-semiconductor-technologies.

188 Niclas Frederic Poitiers and Pauline Weil, "A New Direction for the European Union's Half-Hearted Semiconductor Strategy" (Brussels: Bruegel Institute, June 2021), https://www.bruegel.org/wp-content/uploads/2021/07/PC-2021-17-semiconductors-.pdf.

189 "Strategic Dependencies and Capacities."

190 "European Innovation Council," European Commission, 2021, https://eic.ec.europa.eu/index_en.

191 Jack Parrock, "'It's Going to Kill Your Business': Startups Turn on €2B EU Fund," POLITICO, January 6, 2021, https://www.politico.eu/article/eu-moonshot-startups-alarm-commission-innovation-fund/.

requires Member States to commit a minimum of 37 percent of their national allocations to climate and 20 percent related to digital.[192] The EU sees this major investment vehicle as a booster to EU strategic tech industries and their vulnerable supply chains. For example, the Commission highlights the semiconductor industry and cloud infrastructure as strategic tech targets for Member States national RFF plans and provides examples of specific national RFF investments.[193] In the Digital Decade, too, the Commission highlights both national and multi-country digital projects it discussed with the Member States under the RRF.[194] Whether and to what extent Member States will follow these strategic guidelines of the EU remains to be seen.[195] An early study on member state pledges found that many of the identified investment gaps in the Digital Decade are not sufficiently met in the national plans.[196]

A self-confident tech industrial policy is undeniably emerging in the EU. Making strategic investments in the development of sensitive technologies and vulnerable parts of supply chains has become key tool in the EU toolbox to boost its tech capacity.

But money is not the only issue. Maybe the EU's most ambitious project – to double its share in global semiconductor production by 2030 – is also its most controversial. In face of acute supply crunches, heavy-handed government interventions, and Taiwan's precarious role as the global manufacturing power have made semiconductors the most coveted tech industry globally. Commissioner Breton's posterchild industrial policy project is to ensure EU supply security in semiconductors. But the focus on bringing advanced semiconductor manufacturing (<7nm) to Europe – a highly advanced section of the semiconductor value chain which relies on eyewatering amounts of public subsidies[197] – is a questionable endeavor given European industry's limited demand for such advanced chips. Experts have urged to aim for those subsectors in the semiconductor value chain where Europe already has strong industry players (e.g., manufacturing equipment), while expanding research funding to upstream parts of the value-chain such as design.[198]

A self-confident tech industrial policy is undeniably emerging in the EU. Making strategic investments in the development of sensitive technologies and vulnerable parts of supply chains has become key tool in the EU toolbox to boost its tech capacity. However, while much of the debate focuses on large public investments (an area where the EU will continue to have less clout), EU tech industrial policy is a vast area of action. Attracting and retaining the talent and skills required to boost its capacity is one such field. In AI, for example, one study found that the EU has a good talent pool, more AI researchers than the US or China, and typically produces the most research as well.[199] However, "there is a disconnect between the amount of AI talent in the EU and its commercial AI adoption and funding," the report finds.

192 "Recovery and Resilience Facility," European Commission - European Commission, 2021, https://ec.europa.eu/info/business-economy-euro/recovery-coronavirus/recovery-and-resilience-facility_en.

193 "Recovery and Resilience Plans: Example of Component of Reforms and Investments - Digital Components and Cloud Capabilities" (European Commission, 2021), https://ec.europa.eu/info/sites/default/files/examples_of_component_of_reforms_and_investment_scale_up_en.pdf.

194 "2030 Digital Compass: The European Way for the Digital Decade."

195 16 Member States have received the greenlight for their national recovery and resilience plans. See "Recovery and Resilience Facility."

196 "The Contribution of National Recovery and Resilience Plans to Achieving Europe's Digital Decade Ambition," Deloitte LLP Report (Deloitte, June 21, 2021), https://www.vodafone.com/sites/default/files/2021-06/deloitte-llp-europe-digital-decade-rrf-gap-analysis.pdf.

197 Antonio Varas et al., "Government Incentives and US Competitiveness in Semiconductor Manufacturing" (Boston Consulting Group, August 2020), https://web-assets.bcg.com/27/cf/9fa28eeb43649e-f8674fe764726d/bcg-government-incentives-and-us-competitiveness-in-semiconductor-manufacturing-sep-2020.pdf.

198 Jan-Peter Kleinhans, "The Lack of Semiconductor Manufacturing in Europe," Stiftung Neue Verantwortung, April 6, 2021, https://www.stiftung-nv.de/de/publikation/lack-semiconductor-manufacturing-europe.

199 Daniel Castro, Micheal McLaughlin, and Eline Chivot, "Who Is Winning the AI Race: China, the EU or the United States" (Brussels: Center for Data Innovation, 2019), https://s3.amazonaws.com/www2.datainnovation.org/2019-china-eu-us-ai.pdf.

The EU Commission has noted the global race to attract tech talent: "there is a strong need to strengthen the IT profession and radically re-think education and skilling of students and professionals," a report for the Commission declares.[200] However, while various initiatives exist on the national and regional level to attract tech entrepreneurs and researchers,[201] the EU's ambition to harmonize education, training and migration policies in the service of attracting and retaining talent is complicated by its lack of competencies in these fields.

Other obstacles for small European firms and start-ups to scale up are 27 different tax codes, 27 different social security and employment systems, data inaccessibility, and the underdevelopment of EU capital markets to provide private funding. However, these lie more in the traditional area of single market regulation discussed partly in the next section.

The EU Commission has noted the global race to attract tech talent: "there is a strong need to strengthen the IT profession and radically re-think education and skilling of students and professionals."

5.3.1 Policy Recommendations

1. **Own financial resources**. Without its own serious financial resources, EU tech industrial policy will remain largely dependent on Member States funds, which are less likely to subordinate their national interests to those of the whole EU. This dilemma risks another failure for EU tech industrial policy. Only if the RFF is succeeded by a common finance instrument which can support tech industrial projects by sharing costs and benefits equally can EU tech industrial policy succeed.
2. **Clear lists with targets**. While a narrower list of "critical assets/technologies" is slowly emerging, a clear methodology remains far from obvious. This opens the door to industry lobbyists and dominant firms seeking preferential treatment. Public finance must be provided to all firms in a strategic sector equally and tech industrial policy goals require clear performance targets to be met (or else become political projects).
3. **Mainstream R&D funding**. R&D is critical in determining who develops, defines, and shapes sensitive technologies. While EU R&D ranks highly across the board, more efforts need to be made to focus research on bottleneck technologies and sub-sectors in critical value chains in which Europe may face threat of disruption (e.g., semiconductor design). The EU must create direct linkages following form innovation goals between its different instruments.
4. **Enlist procurement instruments**. Procurement contracts can be critical for tech companies on their path to commercialization. To be able to support its most sensitive technologies, the EU needs a strong procurement instrument – or be able to coordinate national procurement instruments – to leverage scale-up of tech start-ups, for example those firms which received EIC funds.
5. **Move ahead on the European Future Fund**. Before the COVID-19 pandemic, the Commission drafted plans for a €100bn sovereign wealth fund to invest (long-term equity) in strategic industries. Such firepower is critical to allow for more private finance to crowd in. The EU should expediate its efforts to make proposals for such a fund.
6. **A European Tech Visa**. Attracting and retaining tech talent is essential. Some ideas practiced in Member States are promising to scale to the EU level, such as helping founders, employees, investors, and researchers in sensitive tech areas inpatriate more easily with the help of a tech visa valid across the single market.

Tobias Gehrke

200 "Increasing EU's Talent Pool and Promoting the Highest Quality Standards in Support of Digital Transformation" (Brussels: European Commission, 2019), https://skills4industry.eu/sites/default/files/2019-06/Brochure_Digiframe_final20190617.pdf.

201 "What Is the Best Startup Visa Scheme in Europe?," EuroStart Enterprises, April 6, 2021, https://www.eurostartentreprises.com/en/business-advice/what-is-the-best-startup-visa-scheme-in-europe.

7. **International tech industrial cooperation**. International partners for tech industrial policy are critical. Opening the IPCEI for 3rd country participation, for example, could help build resilient value chains with like-minded partners. Within the TTC, the EU should aim for EU-US joint ventures across sensitive tech value chains, e.g., semiconductors or hydrogen energy. Financial support for EU participating firms could come from the RRF.
8. **Common R&D efforts**. Solving the most pressing innovation challenges cannot be done in isolation, especially in a time when innovation and technological advances rely ever more heavily on international collaboration. The EU and international partners (e.g., in the TTC) must identify sensitive technology challenges and devise policies which incentivize international R&D cooperation. For example, more sustainable critical mineral mining technologies or even substitution could support supply security, an innovation goal shared with many like-minded countries.

To be less dependent on judicial redress, the EU wants to flex its digital regulatory power once more, this time to protect both consumers and the single market from the effects of severe market power of digital giants.

5.4 Leveraging rules and standards

5.4.1 Regulation

Talk to any EU policymakers about the EU's capacity to set the rules of the digital economy and they are almost sure to point to the GDPR, the Union's data privacy framework which is said to have shaped over 100 similar national laws around the globe. No tech company can ignore the EU's massive and rich consumer market. The Brussels Effect,[202] as Anu Bradford famously coined this global market mechanism, is effectively a unilateral regulation adopted for the single market which becomes adopted by other regulators to save their businesses from having to abide by multiple regulations.

Optimism that the EU can repeat this feat of relying on its regulatory power to shape the techno-nationalist competition in its favor has been a mainstay in the debate. To set the global regulatory gold standard is driven by both a values agenda – the right to privacy and the defense of democratic norms – as much as it is, more recently driven by economic security considerations: ensuring fair competition in face of (primarily American) digital giants, whose massive platforms have often become unavoidable to connect customers with markets (such as through app stores) fashioning them with exorbitant "gatekeeper" powers.[203] Both the Commission and Member States have been launching numerous antitrust investigations into Apple, Amazon, Google, and Facebook, though with often mixed results drawn out over several years.

To be less dependent on judicial redress, the EU wants to flex its digital regulatory power once more, this time to protect both consumers and the single market from the effects of severe market power of digital giants. The DSA and the DMA are a set of extensive regulatory tools through which the EU wants to introduce a new set of competition standards in digital markets – the do's and don'ts for firms – which will ideally spread beyond its borders once more.[204] For example, to become more agile in addressing anti-competitive behavior in fast-moving digital markets, the DMA proposes rules allowing the Commission to constrain certain gatekeeper

202 Anu Bradford, "The Brussels Effect," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 2012), https://papers.ssrn.com/abstract=2770634.

203 Filippo Lancieri and Patricia Sakowski, "Competition in Digital Markets: A Review of Expert Reports," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, January 30, 2021), https://doi.org/10.2139/ssrn.3681322.

204 "The Digital Services Act Package."

platforms before competition infringement occurs (ex-ante), rather than only being able to respond after rules have been infringed (ex-post).[205]

Other major regulatory innovations include interoperability requirements among online platforms which could allow users to choose between platforms more easily and prevent "lock-ins." The regulation could require gatekeepers to improve interoperability and data portability, which the Commission hopes could help competition. Another major component is access to data. The DMA could require gatekeepers to allow consumers and businesses improved access to data collected by the online platform.

Unsurprisingly, the DMA and DSA are highly controversial. The DMA's shift of enforcement from ex-post to ex-ante means certain conditions are imposed on firms without the evidence of a harmful practice. The anticipation of a pre-defined risk could lead to "precautionary intervention." Some experts warn that this change could come at the expense of innovation and entrepreneurial risk taking, ultimately undermining European digital innovation.[206]

The EU is also working on an EU-wide regulatory framework to govern AI in its proposal for an AI Act. It suggests banning specific AI applications, while demanding extensive reporting requirements for "high risk" application.

Additionally, some policymakers have repeatedly singled out American digital companies as the target, rather than committing to standards which capture all anti-competitive behavior equally.[207] Such discriminations are of questionable legality under the WTO services agreement (GATS) and could also draw bilateral trade retaliation from the US under its Section 301 tool.[208] However, the Biden administration nominated vocal critics of US antitrust failures for digital platforms to key government positions[209] – a move which could see a similar shift in US competition policy following in EU footsteps. Advancing common transatlantic standards in digital platform regulation will be key for the EU's success in this field.

The EU is also working on an EU-wide regulatory framework to govern AI in its proposal for an AI Act (AIA). It suggests banning specific AI applications, while demanding extensive reporting requirements for "high risk" application.[210] Similar to the GDPR, the proposal's scope is extraterritorial, meaning it would apply to any provider or user inside or outside the Union who wishes to operate AI systems in the EU. With this rules framework, the EU hopes to push for another regulatory gold standard which would not only support EU values but also help nurture a competitive European AI sector. In combination with the European Data Strategy, which intends to feed EU AI industry with the necessary data by improving access and flow of data within the single market,[211] the critical importance of its regulatory tools for boosting an EU tech industrial policy becomes apparent.

205 "Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act)."

206 "Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act)."

207 Foo Yun Chee, "EU Tech Rules Should Only Target Dominant Companies, EU Lawmaker Says," *Reuters*, June 1, 2021, sec. Technology, https://www.reuters.com/technology/eu-tech-rules-should-only-target-dominant-companies-eu-lawmaker-says-2021-06-01/.

208 "Section 301 of the Trade Act of 1974" (Congressional Research Service, June 16, 2021), https://crsreports.congress.gov/product/pdf/IF/IF11346.

209 Cecilia Kang, "A Leading Critic of Big Tech Will Join the White House," *The New York Times*, March 5, 2021, sec. Technology, https://www.nytimes.com/2021/03/05/technology/tim-wu-white-house.html.

210 "Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts" (European Commission, April 21, 2021), https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206.

211 "European Data Strategy," European Commission, 2021, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en.

A similar logic applies in the regulation of cloud technologies, for which the EU wishes to improve European competitiveness and decrease dependence on US and Chinese vendors (hosting 80 percent of European cloud data). On the one hand, GAIA-X, conceived by Paris and Berlin, aims to develop a cloud ecosystem governed by EU rules and values on data and thus encourage the adoption of cloud solutions among EU firms. It counts over 270 European and non-European members which seek to develop technical specifications which offer interoperability yet sufficient protection. Other national initiatives, such as in France, also exist.

On the other hand, the EU is boosting initiatives which may compete to some degree with GAIA-X and national initiatives. Member States declared to work together towards a European cloud federation initiative which would not only mobilize up to €10bn for the creation of a federated cloud, but also leverage the EU market by setting technical standards and policy norms – an EU Cloud Rulebook – which foster interoperable EU cloud services – and ideally become global norms.[212] Following this declaration, the EU began developing an IPCEI comprising eleven Member States and in July, the Commission announced a European Alliance for Industrial Data, Edge and Cloud to foster the emergence of such technologies in Europe and support the Commission is setting the standards for cloud services.[213]

Whether and how the EU initiative will converge with Member State driven initiatives and GAIA-X on standards remains to be seen. For example, while GAIA-X membership is open to global stakeholders (including dominant US cloud providers), the new Cloud Alliance is restricted to entities legally represented in the EU. An intra-European competition to develop the regulatory framework, standards, and norms around cloud computing could limit its impact internationally and should be avoided.

European history in technical standardization bodies such as the ISO, IEC, ITU, and 3GPP is strong. But China's techno-nationalist gambit in technical standardization risks corrupting the existing cooperative and non-political institutional frameworks which ensure fair competition among private firms.

5.4.2 Technical standards

Related to the regulatory cluster are technical standards which, even though developed and adopted by private firms voluntarily, have become a techno-nationalist playground. Who sets a technical standard has long been relegated to neutral, apolitical platforms. But states rediscovered the power technical standards can have on shaping an emerging sensitive technology. China, first among them, identified technical standards as foundational to its techno-nationalist agenda. Beijing is keen on its own companies setting the global technical standards for sensitive technologies and is expanding serious resources. This risks undermining not only sensitive technologies adherence to EU values and democratic norms but also fair competition for EU tech firms.

European history in technical standardization bodies such as the ISO, IEC, ITU, and 3GPP is strong. But China's techno-nationalist gambit in technical standardization risks corrupting the existing cooperative and non-political institutional framework which provide fair competition among private firms. Especially in sensitive technologies, EU firms have been sounding alarm bells over their decreasing influence in shaping technologies.[214] Not all of that is because of unfair practice of course. But understanding how China influences international technical standardization is a crucial component to finding an adequate response. The yet to be

212 "Towards a next Generation Cloud for Europe," European Commission, 2021, https://digital-strategy.ec.europa.eu/en/news/towards-next-generation-cloud-europe.

213 "Digital Sovereignty: Commission Kick-Starts Alliances for Semiconductors and Industrial Cloud Technologies," European Commission, 2021, https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3733.

214 Daniel Delhaes, Till Hoppe, and Moritz Koch, "Technologie: Wirtschaftskrieg des 21. Jahrhunderts: Wie China den deutschen DIN-Standard verdrängt," Handelsblatt, March 15, 2021, https://www.handelsblatt.com/politik/deutschland/technologie-wirtschaftskrieg-des-21-jahrhunderts-wie-china-den-deutschen-din-standard-verdraengt-/26986456.html.

released China Standards 2035 strategy, for example, is expected to weave together closely China's other techno-nationalist plans such as Made in China 2025 by exercising control over international standards-setting and promoting the integration of its technical standards into bilateral and multilateral cooperation agreements (e.g., along the BRI).

The Commission identified technical standardization as a strategic imperative for its technological sovereignty agenda. For example, the Digital Strategy[215] and the proposal for the AIA both highlight the importance of technical standards. Similarly, the update to the Industrial Strategy stakes out the EU's aim of "leadership in standard-setting." For sensitive technologies such as hydrogen, batteries, offshore wind, safe chemicals, cybersecurity or space data, global leadership in setting standards is "a critical matter for the competitiveness and resilience of EU industries," the Commission emphasizes.

The Commission has identified technical standardization as a strategic imperative for its technological sovereignty agenda. The Digital Strategy and the proposal for the AIA both highlight the importance of technical standards.

How will the EU achieve this goal? In a forthcoming Standardization Strategy, it wants to "develop a more strategic and coordinated approach to global standards-setting in areas of strategic EU interest."[216] How it wants to achieve this – and what compromises it is willing to make – remains unclear. There have been efforts in the past to cooperate more closely with the US on technical standards including during the TTIP negotiations. But the EU and US systems differ significantly and few compromises could be found in the past.

A new window of opportunity has opened, however, following China's challenge to technical standardization and values. The EU has offered the US to cooperate only in those areas where little to no international technical standards exists to date, such as in sensitive technologies. Among the most promising area of the TTC include cooperation on technical standards in sensitive and sensitive technologies. Above all, they should ensure the proper functioning of international standard bodies in which private companies can develop standards based on engineering merit, not geopolitical clout.

5.4.3 Policy Recommendations

1. **Ensure EU digital regulation is not discriminatory**. The DMA and DSA should commit to standards which capture all anti-competitive behavior equally to avoid a trade war. Technology diplomacy must become a staple of EU foreign policy to ensure EU regulation is not perceived as digital protectionism.
2. **Capture "killer acquisitions" in EU competition policy**. "Killer acquisitions", in which incumbent firms acquire innovative targets solely to discontinue the target's innovation projects and pre-empt future competition,[217] are particularly prevalent among digital platforms. These practices pose serious threats to innovation and are hitherto not captured in EU competition policy.
3. **Data accessibility**. The EU must leverage public data, such as health and geospatial data from governments for its private sector. It requires a data policy which accelerates data access and interoperability between Member States governments, researchers, and companies. The forthcoming European Health Data Space is an important step and should be expanded to other critical fields, for example under the European Data Portal.

215 "ICT and Standardisation," European Commission, 2021, https://digital-strategy.ec.europa.eu/en/policies/ict-and-standardisation.

216 "Standardisation Strategy," European Commission, 2021, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13099-Standardisation-strategy_en.

217 Colleen Cunningham, Florian Ederer, and Song Ma, "Killer Acquisitions," *Journal of Political Economy* 129, no. 3 (2021): 649–702.

