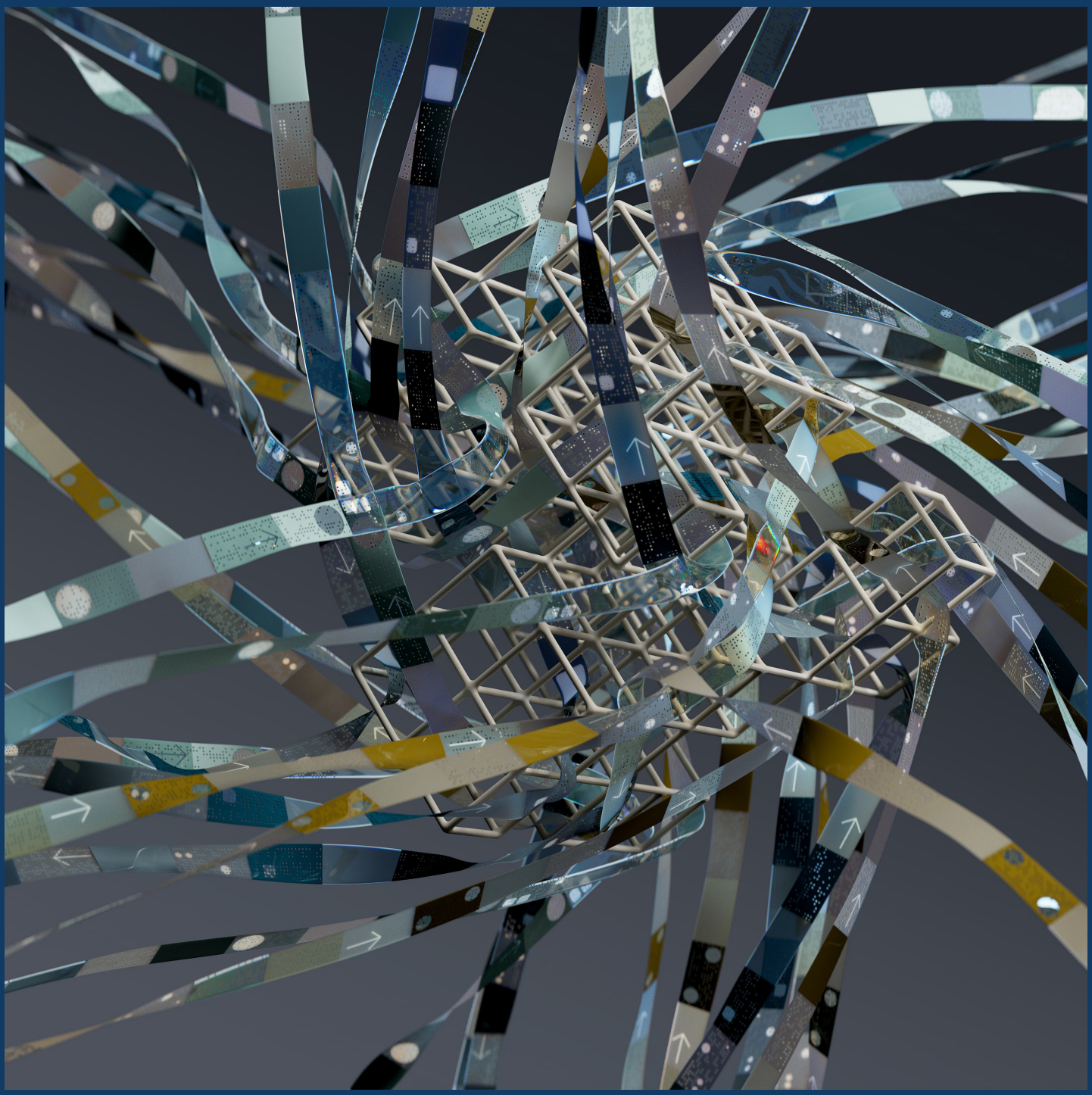
The Hague Centre
for Strategic Studies

Emerging Disruptive Technologies
in an Era of Great Power Competition

Hugo van Manen, Stella Kim, Adam Meszaros and Michal Gorecki

December 2022



The Hague Centre
for Strategic Studies

Emerging Disruptive Technologies
in an Era of Great Power Competition

Authors:
Hugo van Manen, Stella Kim, Adam Meszaros and Michal Gorecki

Contributions by:
Rob de Wijk, Frank Bekkers, Joris Teer and Tim Sweijs

December 2022

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 be construed as, an endorsement by the Netherlands Ministries of Foreign Affairs and Defense.

Table of Contents

Executive Summary

Emerging (and) disruptive technologies (EDTs) play a critical role in generating economic prosperity. But they also generate a bevy of challenges, posing both risks and opportunities, often at the same time. For instance, the way artificial intelligence (AI) is currently employed by social media companies can affect the democratic process. But similar technologies – for example, those used to determine the content of individual posts – can be employed to help create online environments that facilitate inclusive civil discourse and protect against violence incitement. In the case of AI the direction in which the technology is likely to develop, at least within the social media space, depends on what steps lawmakers take to regulate the technology, the companies developing it, and the environments where the technology is employed. In other areas, such as the military and economic domain, the trajectory of the technology's impact on society will largely depend on the degree to which governments can come to agreements that limit AI's acceptable applications.

International cooperation is therefore required but severely hampered by the fact that access to and control over EDTs is increasingly considered to be a zero-sum game. In the current age of interstate rivalry, states are incentivised to leverage the tools at their disposal to expand their access to and control over these technologies to boost their own current and future competitiveness and to undermine that of their adversaries, and also, to some extent, that of their allies. Policy instruments include, but are not limited to, traditional mercantilist practices such as import and export controls, the subsidisation of national champions, laws designed to obligate foreign companies to transfer core technologies, initiatives to revise international technological standards, and even global infrastructure development strategies such as the Chinese Belt and Road Initiative (BRI). A previous HCSS study dating from 2021 considered this phenomenon under the label of 'techno-nationalism'.[1] The current report builds on this study and updates and extends its recommendations.

In the current competitive global environment, Dutch policymakers should seek to reduce the Dutch innovation ecosystem's vulnerability to techno-nationalist practices and to improve its ability to compete internationally, while simultaneously seeking international cooperation to regulate the societal impact of EDTs. The Netherlands has put various forms of long-term funding in place to bolster the productivity of its start-up ecosystem in recent years. However, new legislation must also mitigate Dutch vulnerabilities beyond foreign direct investment (FDI)-based techno-nationalist practises.

This study covers quantum computing, AI, semiconductors, and space-related technologies. These EDTs hold the potential of having (and, in some cases, already have) a broad impact on geopolitics, society and warfare. Some of these EDTs interplay with each other. For example, quantum computing is an avenue for hyper-charging AI-based processes. This has implications for various shifts, such as the erosion of democracy or the transforming of military sensing. EDTs also affect multiple domains. AI applications, for instance, can undermine democratic discourses via their implementation on social media. AI applications can be used to harvest and exploit personal data. They can be employed towards the consolidation of authoritarian models of statecraft. AI applications can furthermore can also be used in

1 Hugo van Manen et al., "Taming Techno-Nationalism: A Policy Agenda," HCSS Progress (The Hague: The Hague Centre for Strategic Studies, September 2021), https://hcss.nl/wp-content/uploads/2021/09/Taming-Techno-Nationalism-Sept.-2021.pdf.

the deployment of autonomous weapon systems and the automated optimisation of military planning and logistics in the short term. The relevance of EDTs in the context of surging interstate competition also brings other concerns to the fore. Semiconductor supply chains, for instance, raise serious concerns regarding Dutch, and European dependence on foreign countries. These chains also have a sizeable environmental footprint, exacerbate global inequalities, and expose workers to toxic compounds during the required mining and refining of critical raw materials (CRM). Space-related technologies, finally, are becoming more and more important for economic prosperity and international and national security. Yet, they are underregulated at the international level, opening the door to competition in and the militarisation of space. The four disruptive technologies and their implications are extensively elaborated on in the Annex to this study.

The threats and opportunities posed by EDTs are enumerated across three dimensions: (1) access to EDTs; (2) warfighting capabilities and EDTs; and (3) the societal impact of EDTs.

The first dimension is primarily geopolitical and geoeconomic. Different countries and regions have unequal access to materials and resources required for the cultivation of EDT development. EDTs are also highly resource intensive. As such, the financial entry barrier into EDT-related sectors is immensely high. This inequity of access to EDTs between various countries and actors is bound to lead to friction within the rules-based international order. Such frictions are further exacerbated by over-optimised 'just-in-time' global supply chains and resulting bottlenecks. The great power rivalry and EDT-related frictions will likely aggravate each other. These developments are likely to drive a process of economic decoupling which ensures security of supply but also removes constraints on competition in the political and military domain. At the same time, for Europe maintaining a strategic edge in the access to and use of EDTs is critical.

The second dimension, warfighting capabilities and EDTs, pertains to the implications of EDTs for the military domain. EDTs allow for ever more autonomous weapon systems to be proliferated and deployed. Similarly, EDTs also empower less sensitive areas, for instance by enabling smarter military logistics. The resulting conundrum is twofold. On the one hand, revisionist actors enhancing their warfighting capabilities via the development of EDTs pose a threat to liberal democracies. Similarly, given these actors' poor human rights track record, the deployment of EDT-empowered capabilities by these actors raises ethical dilemmas. On the other hand, if liberal democracies can successfully harness the warfighting capabilities provided by EDTs, that may contribute to the security of the rules-based order.

The third dimension, the societal impacts of EDTs, addresses the effects of EDTs upon society. For instance, social media, democratic processes, and judicial processes, may all be positively or negatively influenced by EDTs, with a domino effect across various domains. For instance, the echo chamber effect on social media has bearing on democratic processes as well. As such, EDTs pose a threat to liberal democracies by means of populism, disillusionment, and radicalism. However, EDTs may also prove to be a valuable tool for societies to increase resilience. This is notwithstanding systemic rivals' proven reliance on EDTs for social engineering. EDTs may indeed enable autocratic models of statecraft but may also serve as protective checks against the influence thereof. The challenge here will lay in practising restraint and moderation by liberal democracies in harnessing EDTs' possible contributions to safeguarding social cohesion.

The following table summarises the threats and opportunities posed by the four studied EDTs across the three outlined dimensions.

Access to EDTs			
Threat #	**Threat description**	**Opportunity #**	**Opportunity description**
1	Intensification of technology theft	1	Increase in policymaker awareness and understanding
2	Uptick in issue linkage	2	Increase in demand for highly educated individuals
3	Acceleration of China's semiconductor capabilities	3	Support for bolstering applied research capacity
4	Increases in the cost of consumer goods	4	Increases in government funding
5	Tech market fragmentation	5	Increase in amiability for international cooperation
Warfighting Capabilities and EDTs			
Threat #	**Threat description**	**Opportunity #**	**Opportunity description**
6	Overdependence on 3rd countries	6	Increased pressure opens the door to new legislation
7	Adversarial states are likely to gain access independently	7	EDTs offer pathways to cost reductions for military operators
8	Increases in demand for semiconductors	8	Significant operational benefits enabled by EDTs
9	Risk of conflict escalation		
10	Competition incentivises corner cutting during development		
Societal Impacts of EDTs			
Threat #	**Threat description**	**Opportunity #**	**Opportunity description**
11	Alienation and disillusionment on social media	9	Automation of content moderation and "deep fake" detection
12	Democratisation and proliferation of convincing "deep fakes"		
13	Cementing of authoritarian governance models abroad	10	Judicial cost reductions as a result of automation
14	Biases in judicial automation processes		

The Dutch ability to meet challenges posed by EDTs is served by awareness and understanding of EDT-related issues among policymakers and society. This will be key to spearhead and support the creation of national and international regulatory frameworks geared towards governing acceptable use. A short overview of why these policy goals matter, and what can be envisaged as possible solutions, is provided in the bullets below. A much more detailed set of recommendations is provided in Chapter 4 of the report.

1. **Mitigate the vulnerability of Dutch and EU markets.** Dutch and EU markets, despite the introduction of several promising pieces of regulation, remain highly vulnerable to techno-nationalist measures taken by other states. The Netherlands ought to implement more

robust and more comprehensive regulatory frameworks to mitigate the negative impacts of espionage, cybercrime, and various forms of technology theft. The mitigation effort would include reviewing aspects of the Investments, Mergers and Acquisitions Safety Assessment Act (VIFO).

2. **Bolster the competitiveness of Dutch and EU markets.** Adapting to mounting interstate rivalry entails increasing the resilience of the Dutch innovation ecosystem to techno-nationalist foreign practises. Realising an internationally competitive innovation ecosystem would provide the Netherlands with secure access to more Dutch and international talent, transposing theoretical research into real-world use cases, and generating the revenues necessary for cutting-edge research and development (R&D). A necessary step would be the deepening of engagement with mechanisms such as the European Defence Agency (EDA), the Permanent Structured Cooperation (PESCO), and the European Defence Fund (EDF). The Netherlands and Europe should continue doubling down on their support for the semiconductor industry and invest in sensitive technologies. The strengthening of advanced democracies' technological edge in the semiconductor ecosystem could entail active conversation with the semiconductor sector, the mobilisation of Dutch, European, and institutional funds, the allocation of tax incentives, the fast-tracking of fab construction in the Netherlands and the EU, the expansion of pre-competitive research funding for the semiconductor and critical raw material value chains, the cultivation and attraction of students and talent related to EDTs by means of selective visa liberalisation, and the promotion of the science, technology, engineering, and math (STEM) fields. Similar measures to the ones listed above can be extrapolated onto EDTs at large.

3. **Enhance awareness and understanding of EDT-related issues.** The formulation of effective regulatory frameworks on issues surrounding techno-nationalism and negative societal and military impacts of EDTs is contingent on a deep understanding of how these technologies work and what their real-world use cases are. Improving key stakeholders' including lawmakers' awareness and understanding of EDT-related topics will allow for the introduction of more effective legislation. On the level of policy, such measures should include the implementation of incentives to attract human capital also to the public sector. Additionally, the expansion and subsidisation of existing state-funded research commissions such as the Analysis and Research Service (DAO) or the Digital Affairs Committee (DiZa) could serve as an effective framework for the endeavours outlined here.

