The Hague Centre
for Strategic Studies

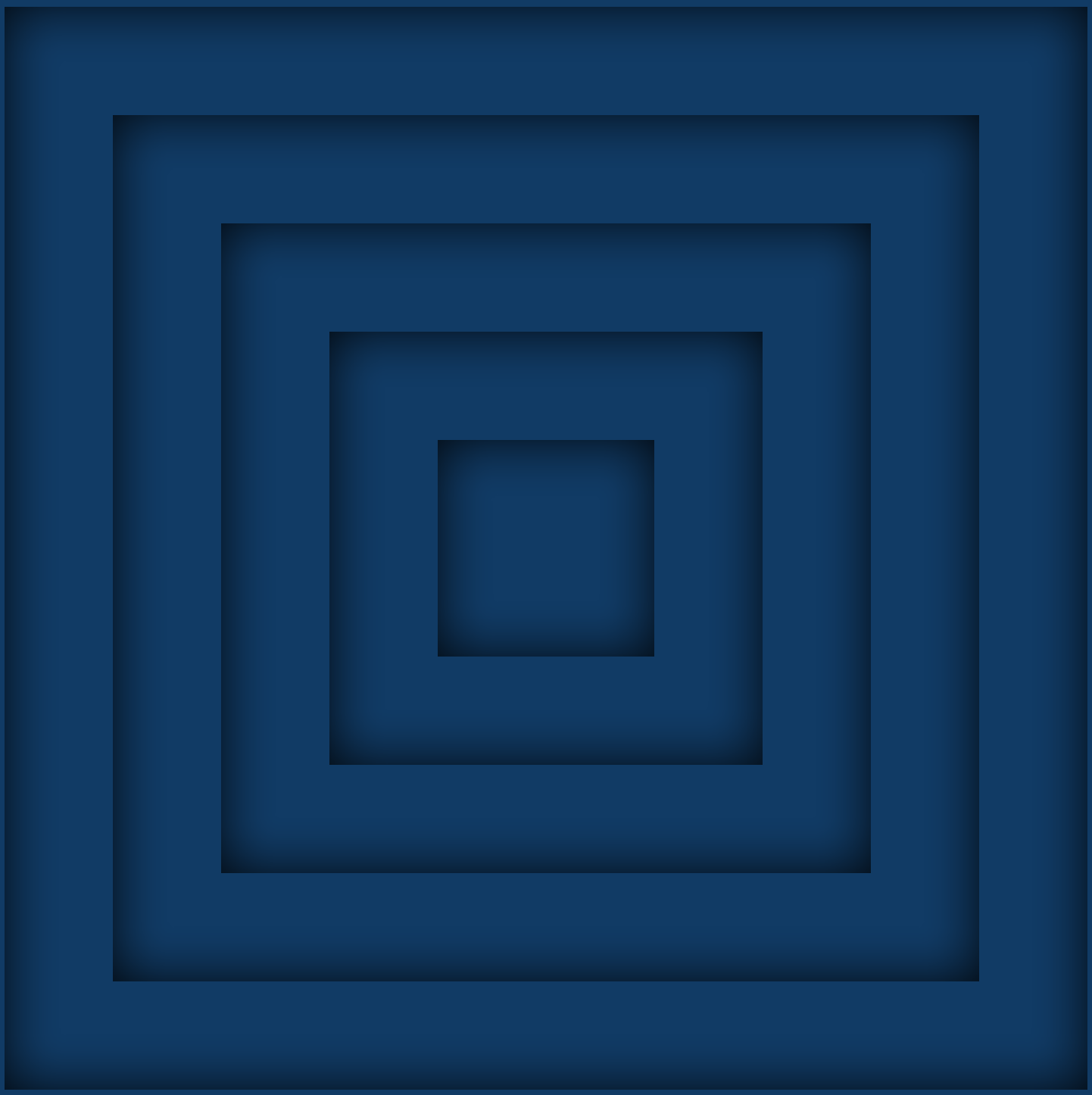
Taming Techno-Nationalism

A Policy Agenda

Executive Summary

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

September 2021



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.«

Taming Techno-Nationalism

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).