4. **Ensure international data flows**. International flow of personal data is crucial for Europe's technological agenda. The GDPR facilitation mechanism ("adequacy") has proven stiflingly cumbersome: only 14 countries have been granted this seal, while two EU-US data transfer arrangements were struck down by EU courts. A reform of the GDPR should eventually remedy these shortcomings. But in the short term, more focus and resources must be committed to finding adequacy decisions.
5. **Regulatory cooperation, not unilateral advances**. Digital and tech regulation must come with an international strategy that identifies priorities and partners for regulatory cooperation – a dimension which still too often is a mere afterthought in EU regulation. The TTC could serve as an important platform to explore synergies on platform regulation, tech market power, AI regulation and more. The EU proposal to work on a transatlantic AI agreement, for example, could be a strong first step towards better tech regulatory cooperation.
6. **Align cloud regulation practices**. While the basic objectives of different European cloud initiatives are similar, their specific standards and regulatory aims diverge in many aspects. Ensuring synergies across different projects is key. The EU must ensure to leverage its regulatory power as one entity by setting the highest privacy and security standards.
7. **Technical standards cooperation**. The TTC also includes ambitions chapters on standards cooperation. For example, transatlantic dialogues between cybersecurity regulators (CNECT and NIST) could be expanded to share upcoming regulatory plans for sensitive technologies where cooperation could lead to new technical standards. The Commission could for example include in its standardization requests to CEN/CENELEC/ETSI a clause inviting US standards development organizations.
8. **International standard coordination**. Beyond the TTC, regular dialogue among regulators from allied nations to discuss strategic priorities could help project common priorities into the ISO, IEC and other international bodies, where cooperation in the relevant technical committees could then jointly develop those standards. Such cooperation could for example be placed in context of the Trilateral Meeting with Washington and Tokyo.
9. **Referees don't win**. EU regulatory and standard power is finite and rests on its enabling factors discussed in the previous section: strategic investments, attracting talent and investors, and more R&D funding. Leveraging rules and standards can only work if the EU manages to run faster.

The EU has become an ambitious tech player in its quest for technological sovereignty.

5.5 Conclusion

The EU has become an ambitious tech player in its quest for technological sovereignty. Meeting the geoeconomic challenge of accelerating techno-nationalist practices in Beijing and Washington is not the only reason for the EU's adjusted stance in this tech battle, but it is among the most important drivers.

Brussels' traditional forte in market regulation and its priority for multilateral, diplomatic solutions have since been flanked with more unilateral tools to ensure fair economic competition internationally. At the same time, the definition of strategic tech sectors which are exempted from free market transactions and receive special attention demonstrate the rising concern of economic security in EU policymaking.

While specific policy recommendations for these clusters can be found at the end of this report, in the bigger picture this shift in approach points to a geoeconomic maturity in EU strategy. A protective agenda – building higher fences around smaller gardens – is critical in

a techno-nationalist era. At the same time, boosting EU competitiveness in tech and digital industries is of equal importance – for offense is the best defense.

Pitfalls are almost impossible to navigate: introduce barriers which are too significant and risk starving EU industry of necessary revenues and networks to develop next-gen technologies; do less and risk technology leakage which may equally disadvantage the EU's tech sector. Equally, the EU's offensive play risks both underdelivering necessary resources, while also not sharing costs and benefits equally across the Union.

The EU's offensive play risks both underdelivering necessary resources, while also not sharing costs and benefits equally across the Union.

Ultimately, balancing this equation will require a comprehensive and sound EU technology strategy – one which can tie together the three clusters discussed in this chapter. Whether this big-ticket item is achievable remains doubtful. In the meantime, though, filling the gaps in each policy cluster can still be meaningful steppingstones to better position the EU in the "technological war."

5.6 Key Takeaways

- The EU has taken initial steps towards putting an infrastructure in place for mitigating the negative impact of techno-nationalism, but a lot of hurdles remain. Most important is that key policies are open to interpretation by Member States, with the result being that enforcement is inconsistent in its scale and scope across the block.
- The EU's approaches to the US and China differ significantly. Diplomatic venues have been explored (to varying degrees of success) with both parties, but the development of new screening instruments has predominantly targeted China. Antitrust cases have been brought against the likes of Google, but their outcomes are uncertain and will take years to manifest.
- The EU has taken significant steps towards increasing funding for EU R&D, though the volume of the funding it has made available still pales in comparison to what has been allocated by the US and China. Early signs point towards funding being allocated more strategically, but the EU is still in need of a better framework for identifying technologies which are critical to its economic prosperity and military capacity.

6. Conclusions and Recommendations

Economic competitiveness and military capacity are both increasingly defined by access to sensitive technologies. This makes the ability to develop and apply them independently key to Dutch and European technological sovereignty. Techno-nationalists have been quick to recognize sensitive technologies' role in fostering dependencies and in establishing spheres of influence. The result has seen sensitive technologies play an increasingly pronounced role in international (great power) competition, something which has served to highlight Dutch and EU vulnerabilities to techno-nationalist measures. A handful of structural factors – many of them interlinked with good-faith assumptions or rooted in European norms and values – undermine the trading bloc's ability to protect the (outputs of) its robust R&D infrastructure. Brain drain, the loss of R&D capabilities, and the transfer (whether through theft or otherwise) of technological know-how are the consequences. Competition over sensitive technologies has also increasingly undermined European companies' ability to compete on the global market, reducing their reach and their turnover and negatively impacting their freedom to finance key R&D activities going forward. This threatens to ultimately lock-in the trading bloc's dependence on US and Chinese technologies in the long term, dashing any serious hopes of achieving a degree of Dutch or European technological sovereignty in the process.

These are not easy problems for the EU to address. Sensitive technologies are likely to grow more (rather than less) central to international competition as the US and China edge closer to technological parity, creating incentives for both to leverage their domestic systems to secure access to even the smallest technological advancements. Other middle powers are likely to step up their efforts to secure access to sensitive technologies, too. Confronted with a choice between being dependent on "gatekeeper" states and safeguarding some degree of independence by pursuing techno-nationalist policies of their own, many will opt to engage in a race to the bottom. This is almost certain to translate into increased pressure on Dutch and European innovation bases, something which will further increase the pertinence of implementing regulatory, procurement-based, fiscal, and diplomatic policies geared towards mitigating the impact of directly and indirectly oriented techno-nationalists alike.

The EU is not taking this in stride. Although this undoubtedly points towards increasing awareness of (and concern over) techno-nationalism's negative effects on the part of Dutch and EU policymakers, both entities can generally be understood as falling short as far comprehensively addressing the high-level goals identified through this study's expert surveys is concerned. Concretely, current policy does little to address indirectly oriented approaches (particularly within the technology space), fails to offer solutions to many directly oriented approaches, and falls short as far as compensating for many of the trading bloc's structural factors is concerned.

This Chapter outlines 36 policy options for reducing the threat that techno-nationalism poses to the Netherlands and to the EU. Many of these recommendations overlap with those outlined in the Dutch Ministry of Finance's (MinFin's) Brede Maatschappelijke Overweging,[218] and in the reflections it catalogues in its publications on "innovatieve samenleving,"[219] "veiligheid en veranderende machtsverhoudingen,"[220] and "spelbal of spelverdeler"[221] more specifically (Box 4).

218 "Brede Maatschappelijke Heroverwegingen" (The Hague: Ministerie van Financiën, 2020), https://www.rijksfinancien.nl/brede-maatschappelijke-heroverwegingen.

219 "Innovatieve Samenleving" (The Hague: Ministerie van Financiën, 2020), https://www.rijksfinancien.nl/bmh/bmh-9-innovatieve-samenleving.pdf.

220 "Veiligheid En Veranderende Machtsverhoudingen" (The Hague: Ministerie van Financiën, 2020), https://www.rijksfinancien.nl/bmh/bmh-15-veiligheid-en-veranderende-machtsverhoudingen.pdf.

221 "Spelbal of Spelverdeler" (The Hague: Ministerie van Financiën, 2020), https://www.rijksfinancien.nl/bmh/bmh-16-speelbal-of-spelverdeler.pdf.

Box 4 – MinFin's Brede Maatschappelijke Overweging vs. the recommendations outlined in this report: a reflection

MinFin's reflections on "innovatieve samenleving,"[222] "veiligheid en veranderende machtsverhoudingen,"[223] and "spelbal of spelverdeler"[224] outline a host of policy options for protecting the Netherlands' innovation ecosystem, bolstering its competitive capacity, and – crucially – achieving a balancing act in which compromises allow both to be pushed forward simultaneously.

Though aspects of all three option categories are represented in the recommendations put forth by this report, the recommendations outlined in this Chapter generally align most closely with the policy options that MinFin describes as contributing to achieving a middle ground between protecting the Netherlands' innovation ecosystem and bolstering its competitive capacity. Specifically, the recommendations outlined in this Chapter align with MinFin's policy options for bolstering the Dutch innovation ecosystem's competitive capacity in that, in paying lip service to relevance of Margrethe Vestager's antitrust initiatives at the EU-level, they echo MinFin's sentiments that growth is likely to be at least partially contingent on the erosion of major tech companies' control over their respective platforms. Other suggestions, including (but not limited to) MinFin's suggestion that domestic competition laws should be loosened, play into this publication's recommendations pertaining to an expansion of the Netherlands' VC scene, though have not been explicitly formulated.

A large number of the policy options MinFin defines as key to protecting the Netherlands' innovation ecosystem are also represented in this Chapter. Specifically, several of the policy options centering around government screening (whether of investments or of students' backgrounds) are echoed in this report's recommendation pertaining to the expansion of critical infrastructure protections and the diligent implementation of EU legislation. Others, including the introduction of legislation which would make espionage a prosecutable offense, are not covered within the context of this report's conclusions & recommendations. This does not mean the authors regard these policy options as unadvisable or as infeasible.

A clear difference between the policy recommendations outlined in this Chapter and those outlined in MinFin's Brede Maatschappelijke Overweging is that this report places a far heavier emphasis on achieving the Netherlands' goals through EU-level cooperation. Outside of speaking to differences in the scope and focus of the two publications, this reflects this report's view that, within the context of safeguarding Dutch technical sovereignty, it is in the Netherlands' best interest to play an active role in incentivizing other EU Member States to take proactive steps to protect and bolster their innovation ecosystems.

The recommendations outlined in the following sections represent the end-product of expert feedback, subject matter expertise, and of an in-depth literature review. They are intended *either* to reduce the negative impact of techno-nationalist policies by putting (regulatory) safeguards in place, *or* by bolstering the competitiveness of EU firms. Each section kicks off with a high-level overview of the reasons that achieving these goals is important to the Netherlands' and/or the EU's (national) security, with concrete policy recommendations for each entity (NL, EU) being subsequently provided in bullet form.

222 "Innovatieve Samenleving."
223 "Veiligheid En Veranderende Machtsverhoudingen."
224 "Spelbal of Spelverdeler."

6.1 Put Safeguards in Place

As has been addressed at length throughout this piece foreign actors, techno-nationalism provides state and non-state actors alike with a strong incentive to engage in activities intended to facilitate the (unwanted) transfer of technology or of technological know-how, or to make for an uneven playing field. This calls, first and foremost, for the implementation of a series of policies geared towards protecting the Netherlands' innovation ecosystem from techno-nationalist approaches.

This policy objective can, broadly speaking, be associated with several high-level goals. First, it is imperative that Dutch authorities' ability to monitor, identify, and intervene in unwanted interactions between Dutch private sector actors and 3rd parties improve. Second, entities comprising the Dutch innovation base should be provided with conditions and with incentives that allow them to grow past the startup phase. This can be partially achieved by policies geared towards providing them with more (financial) support domestically, and partially through policies which increase the viability of investing into improved cybersecurity and counterespionage capabilities or of limiting the depth of their business relationships with and in 3rd countries. Finally, efforts should be made to reduce foreign actors' willingness to pursue techno-nationalist measures.

It is imperative that Dutch authorities' ability to monitor, identify, and intervene in unwanted interactions between Dutch private sector actors and 3rd parties improve.

These policy goals can be associated through the implementation of the following **regulatory**, **procurement-based**, **fiscal**, and **diplomatic** policy initiatives:

Apply critical infrastructure protections to sensitive technologies. One approach to protecting sensitive technologies from market-based approaches is to apply the same regulatory logic to companies working on sensitive technology as to companies involved in maintaining critical infrastructure. These commonly take the form of regulatory systems charged with screening the source and potential motivations of FDI, with a series of guideline-esque safeguards (i.e.: foreign actors cannot hold a controlling interest in or control more than a certain percent of total shares in a company; actors from specific countries are ineligible to purchase shares in specific countries; etc.) having been established to circumvent the lion's share of unwanted scenarios. The Netherlands currently applies such a framework to all companies involved in its "vital processes," with the Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) and EZK both being involved in the screening process. It would be well advised – as part of its efforts to comply with the EU's newly introduced FDI screening mechanism – to iterate on its existing regulatory regime in the following ways:

1. *Formulate a clear set of guidelines detailing what constitutes a sensitive technology and what does not*. The Netherlands' ability to leverage its existing screening and enforcement infrastructure to proactively circumvent unwanted forms of (market-based) techno-nationalism is contingent in it formulating a clear set of enforceable guidelines. This will require, first and foremost, the formulation of a clear set of guidelines detailing those technologies that the country perceives as critical to its economic security and military capacity. The Netherlands currently subscribes to and enforces an EU-formulated list of dual-use technologies.[225] Though this list offers an excellent starting point, it is notably military-centric in its scope. Software-based technologies (such as commercially

225 "L 338," *Official Journal of the European Union* 62 (December 30, 2019), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2019:338:FULL&from=EN.

developed AI) are not adequately covered. The technologies outlined within Chapter 2 offer a helpful starting point for iterating on and updating this list to reflect sensitive technologies' relevance to Dutch economic welfare and military capacity.

2. *Update the NCTV's and EZK's mandates to mirror the US CFIUS' CCTT*. The US CFIUS' CCTT vastly expands the organization's mandate. In the Netherlands, companies working on sensitive technologies are already required to self-report transactions (whether in the form of FDI, patent licensing, sales of goods or services, or otherwise). The Netherlands should – as is being discussed within the context of the adoption of the Bill on *Security Scr eening of Investments, Mergers and Acquisitions*[226] – expand on this existing infrastructure.

The Netherlands' ability to leverage its existing screening and enforcement infrastructure to proactively circumvent unwanted forms of (market-based) techno-nationalism is contingent in it formulating a clear set of enforceable guidelines.

3. *Update exclusion parameters*. Dutch policymakers face difficult considerations as far as *defining* an updated mandate for the NCTV and EZK is concerned. Regulatory overreach may damage the Netherlands' reputation, undermining FDI flows. The country will therefore need to carefully consider what *parameters* it wants to attach to enforcement. The US CFIUS' screening framework offers a helpful tool for identifying transaction types that may be of concern, with parameters pertaining to transactions between a sensitive Dutch company and a Dutch or EU company in which foreign nationals hold more than a predefined percentage of shares being of particular relevance. The Bill on *Security Screen ing of Investments, Mergers and Acquisitions* introduces threshold conditions under which self-reporting would be mandatory for all transaction in which "control" or "significant influence" could feasibly be transferred to foreign actors.[227] While intended to empower enforcing agencies to regulate a wider range of acquisitions, the ambiguity surrounding these terms warrants further specification.

Leverage procurement to improve cybersecurity and counterintelligence. Leveraging existing procurement processes to improve cybersecurity and counterintelligence is regarded as a highly feasible, high impact policy option by experts. The logic underpinning this policy option's robust performance is relatively uncomplicated: by making access to Dutch R&D funding conditional on an organization's ability to meet certain (cyber)security standards or to show a commitment to organizational learning in this area, the Netherlands' innovation ecosystem may well increase its resilience to many of the forced approaches that are commonly utilized by the country's adversaries. This policy option would likely be relatively easy to implement, something which is contingent on the following steps being taken:

4. *Identify requirements for, formulate, and develop a certification process to enforce a clear set of cybersecurity and counterespionage standards for private sector use*. Formulating an industry-backed standard by (for example) engaging an organization such as NEN or CEN-CENELAC to crowdsource information on what can (and cannot) be feasibly implemented will significantly reduce the negative impact of tying compliance with said standard to eligibility to participate in procurement processes going forward.

226 "Regels Tot Invoering van Een Toets Betreffende Verwervingsactiviteiten Die Een Risico Kunnen Vormen Voor de Nationale Veiligheid Gezien Het Effect Hiervan Op Vitale Aanbieders of Ondernemingen Die Actief Zijn Op Het Gebied van Sensitieve Technologie (Wet Veiligheidstoets Investeringen, Fusies En Overnames)" (Tweede Kamer der Staten-Generaal, 2021), https://www.tweedekamer.nl/downloads/document?id=b05e4168-ed0e-4fc0-a77d-bed02e35e64f&title=Advies%20Afdeling%20advisering%20Raad%20van%20State%20en%20Nader%20rapport.pdf.

227 "Regels Tot Invoering van Een Toets Betreffende Verwervingsactiviteiten Die Een Risico Kunnen Vormen Voor de Nationale Veiligheid Gezien Het Effect Hiervan Op Vitale Aanbieders of Ondernemingen Die Actief Zijn Op Het Gebied van Sensitieve Technologie (Wet Veiligheidstoets Investeringen, Fusies En Overnames)."

5. *Identify tenders and procurement processes that make funding available for work relating to sensitive technologies or which commonly attract bids from actors that conduct research into sensitive technologies*. Limit the scope of newly introduced requirements to organizations which have been designated as actors engaged in work relating to sensitive technologies. Also apply to all tenders that make funding available for work relating to sensitive technologies.

6. *Revise identified procurement processes to include adherence to cybersecurity and counterespionage standards as an exclusion criterion*. As a starting point, it should be applied to all contracts granted under the Ambitious Entrepreneurship Action Plan and The Innovative Future Fund.

Arbitrarily blocking 3rd countries from accessing the Netherlands' internal market is viewed as undesirable by experts. Such behavior would undermine the Netherlands' ability to participate in the formation of international norms pertaining to techno-nationalism.

Leverage fairness principles to erect legitimate barriers to trade and to procurement. Arbitrarily blocking 3rd countries from accessing the Netherlands' internal market is viewed as undesirable by experts. Such behavior would undermine the Netherlands' ability to participate in the formation of international norms pertaining to techno-nationalism, an initiative which experts generally view as key to reducing the phenomenon's negative impact. Experts do, however, point to several laws and principles which the Netherlands can cite should it wish to implement barriers to trade or limits on procurement legitimately. One the procurement side, the WTO's Agreement on Government Procurement (GPA) allows from the exclusion of non-parties from public procurement processes. Experts argue that this tool should be leveraged in the following ways:

7. *Exclude Chinese companies from accessing Dutch and/or EU procurement funding*. Restore these companies' ability to participate when and if China signs onto and is shown to comply with the WTO's GPA.

8. *Allow US companies to participate in Dutch and/or EU procurement funding on a case-by-case basis*. Experts cite the reciprocity principle as one which may allow the Netherlands to introduce barriers to trade, arguing that a country's access to the Dutch internal market should be hamstrung if it makes use of legislative approaches to force unwanted technology transfers. Exclude US participating in Dutch or EU procurement processes in instances where the principle of reciprocity can be invoked.

9. *Develop a framework for identifying states' engagement in directly or indirectly-oriented forms of techno-nationalism*. Expand citation of the reciprocity principle to other countries which the Netherlands identifies as engaging in activities that undermine its national security through techno-nationalist practices.

10. **Activate NATO to safeguard economic security.** Outside of incentivizing domestic innovators to take greater responsibility for their (cyber) security, the Netherlands' options for independently addressing the threat that economic espionage and sabotage pose to its economic security are limited. This is because alienating, and ultimately undermining, its economic relationships with the US and China by imposing stringent restrictions on its private sector's ability to interact with these actors is not a feasible course of action for the Netherlands to pursue. Fortunately, the country's NATO membership provides it with a clear opportunity for strengthening its relationship with the US and for mounting a robust multilateral response to these types of activities. The alliance's founding treaty outlines the need for "economic cooperation" on national security matters in its second article

(Article 2),[228] leaving room for cooperation on (dis)allowing foreign vendors to supply sensitive technologies to critical infrastructure providers, and for formulating clear escalation ladders for responding to instances of state-sponsored economic espionage or sabotage. The introduction of these types of policies would serve the purpose of deterring 3rd countries from perpetrating economic espionage and sabotage by explicitly signaling the alliance's recognition of sensitive technologies' relevance to national and economic security and by imposing predictable costs on would-be perpetrators. It would also contribute to avoiding

The Hague should generally strive be more far reaching in its efforts to implement EU Directives quickly and comprehensively. The Netherlands has a vested strategic interest in ensuring that sensitive EU industries are shielded from techno-nationalism.

Encourage and support EU-level initiatives. Although these policy initiatives complement, ensure Dutch compliance with, or supplement several of the EU initiatives outlined in the previous chapter, they are no substitute for a deepening of EU-level cooperation. As can be observed in the (limited) scope of sectors and technologies the Netherlands has moved to safeguard as part of its efforts at complying with the EU's FDI screening mechanism,[229] the Hague should generally strive be more far reaching in its efforts to implement EU Directives quickly and comprehensively. The Netherlands has a vested strategic interest in ensuring that sensitive EU industries are shielded from techno-nationalism, something which it can contribute to by encouraging and supporting the following EU-level initiatives:

11. *Advance WTO reform*. A Trilateral Meeting communiqué from January 2020 detailed the necessary reform to existing WTO rules, especially on subsidies and SOEs. But the agenda has since been dormant. The EU should co-develop a strategy with its close partners how these issues can be introduced at the WTO and how other countries can be brought along.