4. **Reduce overreliance on East Asia within semiconductor supply chains.** A key challenge facing not only Dutch consumers but also the supply chains underpinning the Dutch Armed Forces' warfighting capability, is the country's continued reliance on the Taiwan Semiconductor Manufacturing Company (TSMC). This renders the Netherlands vulnerable not only to supply chain disruptions that might occur because of geopolitical events (for example, a Chinese maritime blockade or invasion of Taiwan) but also to supply and demand dynamics outside its control. These challenges can be mitigated by increasing domestic and regional production capacity. The recent US and European Chips Acts or the Dutch Ministry of Economic Affairs and Climate's (EZK) Early 2022 application for a €230 million subsidy package for R&D projects may serve as relevant precedents and potentially as frameworks for this endeavour.

5. **Support the creation of national and international regulatory frameworks.** A significant share of the risks associated with EDTs can be tied, whether directly or indirectly, to lacking (or consciously ignored) guard rails during the development process of EDTs. This can, in turn, be attributed to an inept international regulatory environment as a by-product

of interstate rivalry. The creation of national and international frameworks to regulate EDTs, the standards they should meet before being employed within military and domestic contexts, and the use cases they should and should not be employed for, will go a long way towards mitigating these risks. Such multilateral or minilateral agreements should address various levels of regulation with different applications on each level. As such, this report breaks down proposed regulations on EDTs on the domestic, regional, international, and commercial levels respectively for each of the four EDTs at hand.

6. **Enact Dutch and European legislation regulating social media platforms.** Much of AI's and potentially quantum computing's negative impacts on the democratic process can be attributed to shortcomings on part of states in regulating social media platforms. There is a wide range of policy options available for reducing the threat posed by misinformation online, some of which the Netherlands has yet to implement. Examples include privacy protection, filtering out deep fakes, and banning algorithms that primarily show the user upsetting content. These measures would mitigate the echo-chamber effect, and thereby curb the impacts of disillusionment and radicalisation.

7. **Facilitate the development of European champions and coalitions of the willing.** The geopolitical hazards stemming from EDT-related risks are exacerbated by incomplete domestic efforts to optimise for resilience. These effects could in turn be mitigated by integration efforts of the military and civilian spheres, subsidisation and incentivisation of European champions and close monitoring of EDT-adjacent activities by coalitions of these actors. This will also strengthen Europe's position at a time when allies such as the US are implementing protectionist policies and putting pressure on European economies to adhere to its policies. The Netherlands could cement the strategic leverage derived from their unique role in semiconductor supply chains through deepened cooperation with bottleneck companies such as ASML as well as with dominant but non-bottleneck companies in that sector such as NXP. In turn, forming coalitions of the willing on the European and on the Transatlantic levels between state actors and industry champions could allow for a strengthened strategic posture against revisionist systemic rivals. Finally, the deepening of integration between the civilian and military spheres on EDT-related issues carry the twofold benefit of enhancing both military capabilities via EDTs and socio-economic resilience to EDTs.

These recommendations should become prominent objectives for Dutch and European policymakers. The geopolitical situation is tense and displaying a straightforward message: the alarm bells have gone off, the time to act is now.

List of abbreviations

EDT – emerging (and) disruptive technologies

AI – artificial intelligence

BRI – Belt and Road Initiative

FDI – foreign direct investment

CRM – critical raw materials

VIFO – Mergers and Acquisitions Safety Assessment Act

R&D – research and development

EDA – European defence Agency

PESCO – Permanent Structured Cooperation

EDF – European Defence Fund

STEM – science, technology, engineering, and math

DAO – Analysis and Research Service

DiZa- Digital Affairs Committee

TSMC – Taiwan Semiconductor Manufacturing Company

EZK – (Dutch) Ministry of Economic Affairs and Climate

EC – European Council

NATO – North Atlantic Treaty Organisation

FAC – Foreign Affairs Council

DSA – Digital Services Act

DMA – Digital Markets Act

GDPR – General Data Protection Regulation

JCER – Japan Center for Economic Research

REE – Rare Earth Elements

DRC – Democratic Republic of the Congo

IP – intellectual property

SIGINT – signals intelligence

KPI – key performance indicator

CFI – Committee for Foreign Investment

BTI – Investment Review Office

VC – venture capital

IPCEI – Important Projects for Common European Investment

NGF – National Growth Fund

SKIA – Strategic Knowledge and Innovation Agenda

RoI – return on investment

ECD – European Copyright Directive

EuroQCI – European Quantum Communications Infrastructure

SMEs – small and medium enterprises

WEF – World Economic Forum

IEEE – Institute of Electrical and Electronics Engineers Standards Association

ISO – International Standardisation Organisation

EEAS – European External Actions Service

ESA – European Space Agency

3SOS – Safety, Sceurity and Sustainability of Outer Space

UNOOSA – United Nations Office for Outer Space Affairs

ISP – internet service provider

NEA – Network Enforcement Act

PAC-2 GEM-T – Patriot Advanced Capability Guidance Enhanced Missile

1. Introduction

Emerging (and) disruptive technologies (EDTs) are an important consideration for Dutch and EU policymakers. They play a critical role in generating economic prosperity and in revolutionising military technology. Conversely, their development – and societal role at large – poses a bevy of challenges. Though a significant share of these challenges amounts to outright risks, many of them can, if addressed effectively, be harnessed as opportunities. For instance, the way artificial intelligence (AI) is currently employed by social media companies undermines the democratic process. The collection of personal data and user preferences, automated profiling of individuals into clusters of distinct personality types, and utilisation of said clusters to serve targeted advertising and promote inflammatory content facilitates the spread of misinformation and leads to the creation of echo chambers. But similar technologies – for example, those used to determine the content of an individual post – can also be employed to automate the moderation of social media, helping create inclusive online environments that facilitate productive civil discourse.

In the case of AI, the direction in which the technology is likely to develop, at least within the social media space, depends entirely on what steps lawmakers take to regulate the technology, the companies developing it, and the environments where technology is employed. In other domains, such as the military, ethical, and economic domains, the trajectory of the technology's impact on society will depend on the degree to which nation-states can come to agreements that limit its acceptable applications. Reaching agreements such as these may contribute, among others, to preventing the (further) development and proliferation of autonomous weapons systems, limiting the scope of states' ambitions regarding the militarisation of space, and complicating the export of sensors and technologies that might be used to facilitate authoritarian governance models.

International cooperation is therefore required, but severely hampered by the fact that access to and control over EDTs is increasingly considered to be a zero-sum game. In the current age of interstate rivalry, states are incentivised to leverage the tools at their disposal to expand their access to and control over these technologies to boost their own current and future competitiveness and to undermine those of their adversaries– and, up to a point, also those of their allies. This holds that international agreements must be considered in light of current efforts to increase Europe's "strategic autonomy". Strategic autonomy has, within the European context, been associated with "digital" and "technological" sovereignty. Digital sovereignty "refers to Europe's ability to act independently in the digital world and should be understood in terms of both protective mechanisms and offensive tools to foster digital innovation (including in cooperation with non-EU companies)."[2] It has now taken on a broader meaning. The European Council (EC) first cited some variation of the concept in relation to the EU's defence industry in 2013, when the Obama Administration withdrew some 7,000 combat troops from Europe.[3] The sentiment that the US commitment to guaranteeing European security was wavering has been reaffirmed by its subsequent pivot to Asia and the pressures

2 Tambiama Madiega, "Digital Sovereignty for Europe" (European Parliamentary Research Service, July 2020), p. 1, https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf.

3 Daniel Dombey, "Obama to Recall US Troops from Europe," Financial Times, April 9, 2011, https://www.ft.com/content/23852314-6236-11e0-8ee4-00144feab49a; "US to Withdraw Two Europe Combat Brigades," BBC News, January 13, 2012, sec. US & Canada, https://www.bbc.com/news/16543456.

placed upon the North Atlantic Treaty Organisation (NATO) alliance under the Trump Administration.[4] These developments led the Foreign Affairs Council (FAC) to use the phrase "strategic autonomy" in 2015, as well to the EC and the European Commission citing it in official policy documents from 2016 onwards.[5]

Recent years have seen this logic linked to sensitive technologies more explicitly. In a 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".[6] Dutch and Spanish officials have argued that the EU must "become more technically and digitally sovereign,"[7] a sentiment which has since been echoed by Paris and Berlin.[8] Combined with pieces of legislation such as the Commission's recently updated industrial and digital strategies, the Digital Services Act (DSA),[9] the Digital Markets Act (DMA),[10] the Cybersecurity Strategy,[11] and the General Data Protection Regulation (GDPR),[12] these statements have served to institutionalise the notion that digital and technological "sovereignty" refer to the EU's ability to maintain independent ownership over and mastery of a predefined list of key (sensitive) technologies and to ensure their application in ways that are consistent with EU values.[13] Russia's war against Ukraine only provided further impetus to efforts within the EU to become more of a geopolitical actor in its own right.

This report sets out to address the questions of what the Netherlands and the EU can do to tackle the challenges associated with EDT's continued development and to advise policymakers on how to strengthen the position of the Netherlands and the EU in this realm. The methods employed in this endeavour were informed by and expanded upon a previous report

4 Peter Baker, "Biden Plays the Long Game as He Justifies the End of the 'Forever War,'" The New York Times, September 1, 2021, sec. U.S., https://www.nytimes.com/2021/08/31/us/politics/biden-politics-afghanistan.html.

5 Josep Borrell, "Why European Strategic Autonomy Matters," European Union External Action, December 3, 2020, https://www.eeas.europa.eu/eeas/why-european-strategic-autonomy-matters_en.; "A Strategic Compass for Security and Defence: For a European Union That Protects Its Citizens, Values and Interests and Contributes to International Peace and Security" (Council of the European Union, March 21, 2022), https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf.

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

7 Ministerie van Buitenlandse Zaken, "Non-Paper on Strategic Autonomy While Preserving an Open Economy," The Netherlands at International Organisations (Ministerie van Buitenlandse Zaken, March 24, 2021), https://www.permanentrepresentations.nl/documents/publications/2021/03/24/non-paper-on-strategic-autonomy.

8 "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.

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

10 European Commission, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Contestable and Fair Markets in the Digital Sector (Digital Markets Act)" (Brussels: European Commission, December 15, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX-:52020PC0842&from=en.

11 "The Cybersecurity Strategy," European Commission, n.d., https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy.

12 "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)" (Strasbourg: European Parliament, May 4, 2016), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX-:02016R0679-20160504&from=NL.

13 "Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: A New Industrial Strategy for Europe" (Brussels: European Commission, March 10, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0102&from=EN.

of HCSS, titled 'Taming Techno-Nationalism: A Policy Agenda'.[14] That publication undertook extensive interviews with various Dutch subjects. The present research expanded on 'Taming Techno-Nationalism' with further extensive desk research, consultations with policymakers, and expert assessment. The present report proceeds as follows:

- Chapter 2 provides a concise overview of the role that competition over access to technology has played in shaping geopolitics in recent years.
- Chapter 3 then examines threats and opportunities associated with the following EDTs: quantum computing, AI, semiconductors, and space-related technologies. It considers (1) access to EDTs; (2) warfighting capabilities and EDTs; and (3) the societal impact of EDTs. The examination is based on detailed assessments of their ethical, judicial, democratic and military impact, which are included in the annex.
- Chapter 4 offers recommendations for meeting the challenges posed by EDTs head-on.
- The Annex offers detailed assessments of the ethical, judicial, democratic and military impact of the four EDTs.

International cooperation is therefore required, but severely hampered by the fact that access to and control over EDTs is increasingly considered to be a zero-sum game.

14 van Manen et al., "Taming Techno-Nationalism: A Policy Agenda."

2. The Geopolitics of Emerging Disruptive Technologies

History shows that the country that becomes the champion of an industrial revolution will emerge as the hegemon of the world.

EDTs are at the centre of geopolitical strife. History shows that the country that becomes the champion of an industrial revolution will emerge as the hegemon of the world. It happened to Great Britain in the 19th century and to the United States in the 20th century.[15] By setting global technological standards, emerging industries were able to make a huge contribution to strengthening the country's economic base. Subsequently, both Great Britain and the United States used their economic dominance for enhancing their global political influence and expeditionary military power, along with their power projection capabilities on the maritime commons. These factors in turn rendered their strategic posture into global hegemons.

The new industrial revolution is a data revolution that focuses on 5G and 6G, the Internet of Things, robotics, and the application of AI. It will not only revolutionise our economies and the way we live but also the relations between countries if China becomes the champion of this revolution.

China has a fair chance of becoming the world's dominant economy. For China, the size of its population is a marked advantage. Its reservoir of highly skilled workers is much bigger than that of the West. The *Times Higher Education World University Rankings 2023* revealed that the top entries in the global ranking are now shifting away from the West. China now has an unprecedented seven universities in the world's top 100– up from six last year and just two five years ago.[16]

In the 21st century, from a European perspective, there is arguably more at stake than in preceding centuries. Following the Second World War, the position of global hegemon shifted from Great Britain to the United States. As such, the hegemon remained a western power. If China emerges as the new hegemon, Beijing will then be able to challenge the world order that was created by the British and the Americans after the end of the Second World War. The present system is founded on Western values, principles, and interests. The (neo)liberal world order is based on liberal economic policies, international law, international institutions, and values such as democracy, human rights and individual liberties. The survival of this system depends on the preferences of the new champion of the data revolution, the way it wants

15 John Lukacs, A Short History of the Twentieth Century (Cambridge, Massachusetts: The Belknap Press of Harvard University Press, 2013), 3, file:///C:/Users/AdamMeszaros/Downloads/A%20Short%20History%20of%20the%20Twentieth%20Century%20(John%20Lukacs)%20(z-lib.org).pdf.

16 "World University Rankings," Times Higher Education (THE), October 4, 2022, https://www.timeshighereducation.com/world-university-rankings/2023/world-ranking.

to strengthen its economic base and the way it wishes to exploit the changes in the global power distribution.

As a state capitalist autocracy, one might expect that China's leaders will promote an anti-liberal policy based on mercantilism, zero-sum and transactional thinking. Protectionism, techno-nationalism and the use of raw materials as instruments of coercion are part of the toolkit for protecting the domestic industrial base. As both the US and the EU have created formidable obstacles, the focus of major companies like Huawei and ZTE is now shifting to the global south. Through the new 'Silk Roads', the Belt and Road Initiative (BRI), China tries to foster close economic relations with other parts of the world that can be turned into political influence. Through the BRI, a group of countries is emerging that share Beijing's view that the world should be 'de-westernised'. A digital side-route ensures that these countries become more and more dependent on the products of the data revolution. So far, only the most vulnerable countries are willing to foster those close ties with China.