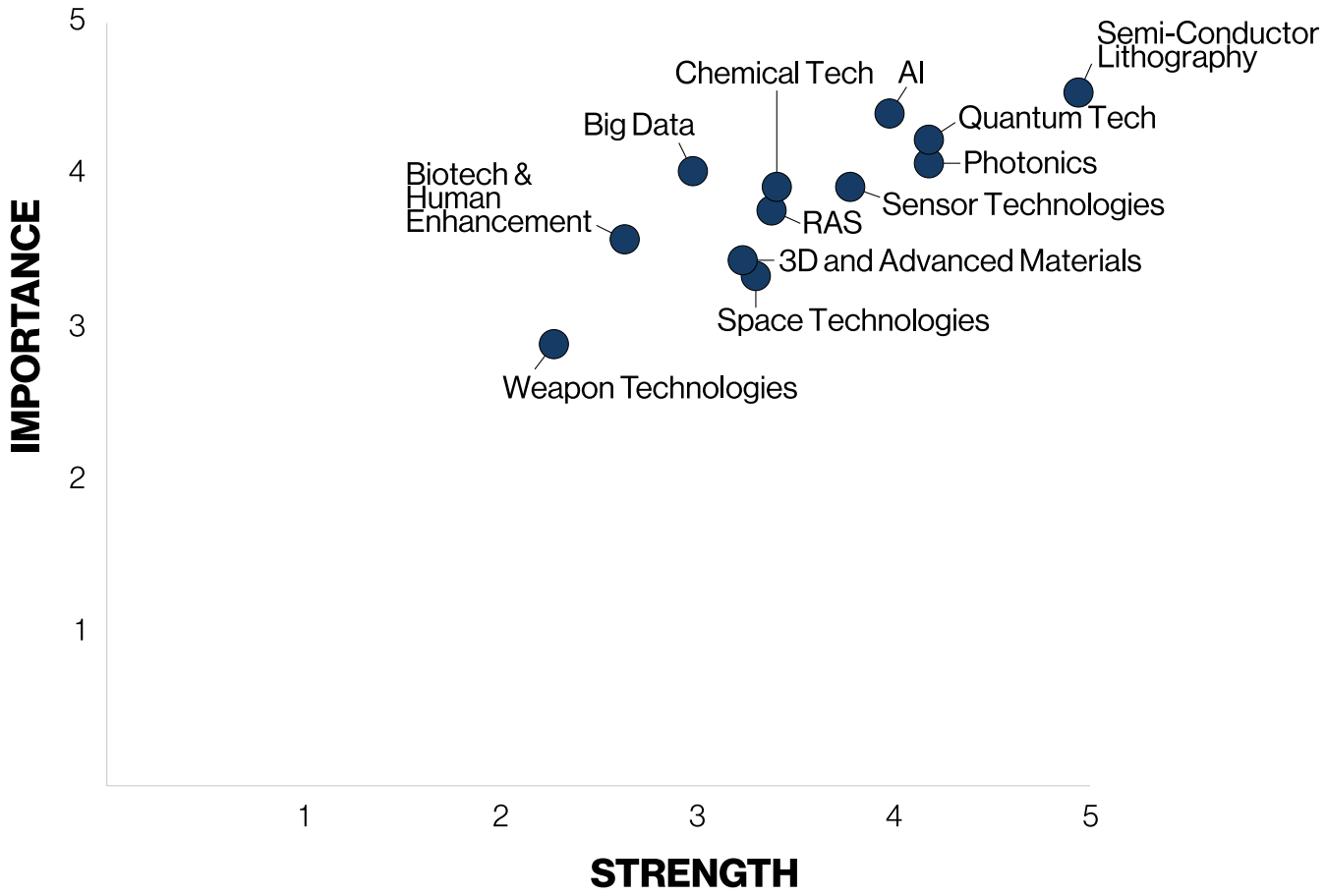


Figure 1 - Experts' appraisal of the strength and importance in sensitive technology areas for the Netherlands

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).