12. *Ratify the CAI and monitor China's implementation*. The EU should be ready to ratify CAI once Chinese sanctions are lifted.

13. *Adopt the foreign subsidy regulation*. The regulation would fill an important gap in the EU's competition regime and sharpen the EU's ability to ensure fair competition in the single market which would support EU tech industry competitiveness.

14. *Aim for an ambitious EU-China STI agreement*. The agreement should allow the EU to set clear limits on STI cooperation, while in turn deepening engagement in those sectors where common interests exist, with the funding made available through Horizon Europe projects potentially constituting a productive venue for incentivizing compliance.

15. *Develop deterrence to techno-nationalist practices*. The EU must develop concrete deterrence instruments – such as financial or trade sanctions, freezing of assets, or waiving of IP protections – and develop an "escalation ladder" of EU action. The effectiveness of these efforts might lend themselves well to coordination within NATO.

16. *Streamline technology across EU foreign policy*. A reference to "Science Diplomacy" in the Global Approach is a good start, but should receive more serious considerations, for example as part of a revamped Global Connectivity Strategy.

228 "The North Atlantic Treaty (1949)" (Washington, D.C.: The North Atlantic Treaty Organization (NATO), 1949), https://www.nato.int/nato_static_fl2014/assets/pdf/stock_publications/20120822_nato_treaty_en_light_2009.pdf.

229 "List of Screening Mechanisms Notified by Member State."

17. *Refine metrics for sensitive goods and technologies*. The Commission's focus on "strategic dependencies" is a good start and allows to quantify some risks. However, there is still little guidance as to what actions are available, necessary, and proportionate for such goods. Ongoing work on the Critical Tech Observatory should seek to introduce more transparent metrics and methodologies which can action.

18. *Continue EU efforts for harmonized investment screening standards*. The EU screening framework represents only the lowest common denominator with little to no central powers. Deeper integration, moving towards FDI screening uniformity, is necessary, for investment screening of global supply chains is only as strong as its weakest link.

19. *Expand screening to include "economic security"*. Economic security considerations are of growing importance. A reform of the EU screening regulation should consider metrics measuring the competitive effect of foreign investment on strategic technology industries.

20. *Develop financial counters*. If a foreign investor is barred from acquiring a sensitive company or asset, finding alternative funding is paramount. State banks have on occasion stepped up, but not all Member States can count on deep state coffers for acquisitions worth billions. The EU needs a common financial instrument (e.g., equipping the EIB with an explicit mandate) which can take controlling stakes of sensitive EU assets should no private, non-risky buyers be found.

21. *Continue defensive efforts for 5G infrastructure*. Member State autonomy in implementing the 5G Toolbox guidelines has resulted in substantially different approaches on limiting Huawei's role in national networks. Even after national network security laws are implemented, defensive efforts must continue including by training qualified staff, sharing of R&D in network security, and exchanging best practices with allies (e.g., in NATO).

22. *International coordination at the TTC*. The EU and US (and other close partners) must develop close coordination on issues related to economic security and technology, including developing best practices for export controls, common standards for investment screening, and other controls. The TTC is uniquely positioned to foster transatlantic coordination, though it should be open to other partners (Canada, Japan, South Korea, Taiwan).

23. *A multilateral agenda*. Technology and economic security are national concerns with global implications and spill-over effects. Stressing sovereignty does not have to be averse to working with other governments to establish new ground rules. International coordination even with non-allies, whether at the UN or the G20, is paramount.

The entities that make up the Netherlands' innovation ecosystem are ill-equipped to protect themselves from market-based, direct, and indirect approaches. They are liable to be acquired or to lose talent to wealthy competitors.

6.2 Bolster Competitiveness

One of the major reasons that the Netherlands' current and future economic competitiveness and military capacity are threatened by techno-nationalism is that the entities that make up its innovation ecosystem are too small to "survive" exposure to techno-nationalist advances. With the exception of a handful of companies (see for example ASML, TNO, Thales), the Netherlands' innovation ecosystem is made up of startups or of university-based research teams. Entities of this size are ill-equipped to protect themselves from market-based, direct, and indirect approaches, meaning that they are liable to be acquired or to lose talent to

The Netherlands has a vested interest in providing the entities that make up its innovation ecosystem with the conditions and with the impetus to grow. It should put policies in place to incentivize university research teams to found startups, empower startups to mature into scale-ups and (eventually) grown-ups has two high-level benefits, and encourage, support, and contribute to (domestic) vertical ecosystem integrations.

wealthy competitors. They also do not have the resources to defend against legislative or forced approaches. Perhaps most importantly, although they arguably punch above their weight as far as their ability to conduct research into sensitive technologies is concerned (see Chapter 2), they cannot compete with the likes of Google, Lockheed Martin, or Huawei when it comes to transposing their cutting-edge research activities into practice.

Taken together, these characteristics mean that the Netherlands has a vested interest in providing the entities that make up its innovation ecosystem with the conditions and with the impetus to grow. Putting policies in place which are designed a.) to incentivize university research teams to found startups, b.) to empower startups to mature into scale-ups and (eventually) grown-ups has two high-level benefits, and c.) to encourage, support, and contribute to (domestic) vertical ecosystem integrations, will benefit the Dutch innovation ecosystem in several ways. First, encouraging and supporting startup growth increases the Dutch innovation ecosystem's ability to defend itself against techno-nationalist advances, serving both to reduce techno-nationalism's impact on the country's national security and to minimize the need for the implementation of potentially damaging protectionist policies. It also contributes to Dutch technological sovereignty by increasing the viability of sourcing sensitive technologies from domestic suppliers.

Second, incentivizing, supporting, and contributing to initiatives to vertically integrate the R&D of sensitive technologies domestically would create long-term lock-in effects and facilitate the growth of new (innovative) technologies within the Dutch innovation ecosystem. As an example, should the company settle on the Netherlands as a suitable investment locale,[230] Intel's proposed initiative to invest $20bn on two EU-based foundries could – due to such a fab's proximity to ASML – see the Netherlands further cement its position as an important player in the ongoing global chip shortage.[231] It could also prompt the emergence of a wide range of complimentary startups and initiatives. The "lock in" effect created by the scope of ASML and Intel's investments into the Netherlands-based manufacturing facilities means that these startups would likely maintain their affiliation with the Netherlands in the long term, even if they were to be acquired by foreign actors somewhere down the road.

Dutch policymakers can contribute to incentivizing Dutch research teams to found startups; to empowering startups to mature into grow-ups; and to the vertical integration of ecosystems through the implementation of the following **regulatory**, **procurement-based**, and **fiscal** policy initiatives:

24. **Facilitate growth in VC funding.** Though regulatory and administrative barriers to conducting business in the Netherlands are minimal, the country's approach to encouraging private sector growth remains relatively state heavy. State funding for R&D is no substitute for a robust VC ecosystem. Though VC funding in Europe has grown sixfold over the past decade, it still lags far behind the US[232] Whereas VC funding in Europe reached €24bn in 2020, US VCs made $73.6bn available in the same year.[233] The Netherlands also does not punch far above its weight as far as the European context is concerned. The UK is home to over 1800 VC firms; the Netherlands hosts 445. France and

230 Peggy Hollinger and Leila Abboud, "Intel Offers to Spread $20bn Chip Factory Investment across EU," *Financial Times*, July 10, 2021, https://www.ft.com/content/40eda20e-17d8-4368-bdeb-a2d1b151bc34.

231 Nilay Patel, "Why the Global Chip Shortage Is Making It so Hard to Buy a PS5," The Verge, August 31, 2021, https://www.theverge.com/2021/8/31/22648372/willy-shih-chip-shortage-tsmc-samsung-ps5-decoder-interview.

232 Petropoulos and Wolff, "What Can the EU Do to Keep Its Firms Globally Relevant?"

233 Isabella Pojuner and Freya Pratty, "The Data: European vs US VCs," Sifted, May 3, 2021, https://sifted.eu/articles/europe-us-vc/.

Germany host 643 and 796 respectively.[234] Dutch policymakers will need to work towards strengthening this ecosystem to incentivize the formation of startups and to empower them to grow.[235] They will also need to work towards incentivizing Dutch and European VCs to allocate a larger share of their investment portfolios to Dutch or European startups. European VCs are – by and large – far more internationally oriented than their US and Chinese counterparts, something which warrants further discussion with Dutch and European VC heads and founders alike.[236]

Given the fact that a major pitfall for projects realized through (public) R&D funding is their inability to find markets for their technologies once funding ends, the government should also weigh sustainability-related KPIs more heavily within its procurement processes.

25. **Further step up and optimize procurement spending and other public investments.** The Netherlands has already taken several concrete steps towards incentivizing growth within its startup sector. The government committed to increase its R&D spending to 2.5 percent of GDP by 2020, has made funding available for entrepreneurs wanting to expand their businesses quickly, and – crucially – has committed to promoting cooperation between researchers and the private sector and to reducing the regulatory burden on entrepreneurs by (among others) putting an infrastructure in place to grant permits more quickly and by making increased use of digital technologies.[237] The Ambitious Entrepreneurship Action Plan set aside €75mn for providing early-stage financing, strengthening the international position of Dutch startups, and growing businesses.[238] The Innovative Future Fund made €200mn available to innovative SMEs and vital research in 2018.[239] These policies go a long way to encouraging growth, but they do not put the Netherlands on an even footing with China or with the US One key area the Netherlands will need to improve in is to take steps to further improve the predictability (and the longevity) of available funding. This can be achieved by increasing contract lengths on the one hand, and by being more selective in how funds are allocated on the other.[240] Given the fact that a major pitfall for projects realized through (public) R&D funding is their inability to find markets for their technologies once funding ends, the government should also weigh sustainability-related KPIs more heavily within its procurement processes.

26. **Step-up military R&D; strive to co-develop technologies through military procurement.** Within the context of its membership of the European Defence Agency (EDA), the Netherlands has committed to spending two percent of its military expenditures on R&D.[241] While estimates of the scope of the Netherlands' investment into R&D within the military context are few and far between, previous estimates have put the Netherlands'

234 Pojuner and Pratty, "The Data: European vs US VCs."

235 Maija Palmer, Marie Mawad, and Catherina Treyz, "Europe Loosens Rules on Stock Options, but Employees Are Still Sceptical," Sifted, January 20, 2020, https://sifted.eu/articles/stock-option-changes-europe/.

236 Pojuner and Pratty, "The Data: European vs US VCs."

237 "The Government Supports Entrepreneurs," Government of the Netherlands (Ministerie van Algemene Zaken, December 21, 2011), https://www.government.nl/topics/enterprise-and-innovation/the-government-supports-entrepreneurs.

238 "Supporting Ambitious Entrepreneurs and Startups," Government of the Netherlands (Ministerie van Algemene Zaken, December 21, 2011), https://www.government.nl/topics/enterprise-and-innovation/supporting-ambitious-entrepreneurs-and-startups.

239 "Encouraging Innovation," Government of the Netherlands (Ministerie van Algemene Zaken, December 21, 2011), https://www.government.nl/topics/enterprise-and-innovation/encouraging-innovation.

240 Funds should be allocated more explicitly to applied research in sensitive technology areas. MinFin outlines a compelling argument for prioritizing technology areas in which the Netherlands already has a competitive advantage over other states in its piece on innovatieve samenleving; see "Innovatieve Samenleving." Investments should focus on creating ecosystem effects where possible.

241 "Position Paper Investeringen Defensie" (The Hague: Ministerie van Defensie, 2017), www.tweedekamer.nl%2Fdownloads%2Fdocument%3Fid%3Dc5bc286a-202d-4819-9556-621d53d323c8%26title%3DPosition%2520paper%2520TNO%2520t.b.v.%2520hoorzitting%252Frondetafelgesprek%2520Defensienota%2520d.d.%252014%2520december%25202017.pdf&usg=AOvVaw1CEQY1ItErVdQxZiqEs_Ar.

overall 2020 expenditures on R&D at less than 0.8 percent of GDP.[242] If the Netherlands' goal is to foster an innovation ecosystem which can make meaningful contributions to its operational strategic autonomy, the size of these commitments will need to increase going forward. They also should not be invested in ways which make them redundant within the wider EU context. One way of doing this is to follow MinFin's framework for investing in technologies which the Netherlands as an international competitive advantage in.[243] Another is to coordinate expenditures through multilateral instrument. On the EDA side, the Permanent Structured Cooperation (PESCO), European Defence Industrial Development Programme (EDPIP), and Preparatory Action on Defence Research (PADR) instruments are of relevance. On the NATO side, the alliance's Defense Planning Process could be leveraged to ensure that – where relevant – expenditures that the Netherlands is committing to have added value within the context of US' R&D activities.

If the Netherlands' goal is to foster an innovation ecosystem which can make meaningful contributions to its operational strategic autonomy, the size of its financial commitments to R&D will need to increase going forward.

Encourage and support EU-level initiatives. As is also the case with putting safeguards in place, the Netherlands has a vested strategic interest in ensuring that sensitive EU industries can maintain and hone their competitive edges internationally, something which it can contribute to by encouraging and supporting the following EU-level initiatives:

27. *Continue development of instruments to combat unfair competition*. While the EU has made great progress in advancing its unilateral toolkit, some policies remain to be finalized and adopted. The EU must ensure to quickly get its instruments in place, even if it will not require their use.

28. *Fair competition in third countries*. Ensuring a level playing field outside the single market is difficult, especially along the BRI and Digital Silk Road. The EU needs to cooperate with like-minded partners through such initiatives as the Blue Dot Network, Build Back Better World, and the EU's own Connectivity Strategy to ensure open standards for infrastructure allow for fair competition.

29. *Own financial resources*. Without its own serious financial resources, EU tech industrial policy will remain largely dependent on Member States funds. This dilemma risks another failure for EU tech industrial policy. Only if the RFF is succeeded by a common finance instrument which can support tech industrial projects by sharing costs and benefits equally can EU tech industrial policy succeed.

30. *Formulate clear lists and targets*. While a narrower list of "sensitive assets/technologies" is slowly emerging, a clear methodology remains far from obvious. This opens the door to industry lobbyists and dominant firms seeking preferential treatment. Public finance must be provided to all firms in a strategic sector equally and tech industrial policy goals require clear performance targets to be met (or else become political projects).

31. *Mainstream R&D funding*. R&D is critical in determining who develops, defines, and shapes sensitive technologies. While EU R&D ranks highly across the board, more efforts need to be made to focus research on bottleneck technologies and sub-sectors in critical value chains in which Europe may face threat of disruption (e.g., semiconductor design). The EU must create direct linkages following form innovation goals between its different instruments.

242 Alexandra Vennekens, Nelleke van den Broek, and Lionne Koens, "Totale Investeringen in Wetenschap En Innovatie 2018-2024" (Den Haag: Rathenau Instituut, 2020), https://www.rathenau.nl/nl/vitale-kennisecosystemen/totale-investeringen-wetenschap-en-innovatie-2018-2024.

243 "Innovatieve Samenleving."

32. *Enlist procurement instruments*. Procurement contracts can be critical for tech companies on their path to commercialization. To be able to support its most sensitive technologies, the EU needs a strong procurement instrument – or be able to coordinate national procurement instruments – to leverage scale-up of tech start-ups, for example those firms which received EIC funds.

33. *Move ahead on the European Future Fund*. Before the COVID-19 pandemic, the Commission drafted plans for a €100bn sovereign wealth fund to invest (long-term equity) in strategic industries. Such firepower is critical to allow for more private finance to crowd in. The EU should expediate its efforts to make proposals for such a fund.

34. *A European Tech Visa*. Attracting and retaining tech talent is essential. Some ideas practiced in Member States are promising to scale to the EU level, such as helping founders, employees, investors, and researchers in sensitive tech areas inpatriate more easily with the help of a tech visa valid across the single market.

35. *International tech industrial cooperation*. International partners for tech industrial policy are critical. Opening the IPCEI for 3rd country participation, for example, could help build resilient value chains with like-minded partners. Within the TTC, the EU should aim for EU-US joint ventures across sensitive tech value chains, e.g., semiconductors or hydrogen energy. Financial support for EU participating firms could come from the RRF.

36. *Common R&D efforts*. Solving the most pressing innovation challenges cannot be done in isolation, especially in a time when innovation and technological advances rely ever more heavily on international collaboration. The EU and international partners (e.g., in the TTC) must identify sensitive technology challenges and devise policies which incentivize international R&D cooperation. For example, more sustainable critical mineral mining technologies or even substitution could support supply security, an innovation goal shared with many like-minded countries.

8. Annex

8.1 Annex I: Technology Descriptions

8.1.1 AI

The term AI refers, in broad terms, to computers that can perform tasks requiring human-level intelligence or cognition. Narrow AI refers to specific tasks that computers can perform, whereas general AI – which does not yet exist – would be capable of performing numerous tasks for which it has not necessarily been trained.

Experts consider AI to be a transformative technology in part because it will have applications in many different areas and will act as an enabler or catalyst for more specific technologies. By assuming tasks previously performed by humans, AI will allow humans to focus on more complicated tasks. Furthermore, systems run by AI will react faster than standard systems, significantly increase the amount of data that can be managed and the speed at which it is processed. This will likely lead to the creation of new types of economic or military applications.[244]

In the field of international security, it is anticipated that AI will have a substantial impact in three areas. First, it will affect advanced algorithms, by improving machine learning and allowing for technologies such as adversarial AI (in which false data is provided to fool machine learning process. This area also includes technologies such as neuromorphic computing, essentially mimicking the human nervous system). A second area of impact will be leveraging AI tools to process large amounts of evidence or data to provide guidance for policymakers. Third, it is expected that AI will play an important role in the area of human-machine symbiosis, which seeks to enhance humans physically and cognitively.[245]

In practice, AI has already begun to reshape military planning and operations. This includes areas such as early warning, intelligence analysis, battlefield analysis, target acquisition and analysis, drone swarming, command and control, and semi-autonomous decision-making. Experts differ widely as to how AI will affect warfare and international security in the long run. A limited variation would entail an intensification of current AI trends and an increase in the speed at which conflict occurs. A more revolutionary trajectory – and one which many experts view as possible, even likely – would entail the advent of "hyperwar," in which humans are almost entirely absent from the so-called OODA (observe, orient, decide, act) loop and war is conducted by autonomous weapons systems.[246]

---

244 Michael C. Horowitz, 'AI, International Competition, and the Balance of Power', *Texas National Security Review* 1, no. 3 (15 May 2018), https://tnsr.org/2018/05/artificial-intelligence-international-competition-and-the-balance-of-power/; Kelley M. Sayler, 'Emerging Military Technologies: Background and Issues for Congress' (Congressional Research Service, 10 November 2020), https://crsreports.congress.gov/product/details?prodcode=R46458; 'Science and Technology Trends, 2020-2040' (NATO, March 2020), https://www.sto.nato.int/pages/tech-trends.aspx.

245 'Science and Technology Trends, 2020-2040' (NATO, March 2020), https://www.sto.nato.int/pages/tech-trends.aspx, 57;

246 Tim Sweijs and Frans Osinga, 'Maintaining NATO's Technological Edge', *Whitehall Papers* 95, no. 1 (2 January 2019): 104–18, https://doi.org/10.1080/02681307.2019.1731216; David Hambling, 'What Are Drone Swarms And Why Does Every Military Suddenly Want One?', *Forbes*, 1 March 2021, https://www.forbes.com/sites/davidhambling/2021/03/01/what-are-drone-swarms-and-why-does-everyone-suddenly-want-one/; Darrell M. West and John R. Allen, *Turning Point* (Brookings Institution Press, 2020), https://www.brookings.edu/book/turning-point/.