The new industrial revolution is a data revolution that focuses on 5G and 6G, the Internet of Things, robotics, and the application of AI.

Western governments are increasingly aware of the consequences of the relative decline of the West. They understand that they are in fierce competition with a 'systemic rival' and understand that they need to safeguard their interests. The international rule of law is now challenged by China's rise. History shows that those global power shifts cause political and economic frictions and may ultimately result in war. The friction between the US and China across the South China Sea and Taiwan, which is the main semiconductor supplier, fits into the picture of the mounting tensions caused by global power shifts. It also applies to the war that Russia started against Ukraine. Putin estimated that due to their relative decline in power, the West would not be able to hit back hard.

In a sense, the West is already involved in a global economic war. It is important to make a clear distinction between sanctions and economic war. Sanctions are essentially restrictions on economic flows aimed at changing the target's behaviour. Economic warfare is the use of, or the threat to use, economic means against a country to weaken its economy and thereby reduce its political and military power. Sanctions targeted at China and Russia are part of economic warfare aimed at weakening their position. Regarding Russia, US Secretary of Defence Lloyd Austin was clear when he stated that "we want to see Russia weakened to the degree that it can't do the kinds of things that it has done in invading Ukraine."[17] Regarding China, President Trump launched a trade war to punish Beijing for what he considered unfair Chinese trade practices, including forced technology transfer, limited market access, intellectual property theft, and subsidies to state-owned enterprises. Behind this was the belief that China's rise must at least be slowed down so that the US has sufficient time to take measures to strengthen its position vis-à-vis China.

By focusing on China's high-tech industry, most notably Huawei and ZTE, Trump showed clearly that the rise of China was mainly a derivative of the success that the country would achieve in the new industrial revolution. President Biden did not alter Trump's course. On the contrary, he sought support from the US' allies in Europe and in the Indo-Pacific. Due to the scale of the challenge, we see countries increasingly cooperating. This resulted, among other things in the EU-US Trade and Technology Council, the EU-India Trade and Technology Council and the EU-Taiwan Trade and Investment Dialogue. Moreover, the Biden administration has pressured the Dutch ASML, one of the most critical companies in the semiconductor

17 Matt Murphy, "Ukraine War: US Wants to See a Weakened Russia," BBC News, April 25, 2022, sec. Europe, https://www.bbc.com/news/world-europe-61214176.

supply chain, to halt selling lithography systems to China.[18] This move aims to restrict China's access to advanced semiconductor manufacturing equipment.[19]

The effects of economic warfare have become visible. According to the Tokyo-based Japan Center for Economic Research (JCER), China will overtake the US as the largest economy only in 2033.[20] Earlier predictions mentioned the second half of the 2020s. Except for American economic coercion, China's zero covid policies and the collapse of the property developer Evergrande also played a role in the stagnation of China's rise. And between the autocratic rule of Xi Jinping and his political agenda and the declining Chinese work force, doubts rise whether China will overtake the US at all.[21]

Now that China is being challenged economically, we also see its leadership taking counter-measures, often in cooperation with like-minded countries, including Russia.

The Ukraine war revealed that trade will not necessarily lead to interdependencies as a stabilising factor.

For the West, a key challenge is the need for critical raw materials (CRM), oil and natural gas supplied by 'systemic rivals' and autocracies with questionable track records in the fields of human rights, working conditions and environmental issues that are willing to use those commodities as political instruments of coercion. Russia is a case in point. President Putin started to use raw materials, energy, and food as coercive instruments against the West. The Ukraine war revealed that trade will not necessarily lead to interdependencies as a stabilising factor. Before the Russian intervention in Ukraine, the US relied on Ukraine for 90% of its semi-conductor-grade neon. Moreover, the American semiconductor industry relied on Russia for 35% of its Palladium imports. In turn, Russia bought 70% of its chips in China, but China itself was denied access to the most advanced semiconductors.

To make matters even more complicated, the mining, refining, conversion, and processing of Gallium, Palladium, Rare Earth Elements (REE), Cobalt, and Germanium are dominated by China, Russia, and the Democratic Republic of the Congo (DRC) while the suppliers of tools and machines to produce semiconductors and the manufacturing of chips itself takes place in the advanced economies of the EU, the US and Taiwan.[22] Without raw materials, semiconductors cannot be produced. As the production of semiconductors is part of a global supply chain, China and Russia can easily disrupt the production process. The vulnerability of global supply chains for the manufacturing of semiconductors requires a completely different approach from the one followed by national governments, one that is based on the acknowledgement of unhealthy interdependencies and the acceptance of pragmatic policies to prevent further disruptions of the supply chains. For industries, this means that geopolitical

18 Tim Culpan, "US Chip Pressure on ASML Is a Tough Sell," Bloomberg, July 6, 2022, https://www.bloomberg.com/opinion/articles/2022-07-06/us-chip-pressure-on-asml-over-china-is-a-tough-sell; Arjun Kharpal, "Globally Critical Chip Firm Tells U.S. Staff to Stop Servicing China Customers after Biden Export Curbs," CNBC, October 13, 2022, https://www.cnbc.com/2022/10/13/biden-chip-curb-asml-stops-us-staff-from-servicing-customers-in-china.html.

19 Kharpal, "Globally Critical Chip Firm Tells U.S. Staff to Stop Servicing China Customers after Biden Export Curbs."

20 "China to Become the World's Largest Economy in 2033," Medium-Term Forecast of Asian Economies - Summary (Japan Center for Economic Research, December 15, 2021), https://www.jcer.or.jp/jcer_download_log.php?f=eyJwb3N0X2lkIjo4NjQyMywiZmlsZV9wb3N0X2lkIjoiODY0MzMifQ==&post_id=86423&-file_post_id=86433.

21 https://www.bloomberg.com/news/newsletters/2022-05-27/us-could-finally-beat-china-s-xi-in-gdp-growth-race

22 Joris Teer and Mattia Bertolini, "The Semiconductor and Critical Raw Material Ecosystem at a Time of Great Power Rivalry," HCSS Progress (The Hague: The Hague Centre for Strategic Studies, October 2022), https://hcss.nl/wp-content/uploads/2022/10/Reaching-breaking-point-The-semiconductor-and-critical-raw-material-ecosystem-at-a-time-of-great-power-rivalry-October-2022-Full-Version.pdf.pdf.

due diligence and understanding of the global flows of commodities should be part of the strategy-making process.

The conclusion is that interdependencies that were always considered to be mutual interests and would contribute to peace and prosperity have come under fire. Already before the Russian invasion of Ukraine, President Biden ordered the review of US reliance on overseas supply chains, in particular REE. The order did not mention China, but it is clear that China has a more than 90% share of the global production of downstream rare earth products and technologies. Also, the EU took the initiative to secure its future economic base by becoming less dependent on too few suppliers for raw materials and semiconductors as part of a broader 'open strategic autonomy' initiative. The West and China strive for improving their respective capabilities in quantum computing – exemplified by an increase of over 100% in investments in quantum computing between 2020 and 2021.[23] In addition, the EU announced three joint quantum research projects with Canada, and the ambitions to develop the Union's first quantum computers in six Member States.[24] On the AI-front, there has been significant progress as well. For instance, in 2019, 35 states announced their national AI strategies, whereas, in 2020, their number rose to 50.[25] The competition has also been intense in outer space. In May 2020, the US drafted the Artemis Accords, teaming up with another 20 states, mainly allies and partners, laying out principles for exploration and use of space, which was received with hostility in Moscow and Beijing.[26] Cooperation with like-minded countries is now more important than ever.

Protectionism, techno-nationalism and the use of raw materials as instruments of coercion are part of the toolkit for protecting the domestic industrial base.

This study focuses on EDTs that are extremely vulnerable to techno-nationalism practices. We're only at the beginning of a fundamental debate on future supply chains, closer cooperation with like-minded countries and strategic autonomy. This study aims at contributing to the discussion on how to mitigate the vulnerability of our future economic base.

23 Mateusz Masiowski et al., "Quantum Technology Monitor" (McKinsey & Company, June 2022), https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/quantum%20computing%20funding%20remains%20strong%20but%20talent%20gap%20raises%20concern/quantum-technology-monitor.pdf.

24 "Quantum," European Commission, n.d., https://digital-strategy.ec.europa.eu/en/policies/quantum; "Joint EU/Canada Quantum Research Projects," European Commission, October 6, 2022, https://digital-strategy.ec.europa.eu/en/news/joint-eucanada-quantum-research-projects.

25 "The Global AI Strategy Landscape," Holon IQ, April 25, 2019, https://www.holoniq.com/notes/the-global-ai-strategy-landscape; "50 National AI Strategies - The 2020 AI Strategy Landscape," Holon IQ, February 20, 2020, https://www.holoniq.com/notes/50-national-ai-strategies-the-2020-ai-strategy-landscape.

26 Elliot Ji, Micheal B. Cerny, and Raphael J. Piliero, "What Does China Think About NASA's Artemis Accords?," The Diplomat, October 17, 2020, https://thediplomat.com/2020/09/what-does-china-think-about-nasas-artemis-accords/.

3. Threats and Opportunities of Emerging Disruptive Technologies

The rising prominence of EDTs' poses various challenges globally. Great power rivalry in turn endangers liberal democracies' ability to ensure EDTs' ethical entry into various domains. EDTs pose threats to supply chains, social stability, democratic processes, and military strategic posture. That said, if harnessed in an informed manner, EDTs may also provide solutions for safeguarding these. As such, the present section enumerates EDT-related threats and opportunities across three dimensions, which are outlined below:

- **Access to EDTs.** The first section in which threats and opportunities are offered in this chapter concerns *access to EDTs*. A combination of techno-nationalist policies on the part of nation-states and shortcomings in the equity of open market mechanisms and (to a lesser extent) supply chain structures means that these technologies are subjected to race-to-the-bottom mechanics in their development and that the benefits of accessing them are unevenly distributed at the international level. The *access to EDTs* section explores the threats and opportunities associated with competition over technology, outlining the strategic and economic implications for the Netherlands, as well as the concrete (short-term) effects that currently unfolding competition (over, for example, semiconductors) is likely to have on Dutch consumers.
- **Warfighting Capabilities and EDTs.** The second section for which threats and opportunities are offered in this chapter deals with warfighting capabilities and EDTs. Based on the findings presented within the context of military domain-level observations, this section provides an overview of how EDTs are likely to impact the character of and the strategic thinking underpinning warfare going forward.
- **Societal Impacts of EDTs.** The third and final section for which the threats and opportunities posed by EDTs are offered deals with societal issues. Whether due to the way they are manufactured, the circumstances surrounding their development, or the use cases they enable, EDTs can – in many cases already do – have profoundly negative impacts on (among others) the right to free speech, the right to legal counsel, access to clean drinking water, and right to life. They can also negatively impact the democratic and judicial processes. The section describes the threats and opportunities associated with EDTs' impact on norms and values and democratic and judicial processes.

EDTs in turn pose these threats and opportunities along four distinct but interplaying domains: judicial, democratic, ethical, and military. A comprehensive overview of EDT-related challenges broken down along these domains is provided in the Annex. Moreover, the Annex also provides an in-depth explanation of what each of the four EDTs studied in this report – (1) quantum computing, (2) AI, (3) semiconductors, (4) and space-related technologies respectively – exactly entail.

3.1. Access to Emerging Disruptive Technologies

Access to the use cases – and economic and military advantages – unlocked by EDTs is a major driver of geopolitical competition and something which has contributed to a pronounced uptick in techno-nationalist policies in recent weeks, months, and years. The unequal distribution of these technologies also results in major wealth and welfare discrepancies between "haves" and "have-nots" at the international and, to a lesser extent, domestic levels. Looking ahead, there exists a very real risk that these trends will intensify. This means that techno-nationalist sentiments, and state reliance on techno-nationalist practices, are likely to (continue) impact Dutch and EU economic prosperity over the next five years, due in no small part to intensifying competition between the US and China. It also means that the gap between "haves" and "have-nots" is likely to widen in the coming years.

Competition over access to EDTs 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.

Competition over access to EDTs 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. 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,[27] as well as Ursula von der Leyen's[28] 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.[29] The proliferation of techno-nationalist sentiments brings with it both threats and opportunities.

Threats include, but are not limited to, an increase in the market pressure faced by Dutch technology firms, an uptick in issue-linkage to technology-related issues within diplomatic circles, the acceleration of China's ongoing efforts to compete on semiconductor manufacturing, a rise in the cost of consumer electronics, and fragmentation in international tech markets. Opportunities include the emergence of more agile and well-informed legislative processes, an increase in the international demand for highly skilled individuals, a renewed focus on the urgency of transposing Dutch theoretical research into real-world applications, and an increase In the amiability of potential partners.

Threats associated with an uptick in techno-nationalism stem almost universally from the fact that techno-nationalist policies result in the politicisation of innovation, erode the functioning of free and open market mechanisms, and undermine competition. As states continue to engage in – and, in many cases, deepen their engagement in – techno-nationalist practices, the Dutch innovation ecosystem is likely to come under increasing pressure. One obvious

27 European Commission, "Proposal for a 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" (Brussels: European Commission, April 21, 2021), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

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

29 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 the Tech War It Just Started," Foreign Policy (blog), January 16, 2020, https://foreignpolicy.com/2020/01/16/europe-technology-sovereignty-von-der-leyen/.