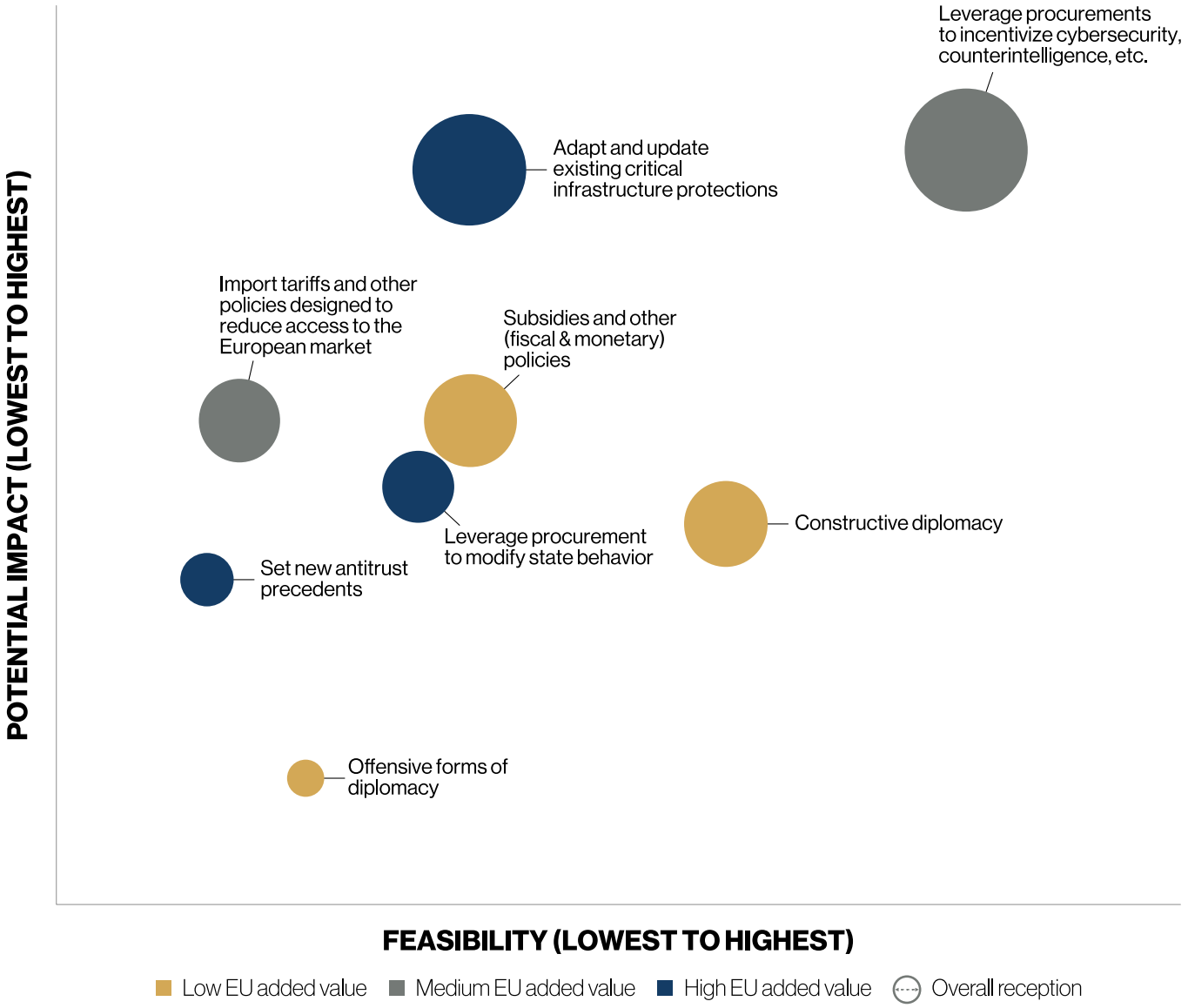


Figure 2 - Survey results: feasibility and potential impact of policy measures

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.

The Hague Centre
for Strategic Studies

Executive Summary

Taming Techno-Nationalism
A Policy Agenda

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

Contributors:
Rob de Wijk, Benedetta Girardi, Sneha Mahapatra

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.

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