AI will also have security implications beyond the battlefield. For example, technologies such as AI are enabling the emergence of effective mass surveillance on a scale that was previously impossible, using techniques such as facial recognition and smart policing. AI technologies for surveillance purposes are currently in use by at least 75 countries. Many liberal democracies (51 percent as of 2019) both produce and use AI-based surveillance technology. However, the utility of the technology for authoritarian regimes has been demonstrated by China's extensive use of the technology and its leading role in disseminating it. The Chinese firm Huawei has provided AI surveillance technology to at least fifty countries, far more than any other company. AI-supported disinformation is another concern, as malicious actors can use fake social media accounts and realistic-looking photographs to disrupt elections or financial processes. A 2021 report by the US National Security Commission on AI warns that, in spite of US strengths in AI research at universities and in the private sector, China is "China is already an AI peer, and it is more technically advanced in some applications. Within the next decade, China could surpass the US as the world's AI superpower." The report expressed particular concern about China's work on military AI, warning that "China sees AI as the path to offset US conventional military superiority by 'leapfrogging' to a new generation of technology."[247]

The impact of AI has been felt more quickly and in a wider range of activities in the economic sphere than in in international security. Many of the world's largest companies, such as Google, Facebook, and Amazon, rely heavily on AI. They're already driving huge growth in areas as banal as online shopping and product placement. This technology is foundational to the business models of almost every small business. In health care, AI is already outperforming humans in some areas of diagnosis and in determining how to organize complicated clinical trials and will likely play a key role in areas such as improving patient adherence to treatments and in administrative activities. AI is also seen as playing an increasingly important role in financial services, for instance by facilitating round-the-clock interaction with consumers through tools such as chatbots powered by natural language processing. In the automotive industry, AI is already playing a role in areas such as design processes, supply chains, automobile production and post-production, and driver assistance technologies. In the chemical industry, AI does not yet play a major role, but is expected to increasingly figure into areas such as process control, chemical synthesis and analysis, waste minimization, mineral exploration, and chemometrics. In the energy industry, oil and gas companies are exploring using AI to optimize digital operations as well as to protect against the growing problem of cyberattacks.[248]

AI is an area of emphasis for Dutch researchers and industry. The AI Coalition seeks to facilitate cooperation between Dutch companies, universities, the public sector, and civil society to encourage research and economic growth. World-class research in AI is taking place at Dutch universities, and Dutch universities are good at developing collaborations with foreign

247 Steven Feldstein, 'The Global Expansion of AI Surveillance' (Carnegie Endowment for International Peace, 17 September 2019), https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847; John Villasenor, 'How to Deal with AI-Enabled Disinformation' (Brookings Institution, 23 November 2020), https://www.brookings.edu/research/how-to-deal-with-ai-enabled-disinformation/; '2021 Final Report', NSCAI.

248 Thomas Davenport and Ravi Kalakota, 'The Potential for AI in Healthcare', *Future Healthcare Journal* 6, no. 2 (June 2019): 94–98, https://doi.org/10.7861/futurehosp.6-2-94; Alicia Phaneuf, 'AI in Financial Services: Applications and Benefits of AI in Finance', *Business Insider*, 9 September 2020, https://www.businessinsider.com/ai-in-finance; 'AI Reshaping the Automotive Industry', *FutureBridge* (blog), 29 April 2020, https://www.futurebridge.com/industry/perspectives-mobility/artificial-intelligence-reshaping-the-automotive-industry/; Raghav Bharadwaj, 'Machine Learning in the Chemical Industry - BASF, DOW, Royal Dutch Shell, and More', Emerj, 22 November 2019, https://emerj.com/ai-sector-overviews/machine-learning-chemical-industry-basf-dow-shell/; 'Transforming the Energy Industry with AI', *MIT Technology Review*, 21 January 2021, https://www.technologyreview.com/2021/01/21/1016460/transforming-the-energy-industry-with-ai/;

companies, such as the Qualcomm-UvA Deep Vision Lab and the UvA-Bosch Delta Lab, both of which focus on AI.

However, brain drain is a problem. Many foreigners studying AI-related fields do not stay in the Netherlands, and many Dutch students go abroad for employment. Some stay in the EU, but many others leave for opportunities outside the EU, such as in the US One concern in the industry is that when compared to countries such as the US, the environment for investment is less than ideal and that there is a lack of innovation in the industrial sector, which helps to prevent the emergence of Dutch companies on the scale of Google or Apple.[249] One exception to this trend is TomTom, a successful Dutch consumer electronics and navigation company which increasingly uses AI for mapmaking.[250]

Though the Netherlands does cutting-edge theoretical research on AI, it struggles to translate this work into applications that have direct relevance for international security. For example, the Dutch government explored the possibility of holding a Dutch version of DARPA's Cyber Grand Challenge – an all-machine cyber tournament featuring top researchers and hackers – but concluded that there was not sufficient expertise in the country.[251]

8.1.2 Big Data

The term big data refers to datasets too large to be handled by typical database software tools. In fact, the advent of digital platforms such as websites, social media, mobile apps, and machine networks generated enormous datasets too large and complicated to be analyzed by normal data-processing tools.[252] The use of big data comes with significant challenges in terms of volume, velocity, variety, veracity and visualization, but it could also represent a revolutionary tool for many aspects of human life.[253] Big data is a foundational component technology for AI, and the two are closely linked. Many of the applications outlined in section 8.1.1. are forms of machine learning that base themselves on big data.

The ever-growing number of internet users that interact virtually creates huge amounts of data that can be collected, analyzed, and used in various contexts to pursue different goals. In the field of international security, big data allows governments and international organizations to map crises and track population flows as well as perform population surveillance and reach out to the public to gather intelligence.[254] Additionally, states and INGOs such as the UN are developing big data-based projects to perform predictive tasks. These types of projects will employ pattern recognition to predict crime hotspots and detect social instability that could lead to conflict. Big data could therefore play a significant role in conflict prevention.[255] Big data analysis is also promising in the military field, where it has the potential to boost situational awareness by providing enhanced contextual information, improve sensor ranges, and augment non-kinetic targeting effectiveness.[256] Moreover, big data could play a decisive role

249 Interview with expert, May 18, 2021.

250 Pierluigi Casale, 'How Does AI Improve Mapmaking? TomTom, 13 February 2020, https://www.tomtom.com/blog/maps/artificial-intelligence-map-making/.

251 Expert interview.

252 Roberto Moro Visconti, Alberto Larocca, and Michele Marconi, "Big Data-Driven Value Chains and Digital Platforms: From Value Co-Creation to Monetization," *SSRN Electronic Journal*, January 2017.

253 D. F. Reding and J. Eaton, "NATO Science and Tech Trends 2020-2040" (NATO Science & Technology Organization, May 2020), 41.

254 Andrej Zwitter, "The Impact of Big Data of International Affairs," Clingendael Spectator, June 12, 2016, https://spectator.clingendael.org/en/publication/impact-big-data-international-affairs.

255 Zwitter.

256 Reding and Eaton, "NATO Science and Tech Trends 2020-2040," May 2020, 14, 45.

in advancing real-time awareness, early warning systems, and predictive assessments of campaign plans, giving an important decision advantage.[257] Finally, big data analytics can be used to respond to and prevent cyberattacks. The MoD's Cyber Commando focuses on the military applications of big data analysis.[258]

When it comes to economic prosperity, market-leading tech companies are those that have invested in data analytics and digital platforms, such as Amazon, Google, Facebook, and Twitter.[259] Big data has created new business opportunities: companies that work as third-party data aggregators for competitors in a given sector are thriving.[260] Big data analytics has the potential to generate massive economic impact in many sectors. Big data analysis could generate up to $2.5 trillion in economic impact by 2025 through adoption of data-driven mobility services, and up to $260bn potential through massive data integration in retail banking.[261] While big data analysis is already employed in fields such as healthcare, public policy, retail, and mobility, its importance should grow further through symbiosis with AI and machine learning.[262]

The use of big data technology is widespread in the Netherlands, for instance in the banking and finance (BFSI) sector. While ING describes itself as a "data-driven software company"[263] and has invested millions in its data strategy and technologies, Booking.com, one of the largest online travel companies in the world, is a Dutch company that has relied heavily on big data to achieve its market-leading position.[264]

8.1.3 BHET

Biotechnology involves modifying living organisms for a wide variety of purposes through different methods, including genetic modification, bioinformatics, and synthetic biology.[265] Human Enhancement technologies are those biomedical interventions that aim at improving "human form or functioning in excess of what is necessary to restore or sustain health."[266]

According to NATO's "Science & Technology Trends 2020-2040," four major areas of BHET have disruptive significance for international security: bioinformatics and biosensors; human augmentation; medical countermeasures and bio-medical technologies; and synthetic biology. Biosensors allow to gather huge volumes of biological data that can be processed thanks to bioinformatics. Developments in this area could significantly improve predictive combat casualty care and diagnostics, operational readiness, monitoring and bio-situational awareness. This positively impacts military health and training. Human augmentation has the potential to create "human-machine symbiotes of unparalleled capabilities" through technologies such as ocular enhancements for imaging, optogenetic bodysuits sensor

257 Reding and Eaton, 14.

258 Ministerie van Defensie, "Defensie Cyber Commando - Cyber security," onderwerp, Defensie.nl (Ministerie van Defensie, March 29, 2017), https://www.defensie.nl/onderwerpen/cyber-security/cyber-commando.

259 Thulara Hewage et al., "Review: Big Data Techniques of Google, Amazon, Facebook and Twitter," *Journal of Communications* 13 (February 1, 2018): 94–100, https://doi.org/10.12720/jcm.13.2.94-100.

260 Nicolaus Henke et al., "The Age of Analytics" (McKinsey Global Institute, December 2016), 7.

261 Henke et al., 9–10.

262 Henke et al., "The Age of Analytics."

263 Monge, "How ING Engages Customers with Big Data and the Internet of Things."

264 Monge.

265 "Strategische Kennis- En Innovatieagenda 2021-2025," 37; Sayler, "Emerging Military Technologies: Background and Issues for Congress," 17.

266 D. F. Reding and J. Eaton, "NATO Science and Tech Trends 2020-2040" (NATO Science & Technology Organization, May 2020), 21.

webs for restoration and programmed muscular control, and auditory enhancement for communication and protection. These kinds of technologies could greatly enhance soldiers' performances and capabilities. Medical countermeasures could provide significant support in several instances, such as combat casualty care, the diagnostic and treatment options of PTSD and traumatic brain injuries, as well as increased immunocompetence. Lastly, synthetic biology makes use of genetic manipulation and engineering to create capabilities not present in nature. The impact of synthetic biology on international security is still speculative given the technical complexities of developing this kind of technology.[267]

Biotechnologies play a substantial role in European economies, generating an estimated economic turnover of €2.4tn and 18.5 million jobs.[268] Investments in European biotechnology companies have more than doubled since 2005, growing from $5.1bn to at least $11.9bn. Three BHET sectors are particularly important. First, healthcare and pharmaceutical applications contribute to growth by developing new drugs and therapies. Second, agriculture, livestock, veterinary products, and aquaculture, improve food processing, animal feed, and plant breeding. Third, industrial processes and manufacturing involve the production of detergents, pulp and paper, textiles, and biomass with reduced consumption of energy and water, hence enhancing the efficiency of production processes.[269]

While the biggest biotech hub in Europe is currently the UK, a recent report by McKinsey & Company argued that BHET is a potential growth area for Belgium and the Netherlands. Large biotech firms, such as Galapagos, Argenx, and UniQure (each with a market capitalization of more than €2bn) are present in the region. The presence of excellent centers of research, universities, and transport infrastructure provides the foundation for further growth in the BHET section, potentially generating additional annual GDP of €7bn and the creation of 100,000 additional jobs by 2030.[270]

The Netherlands is not a world leader when it comes to research into biotechnology and human enhancement technologies with direct international security applications. However, as with some of the other technology areas, research institutes and universities such as TU Delft (with its Interactive Intelligence Group) and TNO (research groups include Human Performance, Perceptual and Cognitive Systems) do cutting-edge work that has numerous theoretical and indirect links to international security.

8.1.4 Chemical Technologies

The next generation of chemical technologies have an important role to play in the modern global economy, and especially in the Netherlands. According to Deloitte, three trends are transforming the sector. Digitalization allows companies to collect extensive amounts of information, which can be used to improve operations and efficiency. Sustainability has become a focus of the sector, both because of changing consumer preferences and because of the broader trend toward greening of economies. The move toward a circular economy model is

267 Reding and Eaton, "NATO Science and Tech Trends 2020-2040," May 2020, 94-100.

268 "Biotech sector can play a critical role in supporting Europe's economic recovery," HollandBIO, October 27, 2020, https://www.hollandbio.nl/nieuws/biotech-sector-can-play-a-critical-role-in-supporting-europes-economic-recovery/.

269 "Biotechnology," Text, European Commission, accessed May 9, 2021, https://ec.europa.eu/growth/sectors/biotechnology_en.

270 "Scaling Innovation: How Benelux Could Become Europes Leading Biotech Hub."

related to the drive for sustainability, and includes increasing efficiency, extending the lifespan of products and components, and reusing and recycling of materials.[271]

For the Netherlands and Europe, four areas hold the potential to boost economic growth and facilitate the greening of the industry: namely, the use of biomass as a raw material for chemistry; waste as a raw material for chemistry; CO2 as a burgeoning raw material for chemistry; and new, innovative processes based on green electricity. Biomass such as wood, sugar beet, sugar cane, vegetable oils and fats, seaweed and grass could be used as alternative raw materials for the now largely petrochemical-based processing industry. Waste, especially plastics, could be recycled thanks to new chemical technologies: this would reduce the amount of waste burned, a major cause of CO2 emission. CO2 itself could be recycled to produce other kinds of fuels and materials. For instance, synthesis gas is created through a chemical process involving hydrogen and CO2 and can be in turn used to generate alcohols, methane, or naphtha. Electrolysis and plasma technology could enable the production of green electricity.[272]

In the Netherlands, there have been several initiatives working in the aforementioned areas to develop greener chemical manufacturing technologies. For instance, the Coalitie 'Geteelde biogrondstoffen als duurzamefeedstock voor de chemie' is intended to establish a processing chain to supply the chemistry industry with bio-based raw materials, while the startup BrigH2 specializes in the gasification of torrefied biomass. G.I. Dynamics is planning to produce ethylene oxide from bioethanol and Synova Power is working on a project focusing on "cracking" plastic waste by means of gasification. There are also private-public partnerships such as Brightsite, which develop solutions for the production of hydrogen and ethylene using plasma technology, as well as several companies and partnerships focused on electrolysis processes.[273]

The Netherlands is home to several institutions at the forefront of research about chemical manufacturing technologies, including Maastricht University, Tilburg University, TU Eindhoven, Brightsite, Chemelot-InSciTe, DIFFER, and TNO, which creates a favorable environment for the development of innovative chemical technologies. Additionally, the Netherlands hosts many large international firms operating in the field of chemical manufacturing, such as OW Chemical, SABIC, Air Products, Yara, OCI Nitrogen, Cosun and Shell Moerdijk. These companies are at the forefront of the effort to implement innovative green chemical technologies.[274]

The Dutch economy is likely to benefit from developments in the field. It is estimated that the new generation of chemical technologies could create between 8,000 and 10,000 jobs in the chemical industry, 4,000 in the agricultural industry, and 1,000-2,000 in the waste processing sector. Overall, new, cross-sectoral value chains will be generated by green chemical technologies that could yield considerable economic benefits for the Netherlands.[275]

271 'Chemistry 4.0: Growth Through Innovation in a Transforming World' (Deloitte, 2021).

272 "Groene Chemie, Nieuwe Economie," 17–20.

273 "Groene Chemie, Nieuwe Economie," 26–31.

274 "Groene Chemie, Nieuwe Economie," 16.

275 "Groene Chemie, Nieuwe Economie," 24–25.

8.1.5 Photonics

Photonics is the science and technology of generating, controlling, and detecting light particles. Photonics is a foundational technology which plays a role in a wide variety of applications, including mobile phones, televisions, fiber-optic cables, medical equipment, and computers.[276]

Photonics also plays an important role in international security. Given their significance in several military technologies, advances in the field could yield faster battlefield communications as well as improvements in sensors. Additionally, they could support the delivery of advanced space technologies, including high-frequency radars and electronic warfare systems.

As a foundational technology, photonics play a key role in economic and commercial sectors. In the healthcare field, they are used in diagnosis and monitoring machines; in the agri-food sector optical sensors used for food safety and precision agriculture use photonics components; numerous production machines and 3D display technology used for manufacturing processes are based on photonics; in ICT, photonics are indispensable for the functioning of optic fiber and satellite communication; and with respect to energy and environment, photonics support the functioning of optical sensors such as the one used to measure fine dust.[277]

In 2018, optics and photonics core components generated $282bn in global revenues and with the photonics industry employing more than one million workers[278] Europe is among the world leader in photonics' research, application, and production. Europe is the second-largest supplier of photonics components and products in the world, after China, and commands a market share of 15 percent to 17%.[279] Most European businesses working in this field participate in the platform 'Photonics21', which is supported also by the EU.

According to the International Society for Optics and Photonics, Dutch companies are among the most competitive in the field. However, their overall market share remains limited, with scope for the Netherlands to expand in this field. From 2015 to 2020, the size of the global photonics market nearly tripled, from $228bn to an estimated $614bn, an annual growth rate of more than 6.4 percent. In the Netherlands, more than 20,000 people work in the industry at an estimated 290 companies, generating a profit of EUR 4.2bn. The most notable companies include ASML, Océ-Canon, Signify, Philips Healthcare and Prysmian Group.[280]

8.1.6 Quantum Technologies

Quantum technologies rely on the principles of quantum physics and the phenomena related to the atomic and sub-atomic scale. In the last decade, quantum phenomena such as superposition and entanglement have contributed to the development of a new generation of technologies: sensors, clocks, unbreakable encryption and communication systems, and quantum computing.[281]

---

276 "Photonics Lights up Dutch Manufacturing Industry" (ABN AMRO, n.d.); "New Horizons: Securing Europe's Technological Sovereignty through Photonics" (Photonics21, November 2020).

277 "National Agenda Photonics," 5.

278 "Optics and Photonics Industry Report" (SPIE - The International Society for Optics and Photonics, 2020), 4-5.

279 "New Horizons: Securing Europe's Technological Sovereignty through Photonics," 24.

280 "National Agenda Photonics," 11-13.

281 Reding and Eaton, "NATO Science and Tech Trends 2020-2040," May 2020, 19.

In the realm of international security, quantum technologies will be especially important when it comes to military communications, encryption, and stealth technologies. Down the line, this computing technique is also likely to be essential to further progress in AI. More computing power will lead to faster processing of data. Quantum computing could enable big advances in decrypting efforts and the creation of secure communications networks through encryption. The creation of ultra-sensitive gravimetric, magnetic, or acoustic sensors have the potential to radically change underwater warfare by rendering sensing operations significantly more effective. The use of quantum radar could make stealth technologies obsolete by enabling more accurate – and potentially covert – identification of aircrafts such as the F-22, F-35, and B-2. Positioning, navigation and timing (PNT) could also benefit greatly from the development of highly accurate clocks, especially in areas where GPS cannot be employed, for example under ice. While promising, quantum technologies international security applications are currently in the early stages of development. The existence of substantial technical hurdles, as well as the fragility of quantum phenomena themselves, mean that the development of operational systems remains a long-term aspiration.[282]

In the commercial sector, quantum technologies are expected to soon have a significant economic impact. A 2019 study estimated that the quantum sector to be worth 300bn USD by 2050.[283] Much of the research is being done by some of the largest corporations, as they view quantum as having the potential to significantly raise productivity and profits. In 2019, Google declared "quantum supremacy": a Google quantum computer was used to perform a series of operations in 3 minutes and 20 seconds. Google estimated that these operations would take a supercomputer at least 10,000 years to complete. However some, such as IBM, questioned the claim.[284] In the communication sector, quantum can create global networks of secure communications, while in the fields of trading and finance , quantum technologies would enable faster algorithms and optimized speed trading.[285] In the mining and extraction sectors, losses could be limited by the ultra-sensitive detection of leakage and faults provided by quantum sensors, while profit could be maximized by employing quantum sensors for detection of materials' reserves. Faster quantum computing could improve healthcare services and quantum advancements could also contribute to the development of batteries that will supersede lithium-ion technology in the energy sector.[286] Other fields that would benefit greatly from quantum technologies are the ICT and HTSM sectors.[287]

The Netherlands is relatively strong when it comes to R&D of quantum technologies, but continues to lag behind the leading countries. One expert interviewed for this project stated that the Netherlands is very good at creating knowledge, but sometimes struggles to commercialize it. One concern that could emerge in the coming years is brain drain, as students at Dutch universities – both foreign and Dutch – frequently depart for higher pay and more opportunities, especially to the US[288] Quantum Delta NL represents an effort to create a European version of Silicon Valley for quantum technologies, by bringing together the public, private and educational sectors, and is funded by a €615 million grant from the Dutch

282 Reding and Eaton, "NATO Science and Tech Trends 2020-2040," May 2020, 19; Sayler, "Emerging Military Technologies: Background and Issues for Congress," 21; "Strategische Kennis- En Innovatieagenda 2021-2025," 29.

283 "Nationale Agenda Quantumtechnologie" (Quantum Delta Netherlands, September 2019), 49.

284 Elizabeth Gibney, 'Hello Quantum World! Google Publishes Landmark Quantum Supremacy Claim', *Nature* 574, no. 7779 (23 October 2019): 461–62.

285 "Economic Impact of Quantum Technologies."

286 "Economic Impact of Quantum Technologies."

287 "Nationale Agenda Quantumtechnologie."