Threats associated with an uptick in techno-nationalism stem almost universally from the fact that techno-nationalist policies result in the politicisation of innovation, erode the functioning of free and open market mechanisms, and undermine competition.

form of pressure that the Netherlands and its innovation ecosystem might face is an uptick in initiatives intended to transfer (control over) key intellectual property (IP) and/or manpower, whether through legal (acquisition-based) or illicit (theft or espionage), away from Dutch entities. Simultaneously, as states double down on investments into national champions, the Netherlands is likely to need to contend with the introduction of localisation barriers to trade intended to keep Dutch firms and technologies from competing. The introduction by the US of a tax credit which incentivises consumers to purchase American-made electric cars that use American-made batteries constitutes an example of such an trade barrier.[30] The introduction of these policies – which amount, in many cases, to conscious efforts on the parts of national governments to silo off (and, by extension, fragment) their technology markets – will have a negative financial impact on the Dutch innovation ecosystem, undermining its ability to compete and to continue investing in research and development (R&D) activities. A doubling down on support for national champions and techno-nationalism is also likely to result in an acceleration of China's ability to manufacture semiconductors at scale. This will serve not only to increase the likelihood of a conflict breaking out between China and Taiwan but also to require the Dutch government to take active measures to avoid its economy growing dependent on Chinese fabs for semiconductors. This challenge is likely to be made more difficult by increases in the cost of many consumer technology items. Scenarios such as the US' recent diplomatic push to preclude ASML from selling chipmaking gear to Chinese manufacturers are likely to become more commonplace,[31] with the practice of issue-linking technology-related policy questions to other domains (economic, military, societal, etc.) being set to grow wider.

Opportunities associated with an uptick in techno-nationalism can generally be conceptualised as stemming from the same factors. Put simply, the politicisation of innovation, erosion of the functioning of free and open market mechanisms, and the undermining of competition are likely to increase the pressure on national governments – the Dutch government included – to put policies in place that increase the productivity of national innovation ecosystems, reduce the costs and impact of dependency on foreign technology providers, and mitigate EDTs' negative impact on society. With this in mind, the first opportunity that is likely to manifest as a result of an uptick in techno-nationalism has to do with policymaker awareness of technology-related issues. As the real-world impacts of techno-nationalism (increased prices, etc.) start to impose themselves on consumers, the likelihood is high that the democratic process will facilitate the emergence of a more tech-oriented political class. This, in turn, is likely to result in the inclusion of more subject matter experts in government advisory and research councils, allowing for the introduction of comprehensive and thoughtful legislation. Increased attention to antitrust-related initiatives is one of the areas in which clear progress is likely to be registered in the short-medium term. The Netherlands is also likely to benefit from its robust education system. An uptick in techno-nationalist sentiment will drive aggressive hiring within the tech sector, creating employment opportunities for thousands of Dutch students and allowing many to, in the medium-long term, to rise to positions of influence within the industry. The Dutch government will need to put policies in place to ensure that sufficient numbers of individuals find careers in innovation in the Netherlands, a goal that is likely to be met – at least in part – through increased government funding for applied research. Because many EU Member States will find themselves in similar predicaments to the Netherlands, the space

30 Andrew J. Hawkins, "Foreign Automakers Are Big Mad about the New EV Tax Credit," The Verge, August 26, 2022, https://www.theverge.com/2022/8/26/23323115/ev-tax-credit-foreign-automaker-hyundai-wto-discriminate.

31 Jillian Deutsch, Eric Martin, and Debby Wu, "US Wants Dutch Supplier to Stop Selling Chipmaking Gear to China," Bloomberg.Com, July 5, 2022, https://www.bloomberg.com/news/articles/2022-07-05/us-pushing-for-asml-to-stop-selling-key-chipmaking-gear-to-china.

for coalition building and introducing legislation at the EU level, is set to increase. This means that, in time, the Netherlands is likely to find relative autonomy and insulation from international tech-related shocks as a result of its EU memberships and the benefits associated with its participation in the EU's open market.

The threats and opportunities associated with the access section are shortly outlined in the bullets below.

Threats

1. Intensification of technology theft in the short term, with the result being an increase in the (market) pressures faced by Dutch and EU technology firms in the medium-long term.
2. Uptick in the degree to which major allies, and the US most prominently, link technology-related issues to other policies. This may result in an increase in Dutch and EU dependence on US technology suppliers in the short term, undermining chances (and increasing the entry cost) of developing competing technologies in the medium-long term. This undermines strategic autonomy and makes it harder to achieve.
3. Acceleration in Chinese efforts to develop and erect foundries capable of fabricating complicated semiconductors. Chinese fabs may have play a role in allowing Russia to avoid the full (negative) impact of US and EU sanctions, and are likely to continue doing so in the medium-long term.
4. Increase in the cost of many consumer goods, including popular consumer electronics (smartphones, laptops, etc.). Fears of a Chinese maritime blockade or invasion of Taiwan – and the chilling effect of techno-nationalist practices on (among others) capital investments into technology firms – will, particularly when combined with bottlenecks in semiconductor supply chains, continue to drive up the prices of many consumer goods. This is likely to exacerbate the negative effects of inflation.
5. Widespread perception of techno-nationalist practices being employed drives more and more states to act in a similar fashion. This will not only increase the pressure on Dutch and EU educators and start-ups; it will also create fragmentation at the international level, with "preferred" technology vendors likely emerging in many of the world's regions. This, in turn, will reduce market exploitation opportunities for Dutch and EU firms, necessitating increased public-sector engagement.

Opportunities

1. An uptick in techno-nationalism increases policymakers' understanding of critical technologies and (in many cases) alerts consumers to the downsides of monopiles and, by extension, techno-nationalist practices in the tech space. This creates a political and economic climate for introducing robust antitrust legislation, something which will facilitate market competition and, in all likelihood, result in strong innovation. Because these sentiments are present both in the US and in the EU, there is space – US elections allowing – for cooperation and streamlining on these issues between these economies. This will reduce the techno-nationalist "threat" the US poses to the EU.
2. An uptick in techno-nationalism is likely to increase demand for highly-educated individuals, something which – particularly in the Dutch case – is likely to contribute to stimulating the economy. Brain drain is a problem the Netherlands has long faced in its tech sector, but increased demand for highly skilled workers is nonetheless likely to result in increased foreign direct investment (FDI), particularly if the Netherlands can (successfully) position itself as one of Europe's most productive innovation ecosystems.

3. An uptick in techno-nationalism offers opportunities for addressing the much-lamented gap between the productivity of the Dutch theoretical and applied research trajectories. Increases in the FDI flowing into the country, combined with a renewed sense of urgency around the need for strategic autonomy in the European technology space, is likely to push the Dutch and European innovation ecosystems towards more applied research work.
4. An uptick in government funding for Dutch innovators.
5. More opportunities at the EU level to find a consensus, accept standardisation, and centralise innovation efforts to create economies of scale.

Table 1: Threats and opportunities, access to EDTs

Access to EDTs			
Threat #	**Threat description**	**Opportunity #**	**Opportunity description**
1	Intensification of technology theft	1	Increase in policymaker awareness and understanding
2	Uptick in issue linkage	2	Increase in demand for highly educated individuals
3	Acceleration of China's semiconductor capabilities	3	Support for bolstering applied research capacity
4	Increases in the cost of consumer goods	4	Increases in government funding
5	Tech market fragmentation	5	Increase in amiability for international cooperation

3.2. Warfighting Capabilities and Emerging Disruptive Technologies

EDTs' potentially transformative impact on military operators' ability to engage in operations is set to contribute to the manifestation of several risks. On the one hand, the need to compete, and to have access to the most cutting-edge use cases associated with these technologies, incentivises the cultivation of R&D programmes which cut corners by failing to adequately correct for the risks associated with these technologies' use and development. On the other, these technologies' integration into military systems creates dependencies (both hardware and software-based) that, if not managed correctly, negatively impact strategic autonomy.

From a military operator's perspective, the benefits of securing access to EDTs are difficult to overstate. Looking just at the EDTs covered in this piece, these range from access to better signals intelligence (SIGINT) (with respect to space-related technologies) to increases in the lethality and combat effectiveness of modern-day systems (see for example the F-35, enabled by space-related technologies, AI, semiconductors), supply chain optimisation (AI), more precise munitions (space-related technologies, semiconductors), and quantum sensing and encryption (quantum computing). The potential it's the impacts of other EDTs

(not covered in this piece) are equally significant, with the overall takeaway being that a military that has access to and is able to integrate EDTs into its operations is likely to outperform one which does not. This elevates the process of developing and accessing EDTs into a bona fide national security issue for many states, incentivising them to forego many of the guardrails that would ordinarily mitigate the impact of negative externalities. The aforementioned negative externalities can, by and large, be conceptualised as being technology specific. In the case of AI, the cutting of corners in military development processes may result in, among others, the development of systems which escalate conflicts without their operators' approval, the further commercialisation of dystopian technologies such as facial recognition algorithms, and the development of algorithms (whether facial recognition, item identification, or other) trained on non-representative data. In the case of space-related technologies, the relative lack of regulation within the domain, combined with a) the financial costs of militarisation, and b) the utility of militarisation, combine to create an environment in which large states are likely to define (military) rules within the domain. This is likely to reduce the competitiveness of or otherwise disadvantage latecomers (smaller states).

The Netherlands is likely to remain dependent on the US for access to capabilities relating to cutting edge technology as quantum computing.

For semiconductors and quantum computing technologies alike, and AI and space-related technologies less prominently, risks, from the Dutch perspective, centre around the problem of over-dependence on 3rd countries. Semiconductors are represented through the Dutch military supply chain, with virtually all systems being reliant on circuit boards to function. The exorbitant cost of manufacturing semiconductors and the facilities necessary for producing them means that they are sourced almost exclusively from Taiwan and South Korea. Even the F-35 relies on, and Lockheed Martin by extension, depend (at least partially) on the Taiwan Semiconductor Manufacturing Company (TSMC) for chip supply.[32] Centralisation within the global semiconductor supply chain is, at least partially, the result of an underappreciation of the dangers of dependence. In this case, an underappreciation of a boom in the global demand for semiconductors likely resulted in governments not offering companies such as Intel sufficient incentives to invest in semiconductor fabs of their own, resulting in a highly centralised – and easily disrupted – supply chain. This oversight (at least as it related to supply chains) is set to be partially addressed in coming years, with the US and Europe alike having invested significant funds into the erection of domestic manufacturing capacities. In other technology areas, the Netherlands has made less progress. AI and quantum computing both represent extremely capital-intensive technologies from an R&D perspective. Without companies such as Google and Huawei, Europe is ill-equipped to develop these technologies domestically, let alone integrate them into its military systems. This implies a prolonged dependence on US arms manufacturers – and the US by extension – to access these technologies within a military context. Because dependence of this type oftentimes goes hand-in-hand with the development of "tertiary" dependencies (for example, dependence on software updates released by foreign companies), this has a significant negative impact on strategic autonomy.

The threats and opportunities associated with the warfighting capabilities section are shortly outlined in the bullets below.

32 Shane McGlaun, "TSMC Under U.S. Pressure As Chip Supplier For Lockheed F-35 Lightning II: Report," HotHardware, January 16, 2020, https://hothardware.com/news/tsmc-under-pressure-to-build-chips-in-us.

Threats

6. The Netherlands suffers from a pronounced (over)dependence on 3rd countries as far as EDTs used within the military context are concerned. This can be attributed, in no small part, to the difficulty of developing and integrating these technologies into operations-ready platforms. This dependence reduces the Dutch ability to make military and other decisions autonomously.
7. Many of the advances made possible by EDTs will not be available to the Netherlands armed forces directly. For example, the Netherlands is likely to remain dependent on the US for access to capabilities relating to cutting edge technology as quantum computing. Given the fact that adversarial states are likely to develop and gain access to these technologies independently, this means that the Dutch dependence on the US and alliance frameworks such as NATO is only set to increase.
8. As demand for semiconductors increases, Taiwan's relevance to military supply chains is set to increase. With plans to erect semiconductor fabs within US and European borders being in their infancy, and the likelihood of these facilities being capable of delivering chips to arms manufacturers within the next five years being low, the US and the Netherlands are set to remain dependent on TSMC. This significantly increases the stakes surrounding a hypothetical Chinese invasion of Taiwan.
9. EDTs, and AI and quantum computing specifically, offer pathways towards significantly increasing the risk of conflicts escalating beyond their intended scopes. The outsourcing of decision-making to machines, even highly capable ones, increases the risk of a miscalculation. The risk of this scenario occurring is increased by the incentivisation of corner-cutting during the development process, something which can be attributed largely to interstate competition over access.
10. A race to integrate EDTs in military operators' toolkits incentivises the cutting of corners during the development process. This leads to the deployment of technologies such as facial recognition. The deployment of these technologies introduces them to popular culture and clears the way for their commercialisation and eventual deployment within society.

Opportunities

6. Increased recognition of the importance of EDTs, and pressures on the semiconductor supply chain, in particular, have opened the door to pieces of legislation such as the US CHIPS Act and the EU's European Chips Act. As the negative effects of relying on 3rd parties to access key technologies continue to manifest, opportunities arise for like-minded countries to come together and reach agreements that ensure their militaries' access to them going forward.
7. EDTs, and AI and quantum computing, in particular, offer pathways to reducing the costs associated with military operations. For example, these technologies are likely to reduce the number of individuals needed to engage in conflict situations, something which is certain to translate into a reduction in conflict fatalities. They also facilitate optimisations in logistics, equipment maintenance, etc.
8. EDTs offer significant operational benefits to military operators beyond those associated with cost reductions or efficiency. As an example, space-related technologies or quantum sensing can provide military operators with reams of actionable intelligence, empowering them to make better decisions vis-à-vis (among others) battlefield asset allocation. Other technologies, such as AI and semiconductors, will enable the development of, among others, more agile, more precise weapons.

Table 2: Threats and opportunities, warfighting capabilities and EDTs

Warfighting Capabilities and EDTs			
Threat #	**Threat description**	**Opportunity #**	**Opportunity description**
6	Overdependence on 3rd countries	6	Increased pressure opens the door to new legislation
7	Adversarial states are likely to gain access independently	7	EDTs offer pathways to cost reductions for military operators
8	Increases in demand for semiconductors	8	Significant operational benefits enabled by EDTs
9	Risk of conflict escalation		
10	Competition incentivises corner cutting during development		

3.3. Societal Impacts of Emerging Disruptive Technologies

EDTs are set to have a significant impact on society and the processes that underpin it. Depending on the technology in question, the development, production, and utilisation of EDTs are likely to (continue to) adversely impact the norms and values safeguarding human rights, as well as the functioning of the judicial and democratic processes.

Norms and values that enshrine the sanctity of the human rights to life, food, clean water, etc. arguably form the foundation of the international order that emerged after the dissolution of the Soviet Union in 1992. The economic conditions that emerged during, and were facilitated by, this (relatively) peaceful order helped to lift millions out of poverty, led to a not-insignificant increase in the standard of living enjoyed by citizens in the Netherlands and Europe more broadly, and arguably laid the foundation for the EDTs covered in this publication to be developed. It is maintained, at least partially, by the Dutch (and other liberal democracies') continued adherence to the norms and values encapsulated within it. Today, the methods through and the conditions by which EDTs are manufactured and the unequal manner by which their benefits have been distributed across societies mean that the degree to which these norms and values are viewed as unassailable by liberal democracies can reasonably be called into question.