288 Expert interview, May 11, 2021.

government. The first quantum computer in Europe, Quantum Inspire, was developed by QuTech, a collaboration between TU Delft and TNO.[289]

The Netherlands is not one of the major players when it comes to work on quantum technology with direct relevance to international security. However, TNO is doing important work on the technical side that has relevance to international security. QuSoft, a research center, is working on cryptography. At least one Netherlands-based researcher is working on a project funded by the US Department of Defense's DARPA. And cutting-edge academic work is being done at TU Delft and the University of Amsterdam.[290]

8.1.7 RAS

Robots are machines directed by humans or computers that have a platform, software, and a power source; autonomous systems are machines that can perform functions independently. RAS (RAS) is a widely used umbrella term for technologies that have both physical (robotic) and cognitive (autonomous) characteristics.[291] To a large degree, RAS is dependent on big data and AI.

In the field of international security, RAS is on the verge of having a sizeable impact. NATO has announced a plan to develop several RAS technologies, especially in four fields: autonomous platforms (such as UAVs, autonomous hypersonic weapons, small satellites etc.); human-machine teaming to enhance human performance; countermeasures such as high-power radio frequency weapons; and autonomous behavior, based on the use of AI.[292] Military forces already use RAS, mainly in the form of unmanned vehicles.[293] For instance, UAVs (drones), have changed key military goals and functions, such as situational awareness, strike operations, and intelligence and surveillance.[294] In the near future, it should be possible to use UAVs in swarms to concentrate attacks on defensive weak points, as well as to employ them as defensive shields.[295] RAS technology will also enable new systems such as self-driving supply vehicles, unmanned vessels, advanced sensor systems, and enhanced defense against fast-attack craft.[296] In Europe, the French company Parrot is a leading producer of drones, including military UAVs. Parrot has several international clients, including the government of the US, to which it sells its products such as RAS-driven UAVs.[297]

289 "Quantum Delta NL," Quantum Delta NL, accessed May 4, 2021, https://quantumdelta.nl/.

290 Expert interview; '$2.1M DARPA Grant Puts Lehigh Univ. Optimization Experts at Vanguard of Quantum Computing', EurekAlert!, accessed 14 June 2021, https://www.eurekalert.org/pub_releases/2020-03/lu-dg032020.php; 'Research', *QuSoft* (blog), 3 January 2017, https://www.qusoft.org/research/; 'Quantum Technology', TNO, accessed 14 June 2021, /en/focus-areas/industry/roadmaps/semiconductor-equipment/quantum-technology/.

291 Ash Rossiter, "The Impact of Robotics and Autonomous Syst Zems (RAS) across the Conflict Spectrum," Small Wars & Insurgencies 34, no. 4 (2020): 692; Michel Rademaker and et al, 'Capstone Report: Robotic and Autonomous Systems in a Military Context' (Hague Centre for Strategic Studies, 10 February 2021).

292 Reding and Eaton, "NATO Science and Tech Trends 2020-2040," May 2020, 59–60.

293 Reding and Eaton, "NATO Science and Tech Trends 2020-2040," May 2020.

294 Ash Rossiter, "The Impact of Robotics and Autonomous Systems (RAS) across the Conflict Spectrum," *Small Wars & Insurgencies* 34, no. 4 (2020): 693–94.

295 Michael O'Hanlon, "Forecasting Change in Military Technology, 2020-2040" (Foreign Policy at Brookings, September 2018), 15.

296 O'Hanlon, 14.

297 María de Miguel Molina and Virginia Santamarina Campos, eds., *Ethics and Civil Drones: European Policies and Proposals for the Industry*, 1st ed. 2018, SpringerBriefs in Law (Cham: Springer International Publishing : Imprint: Springer, 2018), 11–26, https://doi.org/10.1007/978-3-319-71087-7.

With regard to commercial applications, RAS can reduce labor costs, increase productivity, and enhance employee safety by undertaking high-risk tasks.[298] For example, in healthcare, autonomous systems assist surgeons in performing surgeries.[299] In agriculture, drones are used to provide data for smarter irrigation and more precise distribution of chemicals.[300] The Anglo-Dutch company Shell employs an autonomous inspection vehicle to gather inspection data from underwater oil and gas facilities.[301] In addition, Shell has commissioned an Italian company, Saipem, to develop FlatFish, an autonomous underwater vehicle that uses AI to perform subsea inspection tasks.[302] This will allow Shell to avoid costly and potentially dangerous missions carried out by humans.

8.1.8 Semiconductor Lithography

Semiconductor lithography, or photolithography, is a process whereby circuit patterns are drawn onto a photomask and subsequently transferred onto a silicon substrate, commonly referred to as a wafer.[303] Lithography applications play a pivotal role across a number fields. Most notably, lithography is used in the fabrication of semiconductors, and hence microchips, which have long been indispensable for the functioning of countless everyday technologies. More recently, semiconductors have been instrumental in powering new foundational technologies such as AI.[304]

Semi-conductor lithography is an indispensable process for the research and production of military technology. Microchips are a core component of weapons systems such as hypersonic missiles, autonomous weapon systems, the newest generations of nuclear weapons, and cyberweapons.[305]

The semiconductors produced thanks to lithography are also used in common appliances such as smartphones, industrial and consumer electronics, wired and wireless infrastructures, servers, datacenters, the automotive industry, and personal computing.[306] There has been a significant shortage of the devices between 2020-2021, which is driven by changes in consumer habits that experts believe will outlast the COVID-19 pandemic.[307] The global market in 2021 was $452.25bn, and will reach an estimated 803.15bn by 2028.[308] NXP, a Dutch company headquartered in Eindhoven, operates in more than 30 countries and employs about 29000 people.

---

298 "Using Autonomous Robots to Drive Supply Chain Innovation" (Deloitte, 2017), 5.

299 "RAS – Visions, Challenges and Actions" (London: The Royal Society, May 2016), 7.

300 "RAS – Visions, Challenges and Actions," 6.

301 "RAS – Visions, Challenges and Actions," 5.

302 Pam Boschee, "Saipem, Shell Work To Advance Subsea Autonomous Vehicle," Journal of Petroleum Technology, January 30, 2019, https://jpt.spe.org/saipem-shell-work-advance-subsea-autonomous-vehicle.

303 "Lithography," Semiconductor Engineering, Semiconductor Engineering, accessed May 18, 2021, https://semiengineering.com/knowledge_centers/manufacturing/lithography/.2021, https://semiengineering.com/knowledge_centers/manufacturing/lithography/.; "Semiconductor Lithography Systems," Nikon, accessed May 18, 2021, https://www.nikon.com/about/technology/product/semiconductor/index.htm.

304 Harald Bauer et al., "Semiconductor Design and Manufacturing: Achieving Leading-Edge Capabilities" (McKinsey, August 2020).

305 Carrick Flynn, "The Chip-Making Machine at the Center of Chinese Dual-Use Concerns," Brookings, June 30, 2020, https://www.brookings.edu/techstream/the-chip-making-machine-at-the-center-of-chinese-dual-use-concerns/.

306 "2020 Annual Report" (ASML, 2020), 19.

307 Mark Sweney, 'Global Shortage in Computer Chips "Reaches Crisis Point"', *The Guardian*, 21 March 2021.

308 "Semiconductor Market Size & Share," Fortune Business Insights, accessed May 18, 2021, https://www.fortunebusinessinsights.com/semiconductor-market-102365.

The Dutch firm ASML is the global leader in the production of photolithography systems, and is the only company in the world that makes so-called EUV machines, which are the most advanced photolithography systems. (Each EUV machine has more than 100,000 components and costs approximately $120mn.) ASML's competitors, Canon and Nikon, use older photolithography machines that can only manufacture less advanced chips. ASML is at the forefront of the global semi-conductors industry and it has a market capitalization of over USD 150bn.[309] TSMC, a Taiwanese company, is the world leader in semiconductor manufacturing, and is ASML's biggest client.[310]

ASML employs more than 28,000 people.[311] In the foreseeable future, ASML faces challenges such as the rising costs of R&D, the scarcity of highly skilled workers, the skyrocketing consumer demands and the trade tensions between the US and China.[312] ASML has been at the forefront of the US government's efforts to maintain a technological edge vis-à-vis China, not least in the field of photolithography, an area in which China has no domestic capacity. In 2019, amidst concerns on the part of the US government that EUV technology could help China develop advanced weapons, the Dutch government prevented ASML from selling an EUV machine to China.[313]

8.1.9 Sensor Technologies

Sensors detect physical properties and provide related, relevant information. They play an important role in everyday commercial and economic use, for example by tracking traffic flows, measuring water quality, and detecting air pollution. In addition, sensors serve as a foundational technology for sensitive technology areas. When it comes to the internet of things, for instance, they play an important role in health care, by allowing for the remote monitoring of heart rates and medicine intake. By enabling the collection of more and better data, sensors are playing an even larger role in the field of big data. The global market for sensor technology is expected to grow at more than six percent in the coming years, and will reach an estimated $228.08bn by 2026.[314] Sensors will play an important role in developing AI that that has real-world, practical applications for consumers.

Sensors also play a crucial role in military operations by detecting key infrastructures, civilian populations, enemy and friendly troops, weather and terrain conditions, etc. There are several types of sensors: chemical sensors; biological sensors; optical, infrared, and UV sensors; radar and radio sensors; sound, sonar, and motion sensors; magnetic detection; and particle beams as sensors.[315]

309 Flynn, "The Chip-Making Machine at the Center of Chinese Dual-Use Concerns."

310 Shuhei Yamada, 'Rise of TSMC Gives Windfall to Dutch Chipmaking Equipment Giant', *Nikkei Asia*, 18 March 2020. Bauer et al., "Semiconductor Design and Manufacturing: Achieving Leading-Edge Capabilities," 3.

311 "ASML at a Glance - The World's Supplier for Semiconductor Industry," ASML, accessed May 18, 2021, https://www.asml.com/en/company/about-asml/asml-at-a-glance.

312 "2020 Annual Report," 20.

313 Flynn, "The Chip-Making Machine at the Center of Chinese Dual-Use Concerns." Demetri Sevastopulo, Sam Fleming, and Michael Peel, 'Will Europe Sign up to Joe Biden's Plan to Counter China?' *Financial Times*, 7 June 2021.

314 'The Sensor-Based Economy', *Wired*, 18 January 2017; 'Environment and the IoT - 5 Cases', Thales Group, accessed 4 June 2021, https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/magazine/five-ways-iot-helping-environment; 'Sensor Market to Hit USD 228bn by 2026 to Attain CAGR of 6.22%', GlobeNewswire News Room, 2 August 2021, https://www.globenewswire.com/news-release/2021/02/08/2171162/0/en/Sensor-Market-to-Hit-USD-228-Billion-by-2026-to-Attain-CAGR-of-6-22-APAC-Region-to-Spearhead-the-Global-Sensors-Market.html.

315 O'Hanlon, "Forecasting Change in Military Technology, 2020-2040," 4-5.

Sensors are indispensable for military operations. This technology area is continually evolving to facilitate identification of greater distances and provide better situational awareness.[316] For example, chemical and biological sensors can be used to detect chemical and biological weapons; improved sensor technology could mitigate the effects of these weapons.[317] Sonar sensors detect objects underwater; advances in technology will increase the ability of sonar to detect submarines and other vessels in noisy water. Improvements in sensors that use the electromagnetic spectrum, such as infrared, UV, radar, and radio sensors, could contribute to enhancing situational awareness and operational effectiveness, especially when paired with robotics and AI. Magnetic detection technologies can be potentially valuable in anti-submarine warfare, but technical difficulties related to long range targets are slowing down developments in this area. The capabilities of radar sensors are also steadily increasing, especially when it comes to detecting moving objects, maximizing the chances of destroying a target, and coordinating defenses against approaching threats. The use of particle beams as sensors is another area of research that has drawn interest, and at short ranges can already outperform x-rays. However, for now, their use is limited to short range objectives. Overall, experts expect that advances in sensor technology in the military sphere will be gradual.[318]

The US is the global leader when it comes to the development and production of sensors. However, traditional Dutch multinationals such as Philips, with its growing focus on cutting-edge healthcare technology, make extensive use of sensors. In addition, the Dutch SME landscape features some innovative start-ups, such as NOWI, in Delft, a semiconductor company which uses a novel form of energy harvesting that uses sensors.[319] The Netherlands is strong in a few critical areas of sensor technology, especially laser (including firms such as VTEC) and optical (where TNO does cutting edge work).[320]

In the international security sphere, Nederland Radarland is a platform in which different entities collaborate to promote research and innovation in the field of radar sensors. Participants in this initiative are the MoD, Thales Nederland, TNO, TU Delft and EZK, along with some SMEs. Another notable research project is "Unmanned Under Water Sensors 2035," also supported by the MoD. This program is designed to gather the knowledge and expertise required to enable the deployment, by 2035, of several underwater unmanned sensors able to perform multiple tasks independently and in coordination with one another.[321]

8.1.10 Space Technologies

Space technologies exploit or are designed to withstand the extreme conditions found beyond the earth's atmosphere. They include satellites, sensors, space stations, and launchers; most of them operate in Low Earth Orbit (LEO).[322]

Space technologies play an increasingly important role in international security. According to NATO's report "Science & Technology Trends, 2020-2040," space technologies can be used in five areas: Position, Navigation, Time (PNT) & Velocity; Integrated Tactical Warning and Threat Assessment; Environmental Monitoring; Communications; and Intelligence,

316 "Strategische Kennis- En Innovatieagenda 2021-2025," 37.

317 O'Hanlon, "Forecasting Change in Military Technology, 2020-2040," 6–7.

318 O'Hanlon, 12.

319 'Rising Stars: 5 Innovative Dutch IoT Startups That Deserve Your Attention in 2019', 30 April 2019, https://siliconcanals.com/news/rising-stars-5-innovative-dutch-iot-startups-that-deserve-your-attention-in-2019/.

320 Expert interview.

321 "Strategische Kennis- En Innovatieagenda 2021-2025," 48.

322 Reding and Eaton, "NATO Science and Tech Trends 2020-2040," May 2020, 76–80.

Surveillance and Reconnaissance.[323] Smallsats, which are smaller and cheaper models, enable military forces to increase situational awareness, obtain strategic information dominance, secure communications, and enhance resilience to anti-satellite weapons. They can operate in constellations that are able to map the surface of the earth, revealing relevant military changes. The development of other technologies, such as electro-optic and infrared sensors allows for sophisticated space-based imaging and sensing that can enhance military performances.[324]

The decreasing costs of accessing space has fueled private investment in space technology.[325] Several companies, such as SpaceX, Blue Origin, and Virgin Galactic, are working toward the development of innovative space technologies.[326] Much of the focus is on satellites, communication constellations, launchers, on-orbit repair of space infrastructures, and space tourism.[327] Space technologies can be employed in different civil/commercial fields, such as communications in remote areas, low-Earth observation, and weather forecasting.[328] There is already a large sector devoted to exploiting commercial opportunities in space. In 2018, space technologies generated $360bn in revenues. Most of this activity occurred in the satellite industry ($277.5bn) and the telecommunication industry ($126.5bn).[329]

The Netherlands has a sophisticated space industry, with the nexus between universities (notably Delft TU) and the private sector playing an important role.[330] Dutch firms provide services such as smallsats, sensors and satellite components, thermal control systems, space vehicles, and nanosatellites, and many are well-positioned to take advantage of the substantial growth prospects in the sector.[331]

At the same time, as a small country the Netherlands cannot compete in all areas of space technology, so it is specializing in a few key areas. One is providing for secure communications in space (laser and optical communications), based on its expertise in photonics. Cutting edge work is being done at TNO and Airbus, working with some SMEs. Another area of specialization is nanosatellites with miniaturized sensors and EO instruments. Dutch companies such as ISISPACE and NLR are active in this area.[332]

Key priorities for the Netherlands in the coming years will be PNT; SSA; GSA; secure communications; and the development of partly or wholly Dutch-owned space assets.[333]

323 Reding and Eaton, 76.

324 O'Hanlon, "Forecasting Change in Military Technology, 2020-2040," 20; Reding and Eaton, 77–78.

325 van Manen, Sweijs, and Bolder, "Towards a Space Security Strategy Action Points for Safeguarding Dutch Security and Prosperity in the Space Age," 2–3.

326 Kelly Whealan George, "The Economic Impacts of the Commercial Space Industry," *Space Policy* 47 (February 2019): 181, https://doi.org/10.1016/j.spacepol.2018.12.003.

327 Reding and Eaton, "NATO Science and Tech Trends 2020-2040," May 2020, 78–81.

328 O'Hanlon, "Forecasting Change in Military Technology, 2020-2040," 2.

329 Gil Denis et al., "From New Space to Big Space: How Commercial Space Dream Is Becoming a Reality," *Acta Astronautica* 166 (January 2020): 438, https://doi.org/10.1016/j.actaastro.2019.08.031.

330 Hugo van Manen, Tim Sweijs, and Patrick Bolder, "Towards a Space Security Strategy Action Points for Safeguarding Dutch Security and Prosperity in the Space Age" (The Hague Centre For Strategic Studies, March 2021), 4-5.

331 van Manen, Sweijs, and Bolder, 4.

332 Expert interview.

333 Expert interview.

The Netherlands has no military space program and uses other countries' satellites. However, there is a desire to develop more Dutch-controlled assets and capabilities to reduce foreign dependencies. In addition, the MoD will soon publish a Defense Space Agenda.[334]

8.1.11 Weapon Technologies

A new generation of weapons have emerged that promise enhanced precision, higher speed, and increased effectiveness. The most important technologies in this category are DEWs and hypersonic weapon systems.[335]

DEWs produce a beam of concentrated electromagnetic energy, or atomic or subatomic particles designed to injure or kill people and damage or destroy objects.[336] DEWs are useful because of their low cost per shot and ability to engage multiple attackers simultaneously.[337] Moreover, they have the potential to counter drone swarms and missile attacks with higher efficiency and efficacy than current systems. Some DEWs could also be employed to damage communications and radar signals.[338]

Hypersonic weapons reach a speed higher than 5 Mach (6125kph), making them difficult to intercept. There are three types of hypersonic systems: boost glide, cruise missiles, and hypersonic aircraft. Specific weapons include air-launched strike missiles, maneuvering re-entry glide vehicles, ground-sea ship killers, and post-stealth strike aircraft. They could be employed in long-range strikes and quick and precision response against intercontinental ballistic missiles, increasing the probability of a successful strike thanks to the difficulties in intercepting such a quick weapon. Additionally, hypersonic unmanned aerial vehicles could be used for intelligence, surveillance, and reconnaissance operations, granting long-distance capabilities with higher flexibility and the possibility of carrying weapons. The unprecedented speed and maneuverability of hypersonic weapons means that they have revolutionary potential in military operations, especially given the lack of countermeasures against these weapon systems.[339]

However, the significant cost and expertise involved limits the number of countries that can develop hypersonic weapons. With France and the UK being the only European states in the process of developing these weapon systems, Europe is falling behind the US, China, and Russia in the race to develop hypersonics.[340] However, European countries have pooled expertise and resources to develop a system able to intercept hypersonic threats. The TWISTER (Timely Warning and Interception with Space-based Theater surveillance) project is supported by France, the Netherlands, Italy, Spain, Finland, and Germany.[341] TWISTER involves the creation of an endo-atmospheric interceptors with the ability to detect, track, and

334 Expert interview; https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2021/05/20/beantwoording-kamervragen-over-hcssclingendael-publicatie/beantwoording-kamervragen-over-hcssclingendael-publicatie.pdf

335 "Strategische Kennis- En Innovatieagenda 2021-2025," 37.

336 Anna de Courcy Wheeler and Maya Brehm, "Directed Energy Weapons," 2017, 1.

337 Sayler, "Emerging Military Technologies: Background and Issues for Congress," 14.

338 Sayler, 15.

339 Reding and Eaton, 86-89

340 Reding and Eaton, 89-90; Audrey Quintin and Robin Vanholme, "Hypersonic Missiles and European Security: Challenges Ahead," FINABEL, July 28, 2020, https://finabel.org/hypersonic-missiles-and-european-security/.

341 Sebastian Sprenger, "Germany Joins Nascent European Push to Shoot down Hypersonic Missiles," Defense News, November 30, 2020, https://www.defensenews.com/global/europe/2020/11/30/germany-joins-nascent-european-push-to-shoot-down-hypersonic-missiles/.

neutralize a variety of threats, including hypersonic cruise missiles and gliders, and is scheduled to be ready for use by 2030.[342]

For now, DEWs and hypersonic weapons do not have a substantial economic impact in the Netherlands.