The production processes underpinning the manufacture of these technologies – and, in current times, semiconductors more specifically – is the first variable worth considering here. The production of semiconductors exposes workers to, among others, substances such as organic solvents, acids, and heavy metals. These materials irritate the skin and, in some cases, damage the reproductive system or are classified as neurotoxins.[33] Because chip manufacturing is not based in Europe, the Netherlands, or any other (Western) liberal democracy at

33 Myoung-Hee Kim, Hyunjoo Kim, and Domyung Paek, "The Health Impacts of Semiconductor Production: An Epidemiologic Review," International Journal of Occupational and Environmental Health 20, no. 2 (April 2014): 95–114.

present, the realities of this process project the image that the countries which wish to benefit from the perks of accessing these technologies are not willing (or refuse to pay to mitigate) the negative externalities associated with their production. The chip manufacturing process is also extremely energy intensive, meaning it consumes a significant amount of energy, and water, and emits copious amounts of greenhouse gasses. In 2019, Intel's fabs used three times as much water as Ford's plants, while also creating twice as much hazardous waste.[34] TSMC has also not met its key sustainability targets in 2020; the company's water waste has increased with its revenue.[35] This trend is unlikely to abate; as the world continues to digitalise, semiconductors – and the reliable supply and production thereof – are set to continue to grow in relevance.[36]

The technologies can also be easily used to create deep fakes, emulate voices and speech patterns, and – more generally – generate content which is difficult to distinguish from reality.

The outsourcing of labour to circumvent safety standards, environmental regulations, and other economically impactful regulations are not unique to the semiconductor production process or EDTs in general. This means that, while addressing these issues within the context of EDTs is unlikely to dispel all negative perceptions undermining the Dutch (and liberal democracies' more generally) commitment to human rights-related norms and values, doing so nonetheless constitutes a step forward. Because any effort to reduce Dutch consumers' negative impact on the well-being of individuals overseas is likely to go hand-in-hand with a reduction of said consumers' dependence on foreign entities, initiatives to produce EDTs domestically also have obvious benefits as far as strategic autonomy is concerned.

Moreover, the EDTs covered by this study – and AI and quantum computing more specifically – have the potential to seriously undermine the integrity of the democratic and judicial processes. This can be partially attributed to the use cases associated with them *within* liberal democracies themselves, and partially to the way they have been put to use (or may be put to use in the future) by the world's autocracies. EDTs' contribution to undermining the functioning of democratic and judicial systems *within* liberal democracies relates, in no small part, to how they deepen existing disillusionment within these societies' populaces. Disillusionment can be broadly defined as a collection of feelings and processes which, at the macro (societal) level, contribute to trends such as individual-level political apathy, individual-level subscription to fringe or extremist ideologies, and – in extreme cases – a willingness to perpetrate political violence. The concept of disillusionment, as well as the trends and developments which contribute to its proliferation in Dutch society, are key to making sense of violent protests that took place, for instance, during the COVID-19 pandemic. Multiple studies correlate disillusionment (feelings of political apathy, a tendency towards political extremism, etc.) to hopelessness. Its role in shaping contemporary politics received an in-depth exploration in Dale Beran's 2017 essay *4chan: the Skeleton Key to the Rise of Trump*, which explores how feelings of economic, social, and political loss resulted in the cultivation of a "culture of hopelessness" that led hundreds of young, socioeconomically privileged individuals to vote for Donald Trump in the 2016 Presidential Elections.[37] Mis- and disinformation – and the spread thereof – play an outsized role in the proliferation of feelings of hopelessness and disillusionment. This process is not, in and of itself, new but is exacerbated by the use of EDTs.

34 Alan Crawford, Ian King, and Debby Wu, "The Chip Industry Has a Problem With Its Giant Carbon Footprint," Bloomberg.Com, April 8, 2021, https://www.bloomberg.com/news/articles/2021-04-08/the-chip-industry-has-a-problem-with-its-giant-carbon-footprint.

35 Matthew Gooding, "The Environmental Impact of Chip Making Needs Closer Scrutiny," Tech Monitor (blog), July 14, 2021, https://techmonitor.ai/leadership/sustainability/chip-making-and-sustainability-intel-tsmc.

36 Crawford, King, and Wu, "The Chip Industry Has a Problem With Its Giant Carbon Footprint."

37 Dale Beran, "4chan: The Skeleton Key to the Rise of Trump," Medium, July 30, 2019, https://medium.com/@DaleBeran/4chan-the-skeleton-key-to-the-rise-of-trump-624e7cb798cb.

As technological progress and access to education have expanded access to information and at least on paper social reach at the individual level, they have also facilitated among others the spread and proliferation of ideas and growing individual-level situational awareness of society and the world. What *is* new is the use of EDTs such as AI by social media companies (see for example Meta's Facebook and WhatsApp, Twitter, and TikTok). These have, for all intents and purposes, emerged as *the* venues for staying up to date on global and local events and disseminating mis- and disinformation. Social media platforms' facilitation of interpersonal connections and communication fundamentally changes how news and ideas are consumed and interpreted by their users. UMany platforms operate on ad-supported business models which incentivise them to optimise their products to maximise user time spent on the platform (a key performance indicator (KPI), which is often referred to as "user engagement"), which acts as a supercharger for mis- and disinformation. AI and (in the future, quantum computing) are used to increase the reach (amplify the impact of) of divisive content, which tends to generate greater engagement than non-divisive content ("enragement equals engagement"). Furthermore, the technologies can also be easily used to create deep fakes, emulate voices and speech patterns, and – more generally – generate content which is difficult to distinguish from reality. This has the potential to exacerbate the post-truth sentiment delineated from contemporary mis- and disinformation practises and has inflammatory effect on societal polarisation.

Armenia, Azerbaijan, Belarus, Ecuador, Kazakhstan, Kenya, Pakistan, Singapore, Sudan, Tunisia, Venezuela and Zimbabwe have all sought to implement Chinese surveillance technologies in bids to emulate Beijing's model of AI-led repressive governance.

EDTs also contribute to undermining the functioning of democratic and judicial systems as a result of authoritarian countries employing them as domestic control systems. In China, the combination of AI-driven facial recognition, centralisation of communication platforms (WeChat, etc.) and state utilisation of 'ground level' (healthcare, etc.) data has allowed for the inception of an early social credit system in which citizens are awarded credit for 'good behaviour', and penalised for 'bad behaviour', including, jaywalking and walking a dog without a leash.[38] Penalties reportedly range from citizens being precluded from using certain forms of public transport, denying their children enrolment into the best schools, and in the worst cases, imprisonment.[39] EDTs' employment towards these ends undermines the norms underpinning democratic governance models in two ways. First and foremost, it does so by providing would-be autocrats with a set of (easily exportable) tools for centralising their power and repressing their populations. Chinese companies are building smart cities with built-in surveillance technology in Pakistan, the Philippines, and Kenya; and Chinese companies are supplying Singapore with facial recognition cameras.[40] In addition to exporting China's totalitarian governance system internationally, this creates a foundation for global surveillance and a dependency of receiving states on China for technology which could result in a higher pressure for them to align with China's agenda.[41] Armenia, Azerbaijan, Belarus, Ecuador, Kazakhstan, Kenya, Pakistan, Singapore, Sudan, Tunisia, Venezuela and Zimbabwe have all sought to implement Chinese surveillance technologies in bids to emulate Beijing's model of AI-led repressive governance.[42] The second way in which these use cases undermine the norms underpinning democratic governance models is that, in granting them visibility and coverage, they introduce said use cases as a feasible and realistic alternatives. While

38 Alexandra Ma, "China has started ranking citizens with a creepy 'social credit' system — here's what you can do wrong, and the embarrassing, demeaning ways they can punish you," Business Insider Nederland, October 30, 2018, https://www.businessinsider.nl/china-social-credit-system-punishments-and-rewards-explained-2018-4/.

39 Vicky Xiuzhong Xu and Bang Xiao, "'Punishing the Disobedient': China's Social Credit System Could Engineer Social Behaviour by 2020," ABC News, March 30, 2018, https://www.abc.net.au/news/2018-03-31/chinas-social-credit-system-punishes-untrustworthy-citizens/9596204.

40 Steven Feldstein, "How Artificial Intelligence Systems Could Threaten Democracy," The Conversation, April 22, 2019, http://theconversation.com/how-artificial-intelligence-systems-could-threaten-democracy-109698.

41 Feldstein.

42 Michael J. Abramowitz, "Democracy in Crisis," Freedom in the World 2018 (Freedom House, 2018), https://freedomhouse.org/sites/default/files/2020-02/FH_FIW_Report_2018_Final.pdf.

exposing societies to a technology's possible use need not translate into acceptance of said use, it *does* – in creating awareness about its existence – create a framework for forming expectations about technology, its future and current use cases, and its likely role in individuals' lives going forward. As a consequence, aspects of EDTs' totalitarian employment are likely to find their way into consumers' hands thus potentially further eroding the norm preventing authoritarian uses of technology.

The use and production of EDTs may affect the lives of the underprivileged, putting into question the adherence of liberal democracies to western norms and values. This discussion will likely be exacerbated by the carbon footprint constituting one of the negative externalities of EDTs. The prevalence of AI-based algorithms on social media platforms will contribute to spreading disinformation, thereby polarising societies, undermining veritable authorities, and sparking anti-state sentiments. In autocracies, EDTs are expected to be used for surveillance of the citizens to control their behaviours, thereby infringing upon individual rights.

As it is outlined in the above section, the threats and opportunities stemming from EDTs' societal impacts are interlinked and interplaying. That said, five main threats and two main opportunities can be delineated from the nebula of EDTs' societal impact:

Threats

11. Existing patterns of alienation and disillusionment on social media are likely to be exacerbated by EDTs' enhancement of various related factors. Such EDT-influenced factors may include the enhanced efficiency of algorithms via quantum computing and AI. These algorithms in turn exacerbate the presence of echo-chambers and radicalisation on social media platforms. They may also further infringe upon users' privacy.
12. EDTs are likely to democratise users' access to deep fake technology. What is more, bad-faith institutional actors may also proliferate deep fakes in a higher capacity enabled by EDTs. Deep fakes in turn may exacerbate the above-mentioned effects of disillusionment and radicalisation, by cultivating the virulent sentiment of post-truth rationalities. The virality of fake news for example may be enhanced by audio-visual substantiation thereof.
13. Social engineering and social credit systems are likely to be enhanced by the development of EDTs. This enables autocratic regimes such as Russia or China to solidify their control over their populations. Censorship may also benefit from AI language processing in particular. The latter process may have bearing on what information can "escape" these autocratic regimes. Such censorship in turn may increase appreciation for these regimes in western liberal democracies as well, by cultivating an image of efficiency.
14. Judicial automation processes promise to be resource- and time-efficient. They are enabled by EDTs, such as AI. That said, AI may be unable to factor in certain human variables, such as state of mind at the time of committing a crime, or socio-cultural background. What is more, the biases of the algorithm's developer may also translate into biases inherited by the judicial automation system.

Opportunities

9. When used ethically, content moderation and deep fake detection technologies can combat the effect of EDTs within the same fields. Conversely, EDT-enhanced policing may contribute to combatting the negative effects stemming from EDT-related risks.
10. EDT-enabled algorithms may contribute to cost-reduction within the judicial branch of power within western democracies. Furthermore, the biases of human actors may be filtered out by automation of judicial processes.

Table 3: Threats and opportunities, societal impacts of EDTs

Access to EDTs			
Threat #	**Threat description**	**Opportunity #**	**Opportunity description**
11	Alienation and disillusionment on social media	9	Automation of content moderation and "deep fake" detection
12	Democratisation and proliferation of convincing "deep fakes"		
13	Cementing of authoritarian governance models abroad	10	Judicial cost reductions as a result of automation
14	Biases in judicial automation processes		

3.4. **Conclusion**

EDTs are expected to bring about diverse threats and opportunities that will have to be addressed by policymakers. Increasingly politicised access to EDTs and techno-nationalist practices around the globe will likely restrict the competitiveness of Dutch companies and expose them to potential attempts of intellectual property theft. Within the warfighting capabilities domain, the relevance of TSMC to military supply chains will inevitably increase, putting the West in a problematic position if China decides to attack Taiwan. In the societal field, AI-based algorithms of social media platforms promoting divisive content to increase user engagement, undermine the authority of veritable media outlets and deepen the citizens' disillusionment and anti-state sentiments. Nevertheless, EDTs bring various opportunities as well. For instance, techno-nationalist practices will incentivise the Dutch tech industry to create vacancies for the highly skilled, which may entail extensive know-how capabilities in the medium-long term. The recognition of substantial reliance of western warfighting capabilities on TSMC contributed to discussions about the EU's technological sovereignty, while AI and quantum computing will likely decrease the costs of potential military operations.

4. Policy Recommendations

Dutch and EU markets, despite the introduction of several promising pieces of regulation, remain highly vulnerable to techno-nationalist measures taken by other states.

The development of, and ensuing interstate competition over access to, EDTs brings with it a wide range of threats and opportunities. These technologies' development processes may play out over decades, but the impacts associated with deploying them – and the societal, political, economic, and military changes associated therewith – can unfold within years or even months. As a result, the time for policymakers to put laws, funding, or other initiatives in place to meet the threats and to realise the opportunities associated with EDTs is *now*. The Netherlands may not so much be experiencing the negative effects of (over)dependence on the US or China in the present. But if it fails to take steps to ensure those dependencies reduce over time, it will find itself needing to choose between its economic prosperity and its norms, values, or foreign policy objectives at some point in the not too distant future. Likewise, the negative impact of deep fakes on the Dutch democratic process may currently be limited. But if the Netherlands fails to set standards and introduce matching incentives for moderating acceptable speech online, a major escalation could be an App Store release away. And the role of AI in automating conflict escalation may currently be limited. But if the Netherlands reneges on working to shape international agreements aiming to limit the risk of it doing so, competition between the US, China, and (though to a lesser extent) Russia, will ultimately result in it being employed in that way.