8.1.12 3D Printing and Advanced Materials

3D printing, often referred to as additive manufacturing, entails the creation of solid 3D objects based on a digital model through the layering of materials. It can be used to perform repairs, manufacture prototypes, and produce customized and precise components. Advanced materials are produced thanks to techniques such as nanotechnology and synthetic biology and can be used to improve energy storage, heating resistance, stealth, and superconductivity as well as food production, building materials, and fuel.[343]

The potential impact of 3D printing on international security holds promise, particularly in the military field. 3D printing could bolster remote logistics operations by reducing the number of spare parts and supplies needed.[344] Other applications for 3D printing could be: the modelling and prototyping of military technology; the replacement of systems' components; the embedding of electronics straight in or on parts; repairs directly on the battlefield, in space, and on ships; and the manufacturing of weapon systems.[345]

Several advanced materials could also have a substantial impact on international security, especially when it comes to enhanced robustness, operational life, and decreased dimension and weight of weapon systems. In general, advanced materials have the potential to be used for improving infrared photodetection for thermal imaging; rendering communications faster; forming barriers against biochemical weapons; and increasing energy storage and generation. Graphene is an example of an advanced material with extensive military applications. In fact, the use of graphene could lead to the improvement of high-frequency electronics and the provision of anti-corrosion and anti-icing functional coatings, as well as applications in energy storage, weapon technologies, body protection through armors and textiles, and sensors. Another advanced material with potential international security applications is black silicon, which enables the absorption of visible and infrared light because of its surface, which is formed by micro-spike traps. Black silicon could be used in the production of photodetectors, solar cells, and night-vision systems.[346]

3D printing is already highly influential in commercial production and supply chain processes, with the market for this type of technology growing. The 3D printing market is expected to rise from $5.8bn in 2016 to $55.8bn by 2027. In the US, two-thirds of manufacturers have already adopted 3D printing, especially for prototyping purposes. In the construction industry, 3D printing has the potential to contribute to building infrastructures. For healthcare, it will be instrumental in the creation of so-called bio-materials, such as organs and body parts.[347] 3D printing can also play an environmental role, for example by reducing product waste and

342 "TWISTER Missile Defence Project Wins Key European Approval," 2019, https://www.airforce-technology.com/news/twister-missile-european-approval/.

343 Reding and Eaton, "NATO Science and Tech Trends 2020-2040," May 2020, 22.

344 O'Hanlon, "Forecasting Change in Military Technology, 2020-2040," 26.

345 Reding and Eaton, "NATO Science and Tech Trends 2020-2040," May 2020, 107.

346 Reding and Eaton, 106.

347 Reding and Eaton, 107.

cutting transportation costs. 3D printing could also be used for the fabrication of furniture and home appliances.[348]

The applications of advanced materials, such as graphene, are being utilized in a wide range of fields such as electronics, health care, aerospace, the automotive industry, energy storage, water desalination, chemicals, traditional and renewable energy, and communications.[349]

The global market for 3D printing is expected to expand rapidly, from $13.78bn in 2020, at an annual rate of 21 percent between 2021 and 2027. The global market for additive materials is already massive and, with an expected annual growth rate of 4.5 percent, will reach an estimated $2.1 trillion by 20025.[350]

While the US dominates the 3D printing and advanced materials industries, Europe has the second-largest market share. In particular, when it comes to 3D printing, Germany, the UK, Italy, and France lead the way thanks to companies such as EOS, Renishaw, SLM Solutions, and Photocentric. The Netherlands also plays a role in the R&D of 3D printing and advanced materials, albeit to a lesser degree than some of its neighbors. Examples of Dutch ventures in the field are 3D printing company Ultimaker[351] and the Provincie Noord Holland's project XL-3D printers.[352]

348 "The Impact of 3D Printing on the Global Economy and the Environment," NeoMetrix Technologies, accessed May 12, 2021, https://3dscanningservices.net/blog/the-impact-of-3d-printing-on-the-global-economy-and-the-environment/.

349 Reding and Eaton, "NATO Science and Tech Trends 2020-2040," May 2020, 106.

350 '3D Printing Market Size, Share | Industry Report, 2021-2028' (Grand View Research, May 2021); 'Advanced Materials Market Research Report: Market Size, Industry Outlook, Market Forecast, Demand Analysis, Market Share, Market Report 2020-2025', accessed 4 June 2021, https://www.industryarc.com/Report/15380/advanced-materials-market.html.

351 "Additive Manufacturing Around the World."

352 "Sustainable Building Design for the Masses with XL-3D Printers from Amsterdam-Projects."

8.2 Annex II: **Expert Survey – Importance and Strength**

8.2.1 **Strength**

Technology	Score
AI	4.00
Big Data	3.00
Biotech and Human Enhancement Technologies	2.65
Chemical Technologies	3.42
Photonics	4.20
Quantum	4.20
RAS	3.40
Semi-conductor Lithography	4.96
Sensor Technologies	3.80
Space	3.32
Weapon Technologies	2.29
3D and Advanced Materials	3.25

8.2.2 **Importance**

Technology	Score
AI	4.38
Big Data	4.00
Biotech and Human Enhancement	3.56
Chemical Technologies	3.91
Photonics	4.05
Quantum	4.21
RAS	No data available
Semi-conductor Lithography	4.52
Sensor Technologies	3.91
Space	3.32
Weapon Technologies	2.83
3D and Advanced Materials	3.42

8.3 Annex III: **Methodology: What Technologies are of Critical Importance to the Netherlands?**

Study	Technologies and Categories
Brookings, "Forecasting Change in Military Technology, 2020-2040"	• Sensors • Computers and Communications • Projectiles, Propulsion, and Platforms • Other Weapons and Sensitive Technologies
NATO, "Science & Technology Trends, 2020-2040"	• Data • AI • Autonomy • Quantum Technologies • Space Technologies • Hypersonics • Biotech and Human Enhancement • Novel materials and 3D Printing
Congressional Research Service, "Emerging Military Technologies"	• AI • Lethal Autonomous Weapons • Hypersonic Weapons • Directed Energy Weapons • Biotechnology • Quantum Technology
McKinsey Global Institute, "Disruptive technologies: Advances that will transform life, business, and the global economy"	• Mobile Internet • Automation of knowledge work • Internet of things • Cloud Technology • Advanced Robotics • Autonomous vehicles • Next Generation Genomics • Energy Storage • 3D Printing • Advanced Materials • Advanced oil and Gas Exploration and Recovery • Renewable Energy
Netherlands MoD, "Strategic Knowledge and Innovation Agenda, 2021-2025"	• AI • Cyber Operations and Cyber-Electromagnetic Activities • Quantum Technology • Sensor Technologies • Human-Machine Integration • Weapons Technologies • Space Technologies • Novel Materials and 3D Printing • Biotechnology • Simulation and Virtual Reality Technology • Human Performance and Training • RAS • Information and Communication Technology and Networks • Behavioral Engineering • Energy Technologies
EZK, "Quantitative Analysis of Research and Innovation in Key Enabling Technologies in The Netherlands"	• Advanced Materials • Chemical Technologies • Digital Technologies • Engineering and Fabrication Technologies • Life Sciences Technologies • Nanotechnologies • Photonics and Light Technologies • Quantum Technologies

The authors of this report would like to thank the following experts for sharing their time and insights with us: Babette Bakker, Adelbert Bronkhorst, Bert Feskens, Julian Kooij, Ulrich Mans, Olaf Terlouw, Ubo Termote, and Ilse Verdiesen. To allow for frank discussions and predictions about the future of these technology areas, the specific contributions of interviewed experts have been kept confidential.

8.4 Annex IV: Taxonomy of Techno-Nationalism; an Overview

Measures that transfer technology and/or technological know-how	Market-based approaches	**FDI & acquisitions**. FDI & acquisitions offer a clear path to acquiring both technology and technological know-how. Both can be associated with negative side-effects. Within the context of sensitive technologies, this dynamic is particularly pronounced in investments that come with conditionality clauses attached or which afford groups or individuals positions on the boards of publicly traded companies.
		Patent licensing. Patent licensing is a key part of many companies' business models. Typically implemented as B2B arrangements, the practice allows a company that has developed a technology to charge 3rd parties to use said technology in their products. The practice is not intrinsically negative, even when applied within the context of sensitive technologies. The practice has the potential of facilitating the manifestation of several suboptimal scenarios.
		Technology purchases. Similar to patent licensing, the acquisition of high-tech goods and services lends itself to the manifestation of negative outcomes because many of the actors which engage in techno-nationalism behave in uncompetitive ways. Once brought to market, products containing sensitive technologies can be procured, replicated, and reintroduced at reduced prices by firms prepared to engage in unfair competition.
	Legislative approaches	**"Lose the market" laws**. "Lose the market" laws link market access to a series of preconditions. While not always overtly geared towards facilitating the transfer of technologies – see for example laws which require companies to store Chinese consumer data domestically – many combine with other aspects of these countries' regulatory landscapes (ability to defend patents in court, corruption, etc.) to make willingness to accept technology theft a de-facto requirement.
		"Violate the law" laws. Unlike "lose the market" laws – which clearly outline conditions that companies must comply with to access a market – "violate the law" laws are laws that are designed to allow for the easy prosecution and sanctioning of companies that refuse to cooperate with efforts at facilitating technology transfers once they are already active within a country's domestic market. "Violate the law" laws are not as structurally ingrained in countries' techno-nationalist strategies as are "lose the market" laws, but offer governments an ad-hoc tool for pressuring foreign companies.
		"No choice" dynamics. "No choice" dynamics are dynamics that make it difficult for foreign companies to protect themselves from technology theft within a country's borders. These range from corruption to local courts' tendency not to protect foreign companies' IP rights within a country's borders. These dynamics exacerbate the negative impact of "lose the market" and "violate the law" laws. They can also make for hostile environments in countries where neither of these law types is applicable.
	Forced approaches	Forced approaches constitute the final approach type that can be employed to secure technology transfers. These include, but are not limited to, the use of espionage and the leveraging of diaspora.
Measures that make for an uneven playing field	Direct approaches	When pursuing direct approaches, governments provide domestic corporations with forms of support that have a direct positive effect on their ability to compete both domestically and internationally. These forms of support include, but are not limited to, financial support (in the form of investments, gifts, subsidies, etc.) and logistical and/or operational support (i.e.: the use of state intelligence agencies to provide companies with a 3rd party's technological know-how).
	Indirect approaches	When pursuing indirect approaches, governments provide domestic corporations with forms of support that indirectly improve their ability to compete both domestically and internationally. These generally take the form of protectionist or mercantilist policies intended to reduce foreign companies' ability to compete domestically. In the case of countries that preside over sizeable domestic markets (see for example China, the US, India, and the EU) this also reduces foreign companies' ability to compete internationally.
	Standard setting	The strategic pursuit of long-term initiatives geared towards reducing 3rd countries' structural ability to compete. These include, but are not limited to, leveraging first-mover advantages to introduce beneficial (technical) standards through international standard-setting bodies and investing into initiatives such as the BRI, which aid in fostering long-term dependence.

8.5 Annex V: **Expert Survey – Feasibility and Potential Impact**

The policy recommendations outlined at the end of this report are, at least in part, based on the results derived from an expert survey. Policy options – summarized within the text as regulatory, procurement-based, fiscal, and diplomatic instrument types – were identified based on a comprehensive literature review and summarized in Chapter 4.3. The survey conducted within the context of Chapter 6 aims to transpose these policy options into policy recommendations by gauging each policy options' feasibility and potential impact.

Open questions also allow for a rough gauging of whether a policy option would be more or less feasible or impactful if implemented at the EU-level. The distinction this study draws between Member State (NL)-level **feasibility** and **potential impact** and EU-level **feasibility** and **potential impact** is a meaningful one. The nature of techno-nationalism is such – due in no small part to the actors involved – that, under ideal circumstances, the potential impact of virtually all policy options is likely to be highest at the EU level. Unfortunately, ideal circumstances are rarely accessible at the EU level. A complicated legislative process in which 27 Member States must agree on major steps means that many policies face major hurdles to implementation at the EU level. This means that it is productive to consider what policies might best serve the Netherlands if implemented unilaterally (read: without EU cooperation). To avoid potential respondents opting not to engage with the survey due to its length, the survey was structured as follows:

Box 5 – Feasibility and potential impact; survey section 1

Section 1: Regulatory responses

The EU has a robust regulatory infrastructure, but - unlike what is the case in the US and China - its focus is less on bolstering national security, and more on ensuring consumer protection and welfare.

Please indicate what you perceive to be the "feasibility" and "potential impact" of the following policy options within the regulatory space:*

1.) Adapt and update existing critical infrastructure protections to include the producers and developers of sensitive technologies. This would likely require the formulation of a clear (shared) definition of what constitutes a sensitive technology. Under this option, companies would be restricted in their freedom to transact with foreign entities or with domestic entities owned by foreign nationals. This would circumvent many open-market-based market failures, such as the unwanted acquisition of R&D powerhouses or the transfer of strategically important technologies.

2.) Set new antitrust precedents. Many of the actions foreign technology companies pursue raise antitrust concerns. European courts should pursue these more actively, establishing new precedents within the sensitive technologies space.

* All questions are optional - a lack of response will be equated with a "don't know."

1. **Feasibility**: adapt and update existing critical infrastructure protections (1-5);
2. **Potential impact**: adapt and update existing critical infrastructure protections (1-5);
3. **Feasibility**: set new antitrust precedents (1-5);
4. **Potential impact**: set new antitrust precedents (1-5);
5. **Additional thoughts: What should absolutely be considered? Should complementary policy initiatives be kickstarted? What do you view as prerequisites for success? Please feel free to be as thorough as you like, particularly with regards to the feasibility and potential impact of EU-level vs. Member State-level implementation.**

Box 6 – Feasibility and potential impact; survey section 2

Section 2: Procurement-based responses

The value at stake in public sector procurement is massive, with public-sector organizations around the world purchasing more than $9.5tn – a number that amounts to 13 percent of the global GDP – of goods and services annually. EU Member States spend more than €1.9tn annually, a value that amounts to approximately 14 percent of the trading bloc's GDP. Though the majority of these investments cannot be linked (whether directly or indirectly) to sensitive technologies, the strategic management of these kinds of expenditures provides the EU with an effective carrot for modifying the behavior of states and non-state actors alike. This potentially makes them an effective tool for addressing awareness deficits and perverse incentive structures in private-sector actors. Because a large share of EU procurement funding goes to foreign companies – some estimates put the bloc's foreign procurement spending at as high as €50bn – it also makes them a potentially useful tool for mitigating the impact of exploitative behaviors propagated by bad-faith actors.

Please indicate what you perceive to be the "feasibility" and "potential impact" of the following policy options within the procurement-based space:*

1.) Leverage procurements to incentivize cybersecurity, counterintelligence, etc. Tendering processes can be used to incentivize – and, in some cases, require – tendering parties to meet a predefined set of conditions. Within the context of mitigating the impact of techno-nationalism, this creates several avenues worth exploring; namely: 1.) the use of tendering processes to improve the quality (and awareness) of security protocols within the European innovation ecosystem, and 2.) the use of tendering processes to disincentivize EU companies from selling sensitive technologies to foreign actors.

2.) Leverage procurement to modify state behavior. foreign companies participate in – and benefit from – EU procurement funding. As an example, the EU's Horizon 2020 research program, which was at least partially geared towards facilitating research into sensitive technologies, actively encouraged US and Chinese participation, with several calls and topics having been specifically targeted towards Chinese enterprise. EU procurement agencies could feasibly threaten to preclude techno-nationalist countries from participating in research programs. They could also introduce behavioral requirements intended to punish actors (state and nonstate alike) which engage in techno-nationalist practices.

* All questions are optional - a lack of response will be equated with a "don't know."

6. **Feasibility**: leverage procurements to incentivize cybersecurity, counterintelligence, etc. (1-5);
7. **Potential impact**: leverage procurements to incentivize cybersecurity, counterintelligence, etc. (1-5);
8. **Feasibility**: leverage procurement to modify state behavior (1-5);
9. **Potential impact**: leverage procurement to modify state behavior (1-5);
10. **Additional thoughts: What should absolutely be considered? Should complementary policy initiatives be kickstarted? What do you view as prerequisites for success? Please feel free to be as thorough as you like, particularly with regards to the feasibility and potential impact of EU-level vs. Member State-level implementation.**

Box 7 – Feasibility and potential impact; survey section 3

Section 3: Fiscal and monetary policy

Another effective – and commonly applied – tool within most state's toolkits is the use of fiscal & monetary policies. Depending on how aggressively (and within which sectors) they are applied, these policies verge on protectionism. Within the European context, their introduction would likely see them mimic CAP in structure, with subsidies being provided to organizations involved in the development of sensitive technologies and tariff barriers being introduced to reduce foreign industries' ability to compete with domestic producers. The implementation of such a policy would likely be contingent on the successful EU-level formulation of a European equivalent of the US' control list, which features a clear definition of what constitutes a sensitive technology.

Please indicate what you perceive to be the "feasibility" and "potential impact" of the following policy options within the procurement-based space:*

1.) Import tariffs and other policies designed to reduce access to the European market.

2.) Subsidies and other (fiscal & monetary) policies intended to insulate the EU innovation ecosystem from unfair competition, or to put it on an even footing with its US and China-based counterparts.

* All questions are optional - a lack of response will be equated with a "don't know."

11. **Feasibility**: import tariffs and other policies designed to reduce access to the European market (1-5);
12. **Potential impact**: import tariffs and other policies designed to reduce access to the European market (1-5);
13. **Feasibility**: subsidies and other (fiscal & monetary) policies (1-5);
14. **Potential impact**: subsidies and other (fiscal & monetary) policies (1-5);
15. **Additional thoughts: What should absolutely be considered? Should complementary policy initiatives be kickstarted? What do you view as prerequisites for success? Please feel free to be as thorough as you like, particularly with regards to the feasibility and potential impact of EU-level vs. Member State-level implementation.**

Box 8 – Feasibility and potential impact; survey section 4

Section 4: Diplomatic responses

Diplomacy, whether by bilateral or multilateral means, offers the Netherlands and the EU another pathway to mitigating the impact of techno-nationalism. The introduction of sanctions, the forging of new bilateral partnerships such as the US and EU's proposed tech alliance, the introduction of new (international) behavioral norms, and the formulation of binding international agreements within the techno-nationalist space. Diplomatic instruments have the potential of helping to address exploitative behavior and of reducing the space for bad-faith actors, though their efficacy is likely to be defined by the specific contours of eventual agreements and (in the case of sanctions) on the circumstances under which they are implemented (messaging, targeted entities, sanction weight, etc.).

Please indicate what you perceive to be the "feasibility" and "potential impact" of the following policy options within the procurement-based space:*

1.) Offensive forms of diplomacy: implement sanctions, recall or summon diplomats, etc.

2.) Constructive diplomacy: norm-building, formulation of bi and multi-national agreements, etc.

* All questions are optional - a lack of response will be equated with a "don't know."

16. **Feasibility**: offensive forms of diplomacy (1-5);
17. **Potential impact**: offensive forms of diplomacy (1-5);
18. **Feasibility**: offensive forms of diplomacy (1-5);
19. **Potential impact**: offensive forms of diplomacy (1-5);
20. **Additional thoughts: What should absolutely be considered? Should complementary policy initiatives be kickstarted? What do you view as prerequisites for success? Please feel free to be as thorough as you like, particularly with regards to the feasibility and potential impact of EU-level vs. Member State-level implementation.**

7. Bibliography

"2020 Annual Report." ASML, 2020.

Epthinktank. "2021-2027 Multiannual Financial Framework and New Own Resources: Analysis of the Commission's Proposal," July 26, 2018. https://epthinktank.eu/2018/07/26/2021-2027-multiannual-financial-framework-and-new-own-resources-analysis-of-the-commissions-proposal/.

"2030 Digital Compass: The European Way for the Digital Decade." European Commission, September 2, 2021. https://eur-lex.europa.eu/resource.html?uri=cellar:12e835e2-81af-11eb-9ac9-01aa75ed71a1.0001.02/DOC_1&format=PDF.

"A Franco-German Manifesto for a European Industrial Policy Fit for the 21st Century." Bundesministerium für Wirtschaft und Energie, February 19, 2019. https://www.gouvernement.fr/sites/default/files/locale/piece-jointe/2019/02/1043_-_a_franco-german_manifesto_for_a_european_industrial_policy_fit_for_the_21st_century.pdf.

"Accession of the People's Republic of China." WTO, November 23, 2001. https://www.worldtradelaw.net/misc/ChinaAccessionProtocol.pdf.download#:~:text=Upon%20accession%2C%20China%20shall%20eliminate,conformity%20with%20the%20WTO%20Agreement.

"Action Plan on Synergies: Between Civil, Defence and Space Industries." European Commission, February 22, 2021. https://ec.europa.eu/info/sites/default/files/action_plan_on_synergies_en_1.pdf.

AMFG Autonomous Manufacturing. "Additive Manufacturing Around the World: What Is the State of 3D Printing Adoption in North America and Europe?," November 7, 2019. https://amfg.ai/2019/11/07/additive-manufacturing-around-the-world-what-is-the-state-of-3d-printing-adoption-in-north-america-and-europe/.

Allas, Terra, Diego Barillà, Simon Kennedy, and Aly Spencer. "How Smarter Purchasing Can Improve Public-Sector Performance." McKinsey, March 29, 2018. https://www.mckinsey.com/industries/public-and-social-sector/our-insights/how-smarter-purchasing-can-improve-public-sector-performance#.

ASML. "ASML at a Glance - The World's Supplier for Semiconductor Industry." Accessed May 18, 2021. https://www.asml.com/en/company/about-asml/asml-at-a-glance.

NOS. "'ASML had juist goede banden met China,'" February 28, 2015. https://nos.nl/l/2021909.

Atkins, Betsy. "Learning From Apple's Spying Incidents - How To Protect Your Company From Corporate Espionage." Forbes, February 12, 2019. https://www.forbes.com/sites/betsyatkins/2019/02/12/learning-from-apples-spying-incidents-how-to-protect-your-company-from-corporate-espionage/.

Axe, David. "Maybe India Will Get Its Super F-16, After All." *Forbes*, May 18, 2020, sec. Aerospace & Defense. https://www.forbes.com/sites/davidaxe/2020/05/18/maybe-india-will-get-its-super-f-16-after-all/.

Baker, Peter. "Biden Plays the Long Game as He Justifies the End of the 'Forever War.'" *The New York Times*, September 1, 2021, sec. US https://www.nytimes.com/2021/09/01/us/politics/biden-politics-afghanistan.html.

Barker, Tyson. "Europe Can't Win Its War for Technology Sovereignty." *Foreign Policy*, January 16, 2020. https://foreignpolicy.com/2020/01/16/europe-technology-sovereignty-von-der-leyen/.

Bauer, Harald, Ondrej Burkacky, Peter Kenevan, Stephanie Lingemann, Klaus Pototzky, and Bill Wiseman. "Semiconductor Design and Manufacturing: Achieving Leading-Edge Capabilities." McKinsey, August 2020.

HollandBIO. "Biotech sector can play a critical role in supporting Europe's economic recovery," October 27, 2020. https://www.hollandbio.nl/nieuws/biotech-sector-can-play-a-critical-role-in-supporting-europes-economic-recovery/.

European Commission. "Biotechnology." Text. Accessed May 9, 2021. https://ec.europa.eu/growth/sectors/biotechnology_en.

Bloomberg News. "China Set to Pass Law Protecting Vital Tech From US" *Bloomberg*, October 15, 2020. https://www.bloomberg.com/news/articles/2020-10-15/china-moves-to-shield-its-own-advanced-tech-in-fight-with-u-s.

Bobba, S., Samuel Carrara, J. Huisman, F. Mathieux, and C. Pavel. "Critical Raw Materials for Strategic Technologies and Sectors in the EU—A Foresight Study." European Comission, 2020. https://rmis.jrc.ec.europa.eu/uploads/CRMs_for_Strategic_Technologies_and_Sectors_in_the_EU_2020.pdf.

Bohn, Dieter. "Apple Isn't Just a Walled Garden, It's a Carrier." The Verge, June 7, 2021. https://www.theverge.com/2021/6/7/22521476/apple-walled-garden-carrier-app-store-innovation.

Borrell, Josep. "Why European Strategic Autonomy Matters." Text. EEAS, 2020. https://eeas.europa.eu/headquarters/headquarters-homepage/89865/why-european-strategic-autonomy-matters_en.

Boschee, Pam. "Saipem, Shell Work To Advance Subsea Autonomous Vehicle." Journal of Petroleum Technology, January 30, 2019. https://jpt.spe.org/saipem-shell-work-advance-subsea-autonomous-vehicle.

Bradford, Anu. "The Brussels Effect." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, 2012. https://papers.ssrn.com/abstract=2770634.

Bradsher, Keith. "How China Obtains American Trade Secrets." *The New York Times*, January 15, 2020, sec. Business. https://www.nytimes.com/2020/01/15/business/china-technology-transfer.html.

"Brede Maatschappelijke Heroverwegingen." The Hague: Ministerie van Financiën, 2020. https://www.rijksfinancien.nl/brede-maatschappelijke-heroverwegingen.

Bureau of Industry and Security. "Bureau of Industry and Security (BIS) Amendment to the Export Administration Regulations (EAR)," May 16, 2019. https://www.bis.doc.gov/index.php/all-articles/17-regulations.

European Chamber. "Business Confidence Survey 2021," 2021. https://www.europeanchamber.com.cn/en/publications-business-confidence-survey.

Büthe, Tim, and Walter Mattli. "International Standards and Standard Setting Bodies." In *The Oxford Handbook of Business and Government*. Oxford: Oxford University Press, 2010.

Castro, Daniel, Micheal McLaughlin, and Eline Chivot. "Who Is Winning the AI Race: China, the EU or the United States." Brussels: Center for Data Innovation, 2019. https://s3.amazonaws.com/www2.data-innovation.org/2019-china-eu-us-ai.pdf.

Cernat, Lucian, and Zornitsa Kutlina-Dimitrova. "How Open Is the European Union to US Firms and Beyond?" *CEPS Policy Insights*, March 2020, 10.

Chee, Foo Yun. "EU Tech Rules Should Only Target Dominant Companies, EU Lawmaker Says." *Reuters*, June 1, 2021, sec. Technology. https://www.reuters.com/technology/eu-tech-rules-should-only-target-dominant-companies-eu-lawmaker-says-2021-06-01/.

Clark, Gregory. "The British Industrial Revolution, 1760-1860." *University of California Davis*, 2005.

European Commission. "Commission Welcomes Agreement on the Modernisation of EU Export Controls," September 11, 2020. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2045.

"Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on A New Industrial Strategy for Europe." European Commission, October 3, 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0102&from=EN.

"Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Global Approach to Research and Innovation." European Commission, May 18, 2021. https://ec.europa.eu/info/sites/default/files/research_and_innovation/strategy_on_research_and_innovation/documents/ec_rtd_com2021-252.pdf.

"Concept Note on Tackling Foreign Interference in Higher Education Institutions and Research Organizations." European Commission, February 2020. https://s3.eu-central-1.amazonaws.com/euobs-media/3ef6dc3d60ee27a2df16f62d47e93fdc.pdf.

Connor, Steve. "Alarm as Dutch Lab Creates Highly Contagious Killer Flu." The Independent, December 21, 2011. https://www.independent.co.uk/news/science/alarm-dutch-lab-creates-highly-contagious-killer-flu-6279474.html.

Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, Pub. L. No. 32020D1127, 246 OJ L (2020). http://data.europa.eu/eli/dec/2020/1127/oj/eng.

Courcy Wheeler, Anna de, and Maya Brehm. "Directed Energy Weapons," 2017.

"Critical Raw Materials Resilience: Charting a Path Towards Greater Security and Sustainability." European Commission, March 9, 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0474&from=EN.

Cunningham, Colleen, Florian Ederer, and Song Ma. "Killer Acquisitions." *Journal of Political Economy* 129, no. 3 (2021): 649–702.

European Commission. "Cybersecurity Strategy," 2021. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy.

Defensie, Ministerie van. "Defensie Cyber Commando - Cyber security." Onderwerp. Defensie.nl. Ministerie van Defensie, March 29, 2017. https://www.defensie.nl/onderwerpen/cyber-security/cyber-commando.

Delhaes, Daniel, Till Hoppe, and Moritz Koch. "Technologie: Wirtschaftskrieg des 21. Jahrhunderts: Wie China den deutschen DIN-Standard verdrängt." Handelsblatt, March 15, 2021. https://www.handelsblatt.com/politik/deutschland/technologie-wirtschaftskrieg-des-21-jahrhunderts-wie-china-den-deutschen-din-standard-verdraengt-/26986456.html.

Denis, Gil, Didier Alary, Xavier Pasco, Nathalie Pisot, Delphine Texier, and Sandrine Toulza. "From New Space to Big Space: How Commercial Space Dream Is Becoming a Reality." *Acta Astronautica* 166 (January 2020): 431–43. https://doi.org/10.1016/j.actaastro.2019.08.031.

European Commission. "Digital Sovereignty: Commission Kick-Starts Alliances for Semiconductors and Industrial Cloud Technologies," 2021. https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3733.

Dorpe, Simon van. "Google Is Back — under EU Competition Scrutiny." POLITICO, June 22, 2021. https://www.politico.eu/article/google-ads-european-union-competition-scrutiny-margrethe-vestage/.

Drooghaag, Johannes. "US' Double Standards on Intellectual Property," August 10, 2020. https://news.cgtn.com/news/2020-08-10/U-S-double-standards-on-intellectual-property-SPWr9yleqs/index.html.

National Research Council. "Economic Impact of Quantum Technologies." Accessed May 4, 2021. https://nrc.canada.ca/en/research-development/research-collaboration/programs/economic-impact-quantum-technologies.

European Commission. "EIT Raw Materials Summit." Text, June 17, 2021. https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/eit-raw-materials-summit_en.

Government of the Netherlands. "Encouraging Innovation." Ministerie van Algemene Zaken, December 21, 2011. https://www.government.nl/topics/enterprise-and-innovation/encouraging-innovation.

European Commission. "EU – China Comprehensive Agreement on Investment (CAI): List of Sections," January 22, 2021. https://trade.ec.europa.eu/doclib/press/index.cfm?id=2237.

European Commission. "EU Foreign Investment Screening Mechanism Becomes Fully Operational." Text, September 10, 2020. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1867.

"EU Framework for FDI Screening." European Parliament, 2019. https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/614667/EPRS_BRI(2018)614667_EN.pdf.

Trade - European Commission. "EU Steps up WTO Action against China's Forced Technology Transfers," December 20, 2018. https://trade.ec.europa.eu/doclib/press/index.cfm?id=1963.

China Innovation Funding. "EU-China Co-Funding Mechanism." Accessed August 9, 2021. http://chinainnovationfunding.eu/eu-china-co-funding/.

European Commission. "EU-China High Level Dialogue on Research and Innovation," January 25, 2021. https://ec.europa.eu/info/news/eu-china-high-level-dialogue-research-and-innovation-2021-jan-25_en.

"EU-Japan Economic Partnership Agreement." European Commission, 2019. https://trade.ec.europa.eu/doclib/docs/2017/july/tradoc_155724.pdf.

European Commission. "List of Calls Targeting China in Horizon 2020 Work Programme for 2014 and 2015," n.d. https://ec.europa.eu/programmes/horizon2020/sites/default/files/List%20of%20calls%20targeting%20China%20in%20Horizon%202020%20work%20programme%20for%202014%20and%202015_2.pdf.

European Commission. Directorate General for Internal Market, Industry, Entrepreneurship and SMEs. and PwC. *The Scale and Impact of Industrial Espionage and Theft of Trade Secrets through Cyber.* LU: Publications Office, 2018. https://data.europa.eu/doi/10.2873/48055.

European Commission. "European Data Strategy," 2021. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en.

European Commission. "European Industrial Strategy," 2021. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-industrial-strategy_en.

European Commission. "European Innovation Council," 2021. https://eic.ec.europa.eu/index_en.

European Union Chamber of Commerce in China. "The Road Less Travelled: European Involvement in China's Belt and Road Initiative," 2020. https://www.europeanchamber.com.cn/en/publications-belt-and-road-initiative.

"Europe's 5G Plans in Limbo after Latest Salvo against Huawei." *POLITICO*, August 23, 2020. https://www.politico.eu/article/europe-5g-plans-in-limbo-after-latest-salvo-against-huawei/.

Fägersten, Björn, and Tim Rühlig. "China's Standard Power and Its Geopolitical Implications for Europe." Swedish Institute of International Affairs, 2019. https://www.ui.se/globalassets/ui.se-eng/publications/ui-publications/2019/ui-brief-no.-2-2019.pdf.

Faulkner, Cameron. "Apple Is Gearing up to Fight the EU over the Lightning Connector." The Verge, January 17, 2020. https://www.theverge.com/2020/1/17/21070848/eu-apple-european-commission-common-charger-lightning-cable-port.

Feigenbaum, Evan. *China's Techno-Warriors: National Security and Strategic Competition from the Nuclear to the Information Age*. Stanford: Stanford University Press, 2003.

Fitzpatrick, Michael. "Did China Steal Japan's High-Speed Train?" *Fortune*, April 15, 2013. https://fortune.com/2013/04/15/did-china-steal-japans-high-speed-train/.

Departement EWI. "Flanders Future Techfund: Vlaamse regering maakt 75 miljoen euro vrij voor nieuw technologiefonds," April 1, 2019. https://www.ewi-vlaanderen.be/nieuws/flanders-future-techfund-vlaamse-regering-maakt-75-miljoen-euro-vrij-voor-nieuw.

Flynn, Carrick. "The Chip-Making Machine at the Center of Chinese Dual-Use Concerns." Brookings, June 30, 2020. https://www.brookings.edu/techstream/the-chip-making-machine-at-the-center-of-chinese-dual-use-concerns/.

Frederic Poitiers, Niclas, and Pauline Weil. "A New Direction for the European Union's Half-Hearted Semiconductor Strategy." Brussels: Bruegel Institute, June 2021. https://www.bruegel.org/wp-content/uploads/2021/07/PC-2021-17-semiconductors-.pdf.

Frisk, Adam. "What Is Project Maven? The Pentagon AI Project Google Employees Want out Of." Global News, April 5, 2018. https://globalnews.ca/news/4125382/google-pentagon-ai-project-maven/.

"FTC Pledges to Fight Unlawful Right to Repair Restrictions - The Verge." Accessed September 8, 2021. https://www.theverge.com/2021/7/21/22587331/right-to-repair-apple-iphone-ftc-lina-khan-open-meeting.

Gallardo, Cristina. "Commission Seeks to Block China from Sensitive Joint Science Projects." POLITICO, March 30, 2021. https://www.politico.eu/article/commission-plans-to-limit-research-tie-ups-with-china/.

Giancarlo, Angela E., Jason Hungerford, Yoshihide Ito, Timothy J. Keeler, Tamer A. Soliman, Margaret-Rose Sales, and Jing Zhang. "US Government Restricts Certain Exports to Huawei and Affiliates by Adding It to Entity List While Permitting Temporary Narrow Exceptions | Perspectives & Events | Mayer Brown." Mayer Brown, May 22, 2019. https://www.mayerbrown.com/en/perspectives-events/publications/2019/05/us-government-restricts-certain-exports-to-huawei-and-affiliates-by-adding-it-to-entity-list-while-permitting-temporary-narrow-exceptions.

"Groene Chemie, Nieuwe Economie." TNO, February 2021.

Han, Aiping, Jianping Ge, and Yalin Lei. "Vertical vs. Horizontal Integration: Game Analysis for the Rare Earth Industrial Integration in China." *Resources Policy* 50 (December 2016): 149–59. https://doi.org/10.1016/j.resourpol.2016.09.006.

Hannas, William C., and Didi Kirsten Tatlow. *China's Quest for Foreign Technology: Beyond Espionage*. Milton Park, Abingdon, Oxon ; New York, NY, 2020.

Henke, Nicolaus, Jacques Bughin, Michael Chui, Tamim Saleh, Bill Wiseman, James Manyika, and Guru Sethupathy. "The Age of Analytics." McKinsey Global Institute, December 2016.

Hewage, Thulara, Malka Halgamuge, Ali Syed, and Gullu Ekici. "Review: Big Data Techniques of Google, Amazon, Facebook and Twitter." *Journal of Communications* 13 (February 1, 2018): 94–100. https://doi.org/10.12720/jcm.13.2.94-100.

Hollinger, Peggy, and Leila Abboud. "Intel Offers to Spread $20bn Chip Factory Investment across EU." *Financial Times*, July 10, 2021. https://www.ft.com/content/40eda20e-17d8-4368-bdeb-a2d1b151bc34.

Hollister, Sean. "Apple Buys Companies at the Same Rate You Buy Groceries." The Verge, May 6, 2019. https://www.theverge.com/2019/5/6/18531570/apple-company-purchases-startups-tim-cook-buy-rate.

"Huawei Is a Paralyzing Dilemma for the West." *Bloomberg.Com*, November 23, 2019. https://www.bloomberg.com/opinion/articles/2019-11-23/huawei-s-5g-networks-are-a-paralyzing-dilemma-for-the-west.

Ians. "Apple IPhones Get Costly in India after Import Duty Hike." *The Hindu*. March 2, 2020, sec. Gadgets. https://www.thehindu.com/sci-tech/technology/gadgets/apple-iphones-get-costly-in-india-after-import-duty-hike/article30961563.ece.

IBISWorld. "Intellectual Property Licencing in the US: Market Size 2002-2027," March 22, 2021. https://www.ibisworld.com/default.aspx.

European Commission. "ICT and Standardisation," 2021. https://digital-strategy.ec.europa.eu/en/policies/ict-and-standardisation.

"Increasing EU's Talent Pool and Promoting the Highest Quality Standards in Support of Digital Transformation." Brussels: European Commission, 2019. https://skills4industry.eu/sites/default/files/2019-06/Brochure_Digiframe_final20190617.pdf.

"Innovatieve Samenleving." The Hague: Ministerie van Financiën, 2020. https://www.rijksfinancien.nl/bmh/bmh-9-innovatieve-samenleving.pdf.

European Commission. "Innovation Fund," February 12, 2019. https://ec.europa.eu/clima/policies/innovation-fund_en.

European Commission. "Joint Declaration on Processors and Semiconductor Technologies," March 6, 2021. https://digital-strategy.ec.europa.eu/en/library/joint-declaration-processors-and-semiconductor-technologies.

"Joint Statement on the Trilateral Meeting of the Trade Ministers of Japan, the United States and the European Union," January 14, 2020. https://trade.ec.europa.eu/doclib/docs/2020/january/tradoc_158567.pdf.

Kang, Cecilia. "A Leading Critic of Big Tech Will Join the White House." *The New York Times*, March 5, 2021, sec. Technology. https://www.nytimes.com/2021/03/05/technology/tim-wu-white-house.html.

Kelly, Éanna. "Technology Sovereignty: New EU Rules to Block Foreign Takeovers." Science|Business, October 13, 2013. https://sciencebusiness.net/technology-strategy-board/news/technology-sovereignty-new-eu-rules-block-foreign-takeovers.

Kelly, Robert E. "Uber and Classic Asian Mercantilism." *The Diplomat*, July 25, 2014. https://thediplomat.com/2014/07/uber-and-classic-asian-mercantilism/.

Kleinhans, Jan-Peter. "The Lack of Semiconductor Manufacturing in Europe." Stiftung Neue Verantwortung, April 6, 2021. https://www.stiftung-nv.de/de/publikation/lack-semiconductor-manufacturing-europe.

Klossek, Polina, Jakob Kullik, and Karl Gerald van den Boogaart. "A Systemic Approach to the Problems of the Rare Earth Market." *Resources Policy* 50 (December 1, 2016): 131–40. https://doi.org/10.1016/j.resourpol.2016.09.005.

Kornbluh, Karen. "Could Europe's New Data Protection Regulation Curb Online Disinformation?" Council on Foreign Relations, February 20, 2018. https://www.cfr.org/blog/could-europes-new-data-protection-regulation-curb-online-disinformation.

Kratz, Agatha, and Janka Oertel. "Home Advantage: How China's Protected Market Threatens Europe's Economic Power." Policy Brief. Brussels: European Council on Foreign Relations, April 2021. https://ecfr.eu/wp-content/uploads/Home-advantage-How-Chinas-protected-market-threatens-Europes-economic-power.pdf.

"L 338." *Official Journal of the European Union* 62 (December 30, 2019). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2019:338:FULL&from=EN.

Lancieri, Filippo, and Patricia Sakowski. "Competition in Digital Markets: A Review of Expert Reports." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, January 30, 2021. https://doi.org/10.2139/ssrn.3681322.

"Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts." European Commission, April 21, 2021. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206.

Leyen, Ursula von der. "Speech in the European Parliament Plenary Session." Strasbourg, November 27, 2019. https://ec.europa.eu/info/sites/default/files/president-elect-speech-original_en.pdf.

"List of Screening Mechanisms Notified by Member State." European Commission, July 14, 2021. https://trade.ec.europa.eu/doclib/docs/2019/june/tradoc_157946.pdf.

Semiconductor Engineering. "Lithography." Semiconductor Engineering. Accessed May 18, 2021. https://semiengineering.com/knowledge_centers/manufacturing/lithography/.

Macalister, Terry. "Environmentalists Back Putin over Shell's Energy Permit." the Guardian, September 25, 2006. http://www.theguardian.com/business/2006/sep/25/russia.oilandpetrol.

Federal Ministry for Economic Affairs and Energy. "Made in Germany: Industrial Strategy 2030," 2021. https://www.bmwi.de/Redaktion/EN/Dossier/industrial-strategy-2030.html.

"Making the Most of the EU's Innovative Potential: An Intellectual Property Action Plan to Support the EU's Recovery and Resilience." European Commission, November 25, 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0760&from=EN.