This chapter aims to provide recommendations for meeting the challenges posed by EDTs head-on. It explores policy options for addressing the threats and seizing the opportunities the EDFs discussed in this study present. Many of the threats and opportunities are associated with structural problems or shortcomings that need to be addressed. The following list provides an overview of the topics covered in the Sections 4.1. through 4.7 below:

1. **Mitigate the vulnerability of Dutch and EU markets.** Dutch and EU markets, despite the introduction of several promising pieces of regulation, remain highly vulnerable to techno-nationalist measures taken by other states. The Netherlands ought to implement more robust and more comprehensive regulatory frameworks to mitigate the negative impacts of espionage, cybercrime, and various forms of technology theft. The mitigation effort would have to review aspects of the Investments, Mergers and Acquisitions Safety Assessment Act (VIFO).
2. **Bolster the competitiveness of Dutch and EU markets.** Adapting to mounting interstate rivalry entails increasing the resilience of the Dutch innovation ecosystem to techno-nationalist foreign practises. Realising an internationally competitive innovation ecosystem would provide the Netherlands with secure access to more Dutch and international talent, transposing theoretical research into real-world use cases, and generating the revenues necessary for cutting-edge research and development (R&D). A necessary step would be the deepening of engagement with mechanisms such as the European Defence Agency (EDA), the Permanent Structured Cooperation (PESCO), and the European Defence Fund (EDF). The Netherlands and Europe should continue doubling down on their support for the semiconductor industry and invest in sensitive technologies. The strengthening of advanced democracies' technological edge in the semiconductor ecosystem could entail

active conversation with the semiconductor sector, the mobilisation of Dutch, European, and institutional funds, the allocation of tax incentives, the fast-tracking of fab construction in the Netherlands and the EU, the expansion of pre-competitive research funding for the semiconductor and critical raw material value chains, the cultivation and attraction of students and talent related to EDTs by means of selective visa liberalisation, and the promotion of the science, technology, engineering, and math (STEM) fields. Similar measures to the ones listed above can be extrapolated onto EDTs at large.

3. **Enhance awareness and understanding of EDT-related issues.** The formulation of effective regulatory frameworks on issues surrounding techno-nationalism and negative societal and military impacts of EDTs is contingent on a deep understanding of how these technologies work and what their real-world use cases are. Improving key stakeholders' including lawmakers' awareness and understanding of EDT-related topics will allow for the introduction of more effective legislation. On the level of policy, such measures should include the implementation of incentives to attract human capital also to the public sector. Additionally, the expansion and subsidisation of existing state-funded research commissions such as the Analysis and Research Service (DAO) or the Digital Affairs Committee (DiZa) could serve as an effective framework for the endeavours outlined here.
4. **Reduce overreliance on East Asia within semiconductor supply chains.** A key challenge facing not only Dutch consumers but also the supply chains underpinning the Dutch Armed Forces' warfighting capability, is the country's continued reliance on the Taiwan Semiconductor Manufacturing Company (TSMC). This renders the Netherlands vulnerable not only to supply chain disruptions that might occur because of geopolitical events (for example, a Chinese maritime blockade or invasion of Taiwan) but also to supply and demand dynamics outside its control. These challenges can be mitigated by increasing domestic and regional production capacity. The recent US and European Chips Acts or the Dutch Ministry of Economic Affairs and Climate's (EZK) Early 2022 application for a €230 million subsidy package for R&D projects may serve as relevant precedents and potentially as frameworks for this endeavour.
5. **Support the creation of national and international regulatory frameworks.** A significant share of the risks associated with EDTs can be tied, whether directly or indirectly, to lacking (or consciously ignored) guard rails during the development process of EDTs. This can, in turn, be attributed to an inept international regulatory environment as a by-product of interstate rivalry. The creation of national and international frameworks to regulate EDTs, the standards they should meet before being employed within military and domestic contexts, and the use cases they should and should not be employed for, will go a long way towards mitigating these risks. Such multilateral or minilateral agreements should address various levels of regulation with different applications on each level. As such, this report breaks down proposed regulations on EDTs on the domestic, regional, international, and commercial levels respectively for each of the four EDTs at hand.
6. **Enact Dutch and European legislation regulating social media platforms.** Much of AI's and potentially quantum computing's negative impacts on the democratic process can be attributed to shortcomings on part of states in regulating social media platforms. There is a wide range of policy options available for reducing the threat posed by misinformation online, some of which the Netherlands has yet to implement. Examples include privacy protection, filtering out deep fakes, and banning algorithms that primarily show the user upsetting content. These measures would mitigate the echo-chamber effect, and thereby curb the impacts of disillusionment and radicalisation.
7. **Facilitate the development of European champions and coalitions of the willing.** The geopolitical hazards stemming from EDT-related risks are exacerbated by incomplete domestic efforts to optimise for resilience. These effects could in turn be mitigated by integration efforts of the military and civilian spheres, subsidisation and incentivisation

The Netherlands and Europe should continue doubling down on their support for the semiconductor industry and invest in sensitive technologies.

of European champions and close monitoring of EDT-adjacent activities by coalitions of these actors. This will also strengthen Europe's position at a time when allies such as the US are implementing protectionist policies and putting pressure on European economies to adhere to its policies. The Netherlands could cement the strategic leverage derived from their unique role in semiconductor supply chains through deepened cooperation with bottleneck companies such as ASML as well as with dominant but non-bottleneck companies in that sector such as NXP. In turn, forming coalitions of the willing on the European and on the Transatlantic levels between state actors and industry champions could allow for a strengthened strategic posture against revisionist systemic rivals. Finally, the deepening of integration between the civilian and military spheres on EDT-related issues carry the twofold benefit of enhancing both military capabilities via EDTs and socio-economic resilience to EDTs. The sections below provide a per-policy guideline overview of relevant existing and proposed necessary policies. Where possible, policy recommendations offer an assessment of existing initiatives, providing policymakers with an overview of their shortcomings, why they matter, and what additions and/or amendments might contribute to making them more effective. Because several policy recommendations contribute to mitigating multiple threats and realising multiple opportunities, each policy recommendation features an up-front summary of the challenges it addresses.

The Netherlands could cement the strategic leverage derived from their unique role in semiconductor supply chains through deepened cooperation with bottleneck companies such as ASML as well as with dominant but non-bottleneck companies in that sector such as NXP.

4.1. Mitigate the vulnerability of Dutch and EU markets

State toolkits for securing access to the technology and technological know-how developed by others are extensive. Examples of policy instruments available to the Netherlands are laws designed to pressure foreign companies to transfer core technologies upon localising their businesses within the Netherlands, and FDI into the Netherlands. Remaining mindful of the fact that the introduction of draconian measures is likely to undermine the Netherlands' attractiveness as a destination for FDI, Dutch policymakers should work towards putting a robust framework in place for countering the negative impact of these policy instruments. Simply put, obligations of technology transfer must not be allowed to deter high-tech FDI from Dutch markets under the new framework. The new framework must regulate all aspects of technology transfer under instances of FDI. Doing so will not only reduce the negative economic impacts associated with technology theft; contribute to Dutch strategic autonomy, reduce Dutch susceptibility to supply chain disruptions, increase Dutch resilience to the negative effects of international market fragmentation, and reduce its dependence on third countries for the armed forces.

The measures outlined in the present policy recommendation are meant to be informed by and be in accordance with the EU's 2020 call towards member-states to erect committees on foreign investment (CFIs, modelled after the Committee on Foreign Investment in the United States - CFIUS), for purposes such as investment screening. The Dutch framework for implementing such measures is still under development, and expected to be implemented in 2023. HCSS' 'Reaching Breaking Point: The semiconductor and critical raw material ecosystem at a time of great power rivalry' report offers more granular recommendations as to how Dutch

legislation could translate these newfound EU guidelines.[43] That is, in respect to safeguarding Dutch markets from technology theft and to informed policymaking taking into account dynamic geopolitical circumstances

Examples of policy instruments available to the Netherlands are laws designed to pressure foreign companies to transfer core technologies upon localising their businesses within the Netherlands, and FDI into the Netherlands.

Since the publication of 'Taming Techno-Nationalism' in 2021,[44] the Netherlands has – in the introduction of the *Wet veiligheidstoets investeringen, fusies, en overnames* (Investments, Mergers, and Acquisitions Safety Assessment Act, VIFO) – addressed a key recommendation outlined in that piece. More specifically, 'Taming Techno-Nationalism's recommendation that the Netherlands should apply protections to critical infrastructure and the critical technologies ecosystem has, by and large, been implemented.[45] VIFO features, among others, a clear overview of what is and is not considered a critical technology,[46] a robust enforcement mechanism that allows the EZK to undo an acquisition that poses a threat to national security in instances where participating parties have failed to report it, and a clear mandate for the Minister of Economic Affairs and Climate to act. VIFO complements the EU's existing notification requirements, and will, in the near future, likely be supplemented by the EU's proposal for a regulation on foreign subsidies distorting the internal market.[47] All of this means that from a perspective which aims to maintain the Dutch attractiveness as a beneficiary of FDI, the legislative framework responsible for circumventing technology transfers resulting from FDI is, by and large, comprehensive in its scope. This notwithstanding, there are several shortcomings in the way VIFO has been formulated that undermine its utility as an enforcement mechanism. In concrete terms, the report recommends improving VIFO by considering the following measures:

Carefully weigh VIFO's public-private requirement and refine where appropriate. In its current form, VIFO stipulates that providers of critical infrastructure or companies that engage with sensitive technologies should report an acquisition or a significant change in share control to the *Bureau Toetsing Investeringen* (Investment Review Office, BTI) of the EZK. An adverse effect may be that private-sector organisations, in particular start-ups with fewer means to comply with these requirements, become more hesitant to interact with the Dutch public sector. Possible knock-on effects of such a development would be a reduction of the Dutch government's ability to benefit from and support the growth of these companies and, ironically, an increase in these companies' susceptibility to foreign takeovers and acquisitions.

Clarify Articles 19-21 in private to companies and export interest groups. Articles 19-21 of VIFO stipulate, among other things, that factors such as an acquiring party's country of origin and "track record securing sensitive technologies," can serve as grounds for blocking a transaction. These factors are ambiguous, something which may have an adverse effect on Dutch companies' willingness to accept foreign investors in sensitive industries. Whilst the Dutch innovation ecosystem stands to benefit from the R&D capacities, job opportunities, and economic stability provided by FDI, protecting the Netherlands' and Europe's technological edge in this new era of state-sponsored attempts to acquire sensitive technologies abroad inevitably requires greater restrictions. In private consultations with companies and

43 Joris Teer and Mattia Bertolini, "Reaching Breaking Point: The Semiconductor and Critical Raw Material Ecosystem at a Time of Great Power Rivalry" (The Hague Centre for Strategic Studies, October 2022), 85–86.

44 van Manen et al., "Taming Techno-Nationalism: A Policy Agenda."

45 van Manen et al., 12.

46 The law draws on the EU's list of dual-use technologies and the EU's list of common military technologies. Importantly, the Netherlands has distinguished between "sensitive" and "highly sensitive" technologies that occur on this list, though how these technology categories are treated differently under VIFO remains ambiguous.

47 "White Paper on Levelling the Playing Field as Regards Foreign Subsidies" (Brussels: European Commission, June 17, 2020), https://ec.europa.eu/competition/international/overview/foreign_subsidies_white_paper.pdf.

export interest groups, the government may consider providing greater clarity on the decision framework that finally determines whether FDI is permitted or not. Being publicly explicit about which high-risk countries are excluded from investing in sensitive technologies in the Netherlands may risk retaliation by these states.

Except for the recommendation that the Dutch government should pay closer attention to students from adversarial countries attending Dutch technical universities, which has been partially addressed by the introduction of Ursula Von der Leyen's Defence of Democracy package,[48] the remainder of the policy recommendations outlined in 'Taming Techno-Nationalism' have not, as of yet, seen implementation. These include the leveraging of procurement to improve cybersecurity and counterintelligence capacities among Dutch private sector actors, erecting legitimate barriers to trade and procurement based on the fairness principle, enhanced collaboration within NATO to safeguard economic security, and supporting progress on EU-level initiatives.[49] It merits consideration to follow up on theserecommendations.

The Netherlands has a vested interest in providing the entities that make up its broader innovation ecosystem with the conditions and with the impetus to grow and prosper.

4.2. Bolster the competitiveness of Dutch and EU markets

Much as is the case with the previous section, recommendations geared towards increasing the international competitiveness of the Dutch innovation ecosystem received in-depth recommendations in last year's 'Taming Techno-Nationalism'.[50] Bolstering the competitiveness of the Dutch innovation ecosystem constitutes a key policy objective. One of the reasons that Dutch current and future economic competitiveness and military capacity are threatened by techno-nationalism is that the entities that make up its innovation ecosystem are in some cases too small to "survive" exposure to techno-nationalist advances as they are made up of start-ups or 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 wealthy competitors. Although they arguably punch above their weight as far as their ability to conduct research into sensitive technologies is concerned, they cannot realistically compete with the likes of Google, Lockheed Martin, or Huawei when it comes to transposing their cutting-edge research activities into practice. At the same time, innovation in the defence realm is generated by private sector actors that are not integral part of the defence ecosystem (and don't consider themselves as such), but have defence as a secondary or tertiary market. As more and more dual use technology in fact originates on the non-military side, this is increasingly important. Many of these innovative 'dual use' companies are not start-ups but established companies.

Taken together, these characteristics mean that the Netherlands has a vested interest in providing the entities that make up its broader innovation ecosystem with the conditions and with the impetus to grow and prosper. Recommendations offered in 'Taming Techno-Nationalism' called for the implementation of policies geared towards incentivising university

48 European Commission, "Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: On the European Democracy Action Plan" (Brussels: European Commission, December 3, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A790%3AFIN&qid=1607079662423.

49 van Manen et al., "Taming Techno-Nationalism: A Policy Agenda."

50 van Manen et al.

research teams to found start-ups, empowering start-ups to mature into scale-ups and (eventually) grown-ups has two high-level benefits, and towards encouraging, supporting, and contributing to (domestic) vertical ecosystem integrations. More concretely, an argument was made that the Netherlands should reduce the regulatory and administrative barriers to engaging in venture capital (VC)-based backing of Dutch start-ups; that procurement processes ought to be stepped up, optimised, and engaged in for the long haul; and that the Netherlands should deepen its engagement with mechanisms such as the EDA, PESCO, and the EDF.