Manen, Hugo van, Tim Sweijs, and Patrick Bolder. "Towards a Space Security Strategy Action Points for Safeguarding Dutch Security and Prosperity in the Space Age." The Hague Centre For Strategic Studies, March 2021.

Mattioli, Dana. "Amazon Scooped Up Data From Its Own Sellers to Launch Competing Products." *Wall Street Journal*, April 24, 2020, sec. Tech. https://www.wsj.com/articles/amazon-scooped-up-data-from-its-own-sellers-to-launch-competing-products-11587650015.

Mazzucato, Mariana. *Mission Economy: A Moonshot Guide to Changing Capitalism*. London, 2021.

Miguel Molina, María de, and Virginia Santamarina Campos, eds. *Ethics and Civil Drones: European Policies and Proposals for the Industry*. 1st ed. 2018. SpringerBriefs in Law. Cham: Springer International Publishing : Imprint: Springer, 2018. https://doi.org/10.1007/978-3-319-71087-7.

Modderkolk, Huib. "Huawei kon alle gesprekken van mobiele KPN-klanten afluisteren, inclusief die van de premier." de Volkskrant, April 17, 2021. https://www.volkskrant.nl/gs-bd1aece1.

Monge, Juan. "How ING Engages Customers with Big Data and the Internet of Things." Internet of Business, January 13, 2017. https://internetofbusiness.com/ing-customers-big-data-iot/.

"National Agenda Photonics." PhotonicsNL, July 2018.

"Nationale Agenda Quantumtechnologie." Quantum Delta Netherlands, September 2019.

Nelson, Bryce. "Hornig Committee: Beginning of A Technological Marshall Plan?" *Science* 154, no. 3754 (December 9, 1966): 1307–9. https://doi.org/10.1126/science.154.3754.1307.

"New Horizons: Securing Europe's Technological Sovereignty through Photonics." Photonics21, November 2020.

Nicas, Jack, Raymond Zhong, and Daisuke Wakabayashi. "Censorship, Surveillance and Profits: A Hard Bargain for Apple in China." *The New York Times*, May 17, 2021, sec. Technology. https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html.

"Obama to Recall US Troops from Europe." *Financial Times*, April 8, 2011. https://www.ft.com/content/23852314-6236-11e0-8ee4-00144feab49a.

Office of the United States Trade Representative. "Localization Barriers to Trade," n.d. https://ustr.gov/trade-topics/localization-barriers.

O'Hanlon, Michael. "Forecasting Change in Military Technology, 2020-2040." Foreign Policy at Brookings, September 2018.

Ong, Thuy. "Qi Reigns as the Standard for Wireless Charging after Powermat Joins WPC." The Verge, January 8, 2018. https://www.theverge.com/2018/1/8/16862244/powermat-wireless-power-consortium-qi-charging.

"Optics and Photonics Industry Report." SPIE - The International Society for Optics and Photonics, 2020.

Palmer, Maija, Marie Mawad, and Catherina Treyz. "Europe Loosens Rules on Stock Options, but Employees Are Still Sceptical." Sifted, January 20, 2020. https://sifted.eu/articles/stock-option-changes-europe/.

Parrock, Jack. "'It's Going to Kill Your Business': Startups Turn on €2B EU Fund." POLITICO, January 6, 2021. https://www.politico.eu/article/eu-moonshot-startups-alarm-commission-innovation-fund/.

Patel, Nilay. "Nick Clegg Doesn't Think Facebook Is Polarizing." The Verge, March 31, 2021. https://www.theverge.com/2021/3/31/22359026/facebook-nick-clegg-newsfeed-medium-decoder.

———. "Why the Global Chip Shortage Is Making It so Hard to Buy a PS5." The Verge, August 31, 2021. https://www.theverge.com/2021/8/31/22648372/willy-shih-chip-shortage-tsmc-samsung-ps5-decoder-interview.

Petropoulos, Georgios, and Guntram B. Wolff. "What Can the EU Do to Keep Its Firms Globally Relevant?" *Bruegel* (blog), February 15, 2019. https://www.bruegel.org/2019/02/what-can-the-eu-do-to-keep-its-firms-globally-relevant/.

"Photonics Lights up Dutch Manufacturing Industry." ABN AMRO, n.d.

Pojuner, Isabella, and Freya Pratty. "The Data: European vs US VCs." Sifted, May 3, 2021. https://sifted.eu/articles/europe-us-vc/.

"Position Paper Investeringen Defensie." The Hague: Ministerie van Defensie, 2017. www.tweedekamer.nl%2Fdownloads%2Fdocument%3Fid%3Dc5bc286a-202d-4819-9556-621d53d323c8%26title%3DPosition%2520paper%2520TNO%2520t.b.v.%2520hoorzitting%252Frondetafelgesprek%2520Defensienota%2520d.d.%252014%2520december%25202017.pdf&usg=AOvVaw1CEQY1ItErVdQxZiqEs_Ar.

"Positive Peace Report." Institute for Economics and Peace, December 2020. https://reliefweb.int/sites/reliefweb.int/files/resources/PPR-2020web_0.pdf.

Priestap, Bill, and Holden Triplett. "Beyond Economic Espionage." Lawfare, March 3, 2021. https://www.lawfareblog.com/beyond-economic-espionage.

———. "The Transformation of Business in an Age of Espionage." Lawfare, October 20, 2020. https://www.lawfareblog.com/transformation-business-age-espionage.

Priestley, Theo. "Apple Ditching The Headphone Jack Is Less About Music, More About Royalties." Forbes, 2016. https://www.forbes.com/sites/theopriestley/2016/01/11/apple-ditching-the-headphone-jack-is-less-about-music-more-about-royalties/.

"Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act)." European Commission, December 15, 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0842&from=en.

"Proposal for a Regulation of the European Parliament and of the Council on Foreign Subsidies Distorting the Internal Market." European Commission, May 5, 2021. https://ec.europa.eu/competition/international/overview/proposal_for_regulation.pdf.

Propp, Kenneth. "Waving the Flag of Digital Sovereignty." *Atlantic Council* (blog), December 11, 2019. https://www.atlanticcouncil.org/blogs/new-atlanticist/waving-the-flag-of-digital-sovereignty/.

Purpose, Task and. "Hacked: How China Stole US Technology for Its J-20 Stealth Fighter." Text. The National Interest. The Center for the National Interest, July 10, 2019. https://nationalinterest.org/blog/buzz/hacked-how-china-stole-us-technology-its-j-20-stealth-fighter-66231.

Quantum Delta NL. "Quantum Delta NL." Accessed May 4, 2021. https://quantumdelta.nl/.

Quintin, Audrey, and Robin Vanholme. "Hypersonic Missiles and European Security: Challenges Ahead." FINABEL, July 28, 2020. https://finabel.org/hypersonic-missiles-and-european-security/.

European Commission - European Commission. "Recovery and Resilience Facility," 2021. https://ec.europa.eu/info/business-economy-euro/recovery-coronavirus/recovery-and-resilience-facility_en.

"Recovery and Resilience Plans: Example of Component of Reforms and Investments - Digital Components and Cloud Capabilities." European Commission, 2021. https://ec.europa.eu/info/sites/default/files/examples_of_component_of_reforms_and_investment_scale_up_en.pdf.

Reding, D. F., and J. Eaton. "NATO Science and Tech Trends 2020-2040." NATO Science & Technology Organization, May 2020.

———. "NATO Science and Tech Trends 2020-2040." NATO Science & Technology Organization, May 2020.

"Regels Tot Invoering van Een Toets Betreffende Verwervingsactiviteiten Die Een Risico Kunnen Vormen Voor de Nationale Veiligheid Gezien Het Effect Hiervan Op Vitale Aanbieders of Ondernemingen Die Actief Zijn Op Het Gebied van Sensitieve Technologie (Wet Veiligheidstoets Investeringen, Fusies En Overnames)." Tweede Kamer der Staten-Generaal, 2021. https://www.tweedekamer.nl/downloads/document?id=b05e4168-ed0e-4fc0-a77d-bed02e35e64f&title=Advies%20Afdeling%20advisering%20Raad%20van%20State%20en%20Nader%20rapport.pdf.

Regulation (EU) 2016/679 of the European Council of 27 April 2016 on the protection of natural persons with regard to processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Pub. L. No. 2016/679 (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=NL.

"Regulation of the European Parliament and of the Council: Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts," April 21, 2021. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

"Report on the Protection and Enforcement of Intellectual Property Rights in Third Countries." Brussels: European Commission, April 27, 2021. https://trade.ec.europa.eu/doclib/docs/2021/april/tradoc_159553.pdf.

"Robotics and Autonomous Systems – Visions, Challenges and Actions." London: The Royal Society, May 2016.

Rossiter, Ash. "The Impact of Robotics and Autonomous Systems (RAS) across the Conflict Spectrum." *Small Wars & Insurgencies* 34, no. 4 (2020): 691–700.

Sam Harris, and Rob Reid. *Special Episode: Engineering the Apocalypse by Rob Reid and Sam Harris*. Accessed June 29, 2021. https://www.youtube.com/watch?v=UaRfbJE1qZ4&ab_channel=SamHarris.

Sayler, Kelley M. "Emerging Military Technologies: Background and Issues for Congress." Congressional Research Service, 2020.

"Scaling Innovation: How Benelux Could Become Europes Leading Biotech Hub." McKinsey, March 2020. https://www.mckinsey.com/~/media/mckinsey/industries/pharmaceuticals%20and%20medical%20products/our%20insights/biotech%20in%20europe%20a%20strong%20foundation%20for%20growth%20and%20innovation/scaling-innovation-how-benelux-could-become-europes-leading-biotech-hub-march%202020.pdf.

Scott, Mark, and Jacopo Barigazzi. "US and Europe to Forge Tech Alliance amid China's Rise." *POLITICO*, June 9, 2021. https://www.politico.eu/article/eu-us-trade-tech-council-joe-biden-china/.

"Section 301 of the Trade Act of 1974." Congressional Research Service, June 16, 2021. https://crsreports.congress.gov/product/pdf/IF/IF11346.

European Commission. "Secure 5G Networks: Commission Endorses EU Toolbox and Sets out next Steps," January 29, 2020. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_123.

Nikon. "Semiconductor Lithography Systems." Accessed May 18, 2021. https://www.nikon.com/about/technology/product/semiconductor/index.htm.

Fortune Business Insights. "Semiconductor Market Size & Share." Accessed May 18, 2021. https://www.fortunebusinessinsights.com/semiconductor-market-102365.

Sorel, Jean-Jacques. "Le Retard Technologique de l'Europe." *Esprit (1940-)*, no. 365 (11) (1967): 755–75.

"Spain-Netherlands Non-Paper on Strategic Autonomy While Preserving an Open Economy." Kingdom of the Netherlands, March 24, 2021. https://www.permanentrepresentations.nl/documents/publications/2021/03/24/non-paper-on-strategic-autonomy.

"Speech by AKK: Presentation of the Steuben Schurz Media Award," 2020. https://www.bmvg.de/en/news/speech-akk-presentation-steuben-schurz-media-award-3856630.

"Spelbal of Spelverdeler." The Hague: Ministerie van Financiën, 2020. https://www.rijksfinancien.nl/bmh/bmh-16-speelbal-of-spelverdeler.pdf.

Sprenger, Sebastian. "Germany Joins Nascent European Push to Shoot down Hypersonic Missiles." Defense News, November 30, 2020. https://www.defensenews.com/global/europe/2020/11/30/germany-joins-nascent-european-push-to-shoot-down-hypersonic-missiles/.

European Commission. "Standardisation Strategy," 2021. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13099-Standardisation-strategy_en.

European Commission. "State Aid: Commission Invites Stakeholders to Provide Comments on Revised State Aid Rules on Important Projects of Common European Interest," February 23, 2021. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_689.

ECFR. "Strategic Autonomy for the EU? How Europe Can Better Care for Its Security," March 15, 2018. https://ecfr.eu/event/strategic_autonomy_for_the_eu_how_europe_can_better_care_for_its_security/.

"Strategic Dependencies and Capacities." Commission staff working documents. Brussels: European Commission, May 5, 2021. https://ec.europa.eu/info/sites/default/files/strategic-dependencies-capacities.pdf.

"Strategische Kennis- En Innovatieagenda 2021-2025." Ministerie van Defensie, December 2020.

Suire Parron Boggs. "Proposed CFIUS Law WIll Impose New Export Controls on US Businesses," 2018. https://www.squirepattonboggs.com/~/media/files/insights/publications/2018/02/proposed-cfius-law-will-impose-new-export-controls-on-businesses/29559--proposed-cfius-law--new-us-export-controls-client-alert.pdf.

"Summary of the Foreign Investment Risk Review Modernization Act of 2018," n.d. https://www.treasury.gov/resource-center/international/Documents/Summary-of-FIRRMA.pdf.

Government of the Netherlands. "Supporting Ambitious Entrepreneurs and Startups." Ministerie van Algemene Zaken, December 21, 2011. https://www.government.nl/topics/enterprise-and-innovation/supporting-ambitious-entrepreneurs-and-startups.

European Commission. "Sustainable Building Design for the Masses with XL-3D Printers from Amsterdam-Projects." Accessed May 12, 2021. https://ec.europa.eu/regional_policy/en/projects/Netherlands/sustainable-building-design-for-the-masses-with-xl-3d-printers-from-amsterdam.

Sykes, Alan O. "The Law and Economics of 'Forced' Technology Transfer and Its Implications for Trade and Investment Policy (and the US–China Trade War)." *Journal of Legal Analysis* 13, no. 1 (January 1, 2021): 127–71. https://doi.org/10.1093/jla/laaa007.

"Tata, Lockheed Martin to Build F-16 Wings in India," September 4, 2018. https://www.tata.com/newsroom/tata-lockheed-martin-build-f16-wings-in-india.

"The Contribution of National Recovery and Resilience Plans to Achieving Europe's Digital Decade Ambition." Deloitte LLP Report. Deloitte, June 21, 2021. https://www.vodafone.com/sites/default/files/2021-06/deloitte-llp-europe-digital-decade-rrf-gap-analysis.pdf.

European Commission. "The Digital Services Act Package," 2021. https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

Government of the Netherlands. "The Government Supports Entrepreneurs." Ministerie van Algemene Zaken, December 21, 2011. https://www.government.nl/topics/enterprise-and-innovation/the-government-supports-entrepreneurs.

NeoMetrix Technologies. "The Impact of 3D Printing on the Global Economy and the Environment." Accessed May 12, 2021. https://3dscanningservices.net/blog/the-impact-of-3d-printing-on-the-global-economy-and-the-environment/.

"The North Atlantic Treaty (1949)." Washington, D.C.: The North Atlantic Treaty Organization (NATO), 1949. https://www.nato.int/nato_static_fl2014/assets/pdf/stock_publications/20120822_nato_treaty_en_light_2009.pdf.

European Commission. "Towards a next Generation Cloud for Europe," 2021. https://digital-strategy.ec.europa.eu/en/news/towards-next-generation-cloud-europe.

Trade and Agriculture Directorate. "International Technology Transfer Policies." OECD, January 14, 2019. https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2018)8/%20FINAL&docLanguage=En.

European Council. "Trade: Council Agrees Its Negotiating Mandate on the International Procurement Instrument," June 2, 2021. https://www.consilium.europa.eu/en/press/press-releases/2021/06/02/trade-council-agrees-its-negotiating-mandate-on-the-international-procurement-instrument/.

"TWISTER Missile Defence Project Wins Key European Approval," 2019. https://www.airforce-technology.com/news/twister-missile-european-approval/.

CEN-CENELEC. "Types of Standards," 2020. https://www.cencenelec.eu/research/innovation/standardstypes/Pages/default.aspx.

"Updating the 2020 New Industrial Strategy: Building a Stronger Single Market for Europe's Recovery." European Commission, May 5, 2021. https://ec.europa.eu/info/sites/default/files/communication-industrial-strategy-update-2020_en.pdf.

US Department of the Treasury. "Fact Sheet: CFIUS Final Regulations Revising Declaration Requirement for Certain Critical Technology Transactions," September 11, 2020. https://home.treasury.gov/system/files/206/Fact-Sheet-Final-Rule-Revising-Mandatory-Crit-Tech-Declarations.pdf.

US News Staff. "The 10 Safest Countries in the World, Ranked by Perception." US News & World Report, April 27, 2021. https://www.usnews.com/news/best-countries/articles/10-safest-countries-ranked-by-perception.

"US to Withdraw Two Europe Combat Brigades." *BBC News*, January 13, 2012, sec. US & Canada. https://www.bbc.com/news/16543456.

"Using Autonomous Robots to Drive Supply Chain Innovation." Deloitte, 2017.

Varas, Antonio, Raj Varadarajan, Jimmy Goodrich, and Falan Yinug. "Government Incentives and US Competitiveness in Semiconductor Manufacturing." Boston Consulting Group, August 2020. https://web-assets.bcg.com/27/cf/9fa28eeb43649ef8674fe764726d/bcg-government-incentives-and-us-competitiveness-in-semiconductor-manufacturing-sep-2020.pdf.

"Veiligheid En Veranderende Machtsverhoudingen." The Hague: Ministerie van Financiën, 2020. https://www.rijksfinancien.nl/bmh/bmh-15-veiligheid-en-veranderende-machtsverhoudingen.pdf.

Vennekens, Alexandra, Nelleke van den Broek, and Lionne Koens. "Totale Investeringen in Wetenschap En Innovatie 2018-2024." Den Haag: Rathenau Instituut, 2020. https://www.rathenau.nl/nl/vitale-kennisecosystemen/totale-investeringen-wetenschap-en-innovatie-2018-2024.

Verhagen, Paul, Esther Chavannes, and Frank Bekkers. "Flow Security in the Information Age." The Hague Centre For Strategic Studies, December 7, 2020. https://hcss.nl/report/flow-security-in-the-information-age/.

Visconti, Roberto Moro, Alberto Larocca, and Michele Marconi. "Big Data-Driven Value Chains and Digital Platforms: From Value Co-Creation to Monetization." *SSRN Electronic Journal*, January 2017.

EuroStart Enterprises. "What Is the Best Startup Visa Scheme in Europe?," April 6, 2021. https://www.eurostartentreprises.com/en/business-advice/what-is-the-best-startup-visa-scheme-in-europe.

Whealan George, Kelly. "The Economic Impacts of the Commercial Space Industry." *Space Policy* 47 (February 2019): 181–86. https://doi.org/10.1016/j.spacepol.2018.12.003.

Wintour, Patrick. "Europe Divided on Huawei as US Pressure to Drop Company Grows." *The Guardian*, July 13, 2020, sec. Technology. https://www.theguardian.com/technology/2020/jul/13/europe-divided-on-huawei-as-us-pressure-to-drop-company-grows.

World Bank. "GDP per Capita (Current US$) | Data." Accessed June 28, 2021. https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?most_recent_value_desc=true;

World Trade Organization. "Local Content Measures Scrutinized by WTO Members in Investment Committee," June 6, 2019. https://www.wto.org/english/news_e/news19_e/trim_06jun19_e.htm.

Yap, Chuin-Wei. "State Support Helped Fuel Huawei's Global Rise." *Wall Street Journal*, December 25, 2019, sec. Tech. https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736.

———. "State Support Helped Fuel Huawei's Global Rise." *Wall Street Journal*, December 25, 2019, sec. Tech. https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736.

Zhou, Weihuan, and Huiqin Jiang. "Technology Transfer Under China's Foreign Investment Regime: Does the WTO Provide a Solution?" *Journal of World Trade* 54, no. 3 (June 1, 2020). https://kluwerlawonline.com/journalarticle/Journal+of+World+Trade/54.3/TRAD2020021.

Zwetsloot, Remco. "The US Needs Multilateral Initiatives to Counter Chinese Tech Transfer." *Brookings* (blog), June 11, 2020. https://www.brookings.edu/techstream/the-u-s-needs-multilateral-initiatives-to-counter-chinese-tech-transfer/.

Zwitter, Andrej. "The Impact of Big Data of International Affairs." Clingendael Spectator, June 12, 2016. https://spectator.clingendael.org/en/publication/impact-big-data-international-affairs.

"中华人民共和国网络安全法 'Cybersecurity Law of the People's Republic of China,'" November 7, 2016. http://www.gov.cn/xinwen/2016-11/07/content_5129723.htm.

"将源代码和算法一并列入管制物项_中国人大网," October 15, 2020. http://www.npc.gov.cn/npc/c30834/202010/0998a6a07d6e44b9be1d2ca48335f493.shtml.

The Hague Centre
for Strategic Studies

HCSS
Lange Voorhout 1
2514 EA Hague

Follow us on social media:
@hcssnl

The Hague Centre for Strategic Studies
Email: info@hcss.nl
Website: www.hcss.nl