ASML remains the world's only supplier of lithography machines needed for semiconductor production, something which provides the Netherlands with a strategic and competitive advantage that is likely to pay off in the future.

In addition, the strengthening of advanced democracies' technological edge on the micro level must entail active conversation with semiconductor firms, the mobilisation of Dutch, European, and institutional funds, the allocation of tax incentives, the fast-tracking of fab construction in the Netherlands and the EU, the expansion of pre-competitive research funding for the semiconductor and critical raw material value chains, and the cultivation and attraction of students and talent related to EDTs by means of selective visa liberalisation, and the promotion of the STEM fields.[51] Similar measures to the ones listed above can be extrapolated onto EDTs at large.

While, since the publication of 'Taming Techno-Nationalism', barriers to securing venture capital (VC) funding have, with the introduction of VIFO, arguably increased, the Netherlands *has* taken several positive steps towards bolstering its innovation ecosystem. A noncomprehensive list of the actions taken by (among others) EZK is provided in the bullets below, which deserve follow up:

Continue doubling down on support for the semiconductor industry. The Netherlands has sought to support the R&D efforts of its semiconductor industry in significant ways since the publication of 'Taming Techno-Nationalism'. Most significantly, in early 2022 EZK applied for a green light from the EC to provide €230 million in subsidies to R&D efforts to projects run by NXP, ASML, NearField Instruments, TechnoFischer, and Smart Photonics. Subsidies of this kind, if greenlit, fall under the EC's Important Projects for Common European Investment (IPCEI), a mechanism which aims to allow Member States to make microelectronic-related investments which might otherwise have a distorting or anti-competitive impact on the EU's open market.[52] The Dutch focus on bolstering its semiconductor industry, which is also explicitly outlined in its industrial policy,[53] is prudent for several reasons. First, the Dutch semiconductor industry is one of the few Dutch-sensitive technology industries to be transposing theory into applied research in a meaningful way. ASML remains the world's only supplier of lithography machines needed for semiconductor production, something which provides the Netherlands with a strategic and competitive advantage that is likely to pay off in the future. Second, insofar as investments under IPCEI reduce the Dutch dependence on TSMC, they play a significant role in blunting the economic impacts of a Chinese invasion of Taiwan.[54]

51 For an in-depth overview of how these measures can be implemented, please consult the HCSS' report Reaching Breaking Point: 'The semiconductor and critical raw material ecosystem at a time of great power rivalry'. Teer and Bertolini, "Reaching Breaking Point: The Semiconductor and Critical Raw Material Ecosystem at a Time of Great Power Rivalry," 86–87.

52 Thierry Breton, "IPCEI on Microelectronics – A Major Step for a More Resilient EU Chips Supply Chain," Text, European Commission, December 20, 2021, https://ec.europa.eu/commission/commissioners/2019-2024/breton/blog/ipcei-microelectronics-major-step-more-resilient-eu-chips-supply-chain_en.

53 Ministerie van Economische Zaken en Klimaat, "Het Verschil Maken Met Strategisch En Groen Industriebeleid" (The Hague: Ministerie van Economische Zaken en Klimaat, July 8, 2022), https://open.overheid.nl/repository/ronl-f083c1c77a651997beadb00de52de79dacaf1c2c/1/pdf/het-verschil-maken-met-strategisch-en-groen-industriebeleid.pdf.

54 "Opinie | Deep tech moet de ruimte krijgen in Nederland," NRC, n.d., https://www.nrc.nl/nieuws/2022/09/15/deep-tech-moet-de-ruimte-krijgen-in-nederland-a4141984.

Invest in sensitive technologies. In addition to leveraging IPCEI to allow for the outright subsidisation of the Dutch semiconductor industry, EZK has made €20 billion in funding available for innovation and knowledge development over the period spanning 2021-2025. Distributed by the *Nationaal Groeifonds* (National Growth Fund, NGF), projects dealing with sensitive technologies, including quantum computing and semiconductors, are set to be prioritised.[55] Funds distributed through the NGF are available through calls for proposals, with an "independent commission" being responsible for selecting projects based on their contribution to the long-term growth of the Dutch economy and their societal impact. Two rounds of funding have been completed through the NGF, with proposals currently being accepted for a third round scheduled to take place in 2023. The 2021 (first) round saw 10 projects funded,[56] while the 2022 (second) round saw 28.[57] Round 1 provided funding to (among others) quantum computing (Quantum Delta) and AI-related (AiNed) research. Round 2 saw less funding for the sensitive technologies addressed in this publication, though projects in the pharmaceutical and biotech sectors received significant support.[58]

The current geopolitical environment requires greater investments into defence.

The initiatives undertaken by EZK since the publication of 'Taming Techno-Nationalism' go a long way towards addressing the recommendations outlined in that report. Specifically, funding made available through NGF acts as a robust supplement to EU-level initiatives such as Horizon Europe and, to a lesser extent, the soon-to-be-unveiled European Chips Act.[59] It also addresses a key concern outlined in 'Taming Techno-Nationalism'; namely, that procurement ought to prioritise longer-term funding for projects and that those projects ought to have clear business cases to ensure their longer-term sustainability.

From a military R&D perspective, the current geopolitical environment requires greater investments into defence. In the wake of the initiation of Russia's war against Ukraine, the Dutch Ministry of Defence has seen a sizeable (40%) increase in its budget, an upscaling that amounts to €5 billion in defence spending being made available to it on a structural basis.[60] Despite the fact that a not-insignificant share of the Ministry's budgetary increases will be allocated to restocking depleted munitions, repairing and modernising existing hardware, and procuring equipment, it is also leading to more funding for R&D.[61] The Dutch *Strategische Kennis- en Innovatieagenda* (Strategic Knowledge and Innovation Agenda, SKIA) outlines a plan for conducting ongoing research in several technology areas, one of which is referred to as "sensitive technologies".[62] Combined with the goals outlined in (among others) the EU's Strategic Compass and joint communications published in the wake of Russia's invasion of

55 Ministerie van Economische Zaken en Klimaat, "Het Verschil Maken Met Strategisch En Groen Industriebeleid."

56 "Projecten ronde 1 - Nationaal Groeifonds," webpagina, Ministerie van Economische Zaken en Klimaat (Ministerie van Economische Zaken en Klimaat, June 28, 2022), https://www.nationaalgroeifonds.nl/projecten-ronde-1.

57 "Projecten ronde 2 - Nationaal Groeifonds," webpagina, Ministerie van Economische Zaken en Klimaat (Ministerie van Economische Zaken en Klimaat, September 29, 2022), https://www.nationaalgroeifonds.nl/projecten-ronde-2.

58 "Projecten ronde 2 - Nationaal Groeifonds."

59 "European Chips Act," Text, European Commission, n.d., https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en.

60 "Additional EUR 5 Billion in Defence Spending on a Structural Basis," Ministerie van Defensie (Ministerie van Defensie, May 20, 2022), https://english.defensie.nl/latest/news/2022/05/20/additional-eur-5-billion-in-defence-spending-on-a-structural-basis.

61 "A Stronger Netherlands, a Safer Europe Investing in a Robust NATO and EU," Ministerie van Defensie (Ministerie van Defensie, July 19, 2022), https://english.defensie.nl/downloads/publications/2022/07/19/defence-white-paper-2022.

62 "Strategische Kennis- en Innovatieagenda (SKIA) 2021-2025 - Publicatie - Defensie.nl," Ministerie van Defensie (Ministerie van Defensie, November 27, 2020), https://www.defensie.nl/downloads/publicaties/2020/11/25/strategische-kennis--en-innovatieagenda-2021-2025.

Ukraine,[63] an increase in Dutch defence spending creates a clear opportunity to maximise returns on investment (RoIs) by, as recommended in 'Taming Techno-Nationalism', stepping up Dutch commitments to co-develop technologies through European frameworks such as PESCO and the EDF.

4.3. Enhance awareness and understanding of EDT-related issues

The formulation of effective regulatory frameworks on issues surrounding techno-nationalism and negative societal and military impacts of EDTs is contingent on a deep understanding of how these technologies work and what their real-world use cases are. Improving key stakeholders', including lawmakers'awareness and understanding of EDT-related topics will allow for the introduction of more effective legislation. On the level of policy, such measures should include the implementation of incentives to attract human capital also to the public sector. Additionally, the expansion and subsidisation of existing state-funded research commissions such as the Analysis and Research Service (DAO) or the Digital Affairs Committee (DiZa) could serve as an effective framework for the endeavours outlined here.

Shortcomings in lawmakers' knowledge of EDT-related issues result in not only a lag between possible and regulated use cases but also in the introduction of legislation that has adverse effects. The European Copyright Directive (ECD) provides a good example of this dynamic. Introduced in 2019, the ECD provides the EU Member States with a framework for enforcing copyright claims online. The ECD's 17th Article overhauls the long-standing precedent that social media companies are not financially liable for the damages incurred by their users hosting content that infringes copyrights on their platforms. Specifically, it reframes the aforementioned relationship so that social media companies *can* face liability charges. The Article has led to the introduction of extremely stringent (automated) content moderation systems on platforms such as Twitch and YouTube. This has resulted not only in reduced opportunities and increased risk for content creators and freelance journalists; it has also had a chilling effect on free speech, resulting in an internet that is "less diverse, interesting, equitable, and useful."[64] This is an example of overshoot.

Circumstances surrounding the ECD's implementation clearly showcase the difficulties of formulating policies that regulate modern technologies and the internet. This involves understanding the specifics of how the online creator economy, which relies heavily on "reacting" to content published through official channels, functions. It is likely that the level of sophistication of the automated moderation tools available to social media platforms, assuming that algorithms capable of nuanced moderation could easily be put in place, was overestimated, while the costs of developing such algorithms was either underestimated or it was assumed that it was financially or technologically feasible to conduct this type of moderation manually.

63 "EU Steps up Action to Strengthen EU Defence Capabilities, Industrial and Technological Base: Towards an EU Framework for Joint Defence Procurement," European Commission, May 18, 2022, https://ec.europa.eu/commission/presscorner/detail/en/IP_22_3143.

64 John Villasenor and Ally Boutelle, "The European Copyright Directive: Potential Impacts on Free Expression and Privacy," Brookings (blog), February 2, 2021, https://www.brookings.edu/blog/techtank/2021/02/02/the-european-copyright-directive-potential-impacts-on-free-expression-and-privacy/.

The challenges underlying the regulation of EDTs are, in many cases, far more nuanced – and potentially far more impactful – than those underlying an issue such as online copyrights. Backlash against the ECD highlights that a lack of policymaker awareness of the nuances surrounding the issues they regulate risks the creation of legislation that has negative economic, societal, or political impacts, but the question of how to educate ageing, not technologically disoriented class on these issues remains open. A non-comprehensive list of possible solutions is outlined in the bullets below:

For a more detailed overview of possible financial and career incentives related to policymaker awareness the reader is encouraged to consult HCSS' recent publication from October 2022: 'Reaching Breaking Point: The semiconductor and critical raw material ecosystem at a time of great power rivalry'.[65]

Implement incentives to attract talent. It is recommended to put incentives in place to draw highly skilled individuals to roles in public service. Doing so likely requires, first and foremost, providing them with competitive salary packages and including public-private interaction. A good example of such a salary structure being implemented can be observed in Singapore.[66] This incentive structure creates a dynamic in which many work in the industry or well-paying private sector jobs specifically to improve their eligibility for transitioning to high-level jobs in the civil service, allowing ministries' access to their pick of highly qualified, professional, and – above all – situationally aware individuals. It also includes strengthening both the quality and quantity of the interaction between public and private sector.

Expand existing research commissions. The Dutch Parliament has access to the work outputs generated by a series of research commissions through the DAO. One commission that the DAO has, to its credit, set up in recent years – DiZa – deals with issues relating to sensitive technologies. More specifically, DiZa, which is staffed by 34 parliamentarians and an unspecified number of civil servants,[67] provides the Parliament with information on six themes, one of which is "upcoming and future technologies". Other themes falling within DiZa's purview include digital citizenship and democracy, digital rights and ethics, digital infrastructure and economy, online safety and cybersecurity, and digital government.[68] It has worked on several relevant subjects, including how algorithms collect and use data pertaining to children, issues relating to the protection of user privacy online, and – most recently – research into AI and its use cases more generally.[69] In and of itself, DiZa's existence is positive. Its work is certain to improve parliamentarians' understanding of EDT-related activities and to contribute to the formulation of more concentrated pieces of legislation. But its sparse staffing, combined with its relatively wide focus area, means that it is unlikely to have the capacity to address all the issues that need addressing in a holistic manner. Furthermore, because the nature of DiZa's work is shaped by parliamentary requests, usually to provide context to discussions surrounding ongoing legislative proposals, its ability to shape the law-making process is limited. In an ideal scenario, DiZa's research area would be focused

65 Teer and Bertolini, "Reaching Breaking Point: The Semiconductor and Critical Raw Material Ecosystem at a Time of Great Power Rivalry," 86–87.

66 Senior civil servants in Singapore receive remunerations of between $200,000 and $260,000 per annum, depending on economic growth for the year and on officers' individual performances. Daryl Choo, "Parliament in Brief: 4 Things You Need to Know," TODAY, July 5, 2022, https://www.todayonline.com/singapore/parliament-brief-4-things-you-need-know-1936671.

67 "Samenstelling en contact van Digitale Zaken," Tweede Kamer der Staaten-General, n.d., https://www.tweedekamer.nl/kamerleden_en_commissies/commissies/diza/samenstelling.

68 "Thema's," Tweede Kamer der Staaten-General, June 9, 2021, https://www.tweedekamer.nl/kamerleden-en-commissies/commissies/digitale-zaken/thema%E2%80%99s.

69 "Kennisagenda," Tweede Kamer der Staaten-General, n.d., https://www.tweedekamer.nl/kamerleden-en-commissies/commissies/digitale-zaken/kennisagenda.

more explicitly on sensitive technologies, its staffing and available resources increased, and its role as an agenda setter – similar to (for example) the *Sociaal-Maatschappelijke Raad* (Social and Economic Council) – encoded in law.

4.4. **Reduce overreliance on East Asia within semiconductor supply chains**

Dutch, European, and North American legislators have taken concrete steps towards bolstering their domestic capacity to fabricate semiconductors or to ensure their markets remain key to the integrity of global semiconductor supply chains. Their investments in achieving these ends can be attributed to, among others, the Russian invasion of Ukraine, the prospect of a Chinese invasion of Taiwan, and the global chip shortage brought on by supply chain limitations and demand surges during the COVID-19 pandemic. Key pieces of legislation introduced since the publication of 'Taming Techno-Nationalism' include the US CHIPS Act and the yet-to-be-ratified European Chips Act. The contents of these pieces of legislation are outlined shortly in the paragraphs below.

US CHIPS Act. The CHIPS Act, which was signed into law in August of 2022, earmarks $52.7 billion in federal subsidies to boost the US' domestic semiconductor research and production. Of these $52.7 billion, an estimated $39 billion has been allocated to the construction of semiconductor fabrication plants (fabs).[70] $2 billion of the aforementioned $39 billion have been earmarked for the production of semiconductors essential to the US military, automotive, and manufacturing industries. The remainder of the allocated $52,7 billion (± $13,7 billion) will be used to foster a more robust domestic ecosystem; it will be made available to R&D and, importantly, to workforce cultivation.[71] An important caveat to the receipt of funding through the CHIPS Act is that companies which apply for and accept it are prohibited from expanding their use of fabs in China and other countries defined as posing a national security threat to the United States for 10 years. The act is, in other words, geared towards cushioning US chip designers and manufacturers from the economic losses they might incur as a result of winding down their reliance on China, as well as towards building up, creating a market for, and incentivising collaboration with US-based manufacturers such as Intel.[72] Because chip designers and chip manufacturers alike are based in the US, the CHIPS Act, especially considering the scale of the funding made available, arguably has a good chance of succeeding in achieving its objectives. A key, but unsurprising, observation to note is that the act has a clear techno-nationalist angle, with access to technology being framed as a zero-sum game and the US' contribution to fragmenting global technology markets being evident.

The European Chips Act. Based on, among others, the EC Chip Survey's finding that the industry expects demand for chips to double by 2030,[73] the Commission unveiled the

70 Frank Holmes, "What Is The Semiconductor CHIPS Act, And Why Does The U.S. Need It?," Forbes, n.d., https://www.forbes.com/sites/greatspeculations/2022/08/15/what-is-the-semiconductor-chips-act-and-why-does-the-us-need-it/.

71 "The CHIPS Act: What It Means for the Semiconductor Ecosystem," PwC, n.d., https://www.pwc.com/us/en/library/forward-now-accounting-business-news/chips-act.html.

72 "The CHIPS Act."

73 "European Chips Survey Report" (European Commission, July 2022), https://ec.europa.eu/newsroom/dae/redirection/document/89124.

European Chips Act in February of 2022.[74] Geared towards addressing semiconductor shortages and strengthening Europe's technological leadership, the Act will mobilise over €43 billion of public and private investments by 2030. As is the case with the US CHIPS Act, the European Chips Act is set to make significant amounts of money available for R&D, workforce development, and – not insignificantly – to increase European production capacity to 20% of the global market by 2030. Importantly, the European Chips Act promises to support innovative European start-ups, scale-ups, and small and medium enterprises (SMEs) in accessing equity finance, as well as to create a more investor-friendly climate for establishing manufacturing facilities within the Union. These provisions, though limited to semiconductor-related technologies specifically, are in-line with the recommendations outlined in 'Taming Techno-Nationalism', which argued for measures to improve accessibility to VC funding and private equity. The European Chips Act will supplement pre-existing initiatives, including Horizon Europe and the Digital Europe Programme, which respectively make €95.5 billion and €7.6 billion available for the development of sensitive technologies.[75]

Closer collaboration and coordination between Europe and East Asian states may also contribute to supply chain security.

As previously outlined, the Netherlands has also made significant commitments to bolster the competitiveness of domestic actors. Specifically, EZK applied, in Early 2022, for a greenlight from the EC to provide €230 million in subsidies to R&D efforts to projects run by NXP, ASML, NearField Instruments, TechnoFischer, and Smart Photonics.[76] Though the scope of this funding pales when compared to the funding made available through mechanisms such as the European Chips Act, the Dutch decision to make funding available for these companies speaks to a robust awareness of the country's competitive advantage. In investing in companies that are critical to (and unique within) international supply chains, The Hague is arguably doubling down on, and committing to maintaining, an advantage in developing and delivering a strategic good that a wider industry (and other countries by extension) are dependent on. This will likely contribute to safeguarding the Dutch relevance to semiconductor supply chains when (and if) they diversify beyond Taiwan and TSMC, a decision that will continue to pay economic and strategic dividends far into the future.

The European Chips Act may offer a relevant legislative framework for reducing overreliance on East Asia for EDT more generally. In fact, also smaller scale legislative actions such as the ones undertaken by the EZK remain valuable precedents for laying the groundwork for future legislation and incentive distribution.

In addition to reducing the Dutch strategic dependence on East Asia, the long-term investments outlined in this piece – those made within the context of the US CHIPS Act included – will also serve to reduce Dutch consumers' negative impact on the health of overseas workers. EU and US-based fabs, many of which are slated to come online by 2030, are likely to adhere to more stringent labour and environmental standards than those based in East Asia. As a consequence, the commitments announced by the Netherlands and its partners can, by and large, be understood as addressing the semiconductor-related concerns outlined throughout Chapter 3.

Enhance security of supply of semiconductors in vital sectors. It is key to manage expectations regarding the development of Dutch domestic and European advanced and mature

74 "European Chips Act: Communication, Regulation, Joint Undertaking and Recommendation | Shaping Europe's Digital Future," European Commission, February 8, 2022, https://digital-strategy.ec.europa.eu/en/library/european-chips-act-communication-regulation-joint-undertaking-and-recommendation.

75 "Funding for Digital in the 2021-2027 Multiannual Financial Framework | Shaping Europe's Digital Future," European Commission, n.d., https://digital-strategy.ec.europa.eu/en/activities/funding-digital.

76 Breton, "IPCEI on Microelectronics – A Major Step for a More Resilient EU Chips Supply Chain."

semiconductor production capacity in particular. Most experts do not expect TSMC to lose dominance within the fabrication stage of the advanced semiconductor manufacturing supply chain within the next 10 years. Instead, invitation of investment from TSMC, Intel, or Samsung to set up fabs in Europe would be a more viable avenue for increasing European production capacity. This pertains mainly to advanced semiconductors

However, Europe already possesses many strengths in terms of manufacturing mature semiconductors. While full self-reliance in terms of advanced chips is a mirage for Europe, companies like NXP are already leaders in the production of mature chips. These semiconductors are also essential for many strategic sectors, such as medical and military equipment. While many automated systems and automotives use advanced chips, the number of mature chips within the same system is usually orders of magnitude higher.[77] The medical sector relies exclusively on mature chips.

As such, European leverage over the medical sector may well be harnessed from further developing mature chip building capacity. With the exception of next generation military equipment, the defence sector also relies mainly on mature semiconductor chips. Consequently, the development of conventional and current generation arms manufacturing in Europe is also a possibility. These sectors are at a particular risk of chip shortage, as TSMC prioritises advanced semiconductors, despite the supply chain pressures on often lifesaving equipment.[78]

In addition, while Taiwan and South Korea have dominance within the advanced semiconductor market, Europe and China both possess vast capacities to manufacture mature chips. As such, Europe by developing mature semiconductor producing capacity would be both leveraging geopolitical posture and filling a pressing market vacuum.

Finally, closer collaboration and coordination between Europe and East Asian states may also contribute to supply chain security. Cooperation may entail government incentives for collaboration between the corporate and knowledge sectors.

International agreements have a role to play in, among others, reducing the impact of technology theft, reducing the risk that the use of AI or quantum computing-based technologies will escalate a conflict, reducing the prevalence of deep fakes, and counteracting the export of authoritarian use cases.

4.5. Support the creation of national and international regulatory frameworks

A key challenge to mitigating the negative effects associated with the EDTs covered in this publication is the absence of national and international regulatory frameworks. The creation of a robust set of such frameworks is vital to reducing the role that race-to-the-bottom dynamics play during the development process. By extension, it is also vital to pre-meeting the emergence of dangerous use cases and to preventing military miscalculations and miscommunications between states. International agreements have a role to play in, among others, reducing the impact of technology theft, reducing the risk that the use of AI or quantum

77 "Grootmachtcompetitie, Master Working Document - 14Nov2022.Docx," 50, accessed November 29, 2022, https://hcssnl.sharepoint.com/:w:/s/22.008PolitieStrategischeMonitor/ERjF1LNoTqtPkmvd1y2DbR0BHkY-bA1EQJgDM7BFuRRAqaw?e=72qsmv.

78 "Global Chip Shortages Put Life-Saving Medical Devices at Risk," World Economic Forum, accessed November 29, 2022, https://www.weforum.org/agenda/2022/05/global-chip-shortages-put-life-saving-medical-devices-at-risk/.

computing-based technologies will escalate a conflict, reducing the prevalence of deep fakes, and counteracting the export of authoritarian use cases.

The degree to which policies, whether at the Dutch (domestic) level, the EU level (regional), the UN level (international), or within industry associations (commercial), have been put in place to mitigate EDTs' negative impacts varies significantly by technology. As a result, this recommendations section has been split up into technology-specific subsections. Each subsection provides a non-comprehensive overview of initiatives that have already been put in place to mitigate the negative implications associated with the relevant EDTs, as well as a short overview of policy recommendations.

Unlike the other technologies included in this report, quantum computing has not yet grown so entrenched in military, government, and civilian workflows that an expectation has developed around its de-facto role in society.

The Netherlands have so far been spearheading the implementation of the present policy recommendation. For instance, earlier this year, the Netherlands will host an international summit on the responsible use of AI in the military domain.[79] It is key that such endeavours are sufficiently multilateral. This means that all parties that possess relevant capabilities must be invited, including revisionist actors and systemic rivals, such as China. Only with the inclusion of these subversive parties can the danger posed by them be mitigated in EDT-related fields.

4.5.1. Quantum computing

Quantum computing constitutes an emerging technology. Only a handful of quantum computers are operational in the world today, all of which have, to date, seen their use limited to the support of scientific projects. As research into the technology progresses, a "standardised" understanding of what constitutes a quantum computer emerges, and the technology progresses towards securing support from software developers, this status quo is set to change. As previously outlined, this is likely to result in, among others, an acceleration of military and civilian AI-based workflows, the emergence of new vulnerabilities in cyberspace, and an arms race that concerns itself with issues surrounding quantum sensing. Technology is in its infancy. From an international regulation-oriented perspective, this amounts to a significant opportunity. Unlike the other technologies included in this report, quantum computing has not yet grown so entrenched in military, government, and civilian workflows that an expectation has developed around its de-facto role in society. This means that the rules that govern this technology can aim to pre-empt (rather than mitigate) its negative effects on society. Several domestic, regional, international, and commercial frameworks have been put in place, or have started to form, for doing so. These are outlined in the bullets below:

- **Domestic**. The Netherlands has not introduced any pieces of legislation to regulate quantum computing, relying instead on the introduction of well-informed (comprehensive) EU-level regulation.
- **Regional**. Several initiatives regulating quantum computers have been put in place at the European level The European Council published a Regulation establishing the European High-Performance Computing Joint Undertaking and repealing Regulation 2018/1488 in 2021.[80] In addition, the Commission launched the European Quantum Communications

79 Ministerie van Buitenlandse Zaken, "The Netherlands to host international summit on artificial intelligence - News item - Government.nl," nieuwsbericht (Ministerie van Algemene Zaken, September 21, 2022), https://www.government.nl/latest/news/2022/09/21/the-netherlands-to-host-international-summit-on-artificial-intelligence.

80 "European High Performance Computing Joint Undertaking: Council Adopts Regulation," European Council of the European Union, July 13, 2021, https://www.consilium.europa.eu/en/press/press-releases/2021/07/13/european-high-performance-computing-joint-undertaking-council-adopts-regulation/.

Infrastructure (EuroQCI) initiative in 2019.[81] It has also made funds available for research and innovation relating to quantum computing through (among others) the Quantum Technologies Flagship programme and through Horizon Europe.[82] The EU maintains a Strategic Research Agenda for quantum technologies,[83] though no discernible amount of funding has been allocated towards the identification and mitigation of the technology's potential negative externalities.

- **International**. The World Economic Forum (WEF) has developed Quantum Computing Governance Principles. These suggest a variety of principles for governance in the dimensions of transformative capabilities, access to hardware infrastructure, open innovation, creating awareness, workforce development & capability-building, cybersecurity, privacy, standardisation, and sustainability.[84] Due to its decidedly "emerging" nature, and due to the fact that the range of its possible applications remains largely hypothetical in nature, quantum computing has not, as of yet, been subjected to a targeted arms control regime.[85]
- **Commercial**. The Institute of Electrical and Electronics Engineers Standards Association (IEEE) is actively working towards setting standards for terminology and performance metrics in quantum computing.[86] While this form of standardisation is likely to do little to mitigate the negative effects associated with quantum computers' acceleration of AI-based workflows, it *is* likely to facilitate software development and interoperability.

4.5.2. **AI**

Unlike quantum computing, AI is – by and large – an established technology. Employed daily within a multitude of industries, the technology's use cases have crystallised. There exists a clear understanding of what the technology is likely to enable going forward, though the authors consider projections beyond the 20-year mark as considerably less reliable than those before. As a result of AI's status as an "established" technology, and as a result of the technology's observable (negative) impacts on society, a not-insignificant number of efforts at regulating it can be observed at the domestic, regional, international, and commercial levels. These are outlined in the bullets below:

- **Domestic**. The Netherlands has not introduced any pieces of legislation to regulate AI. The governing coalition submitted a reflection on the EC's proposed Artificial Intelligence Act in 2020.[87]
- **Regional**. The EU has introduced a bevy of regulatory and other initiatives geared towards mitigating the risks associated with AI. The European Parliament introduced a non-binding regulation banning police from using facial recognition in public places and creating a facial

81 "EU Lays Foundation for Implementation of European Quantum Communication Infrastructure (EuroQCI)," ID Quantique (blog), February 3, 2022, https://www.idquantique.com/euroqci/.

82 "Quantum Technologies Flagship," European Commission, n.d., https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship.

83 "New Strategic Research Agenda on Quantum Technologies," European Commission, March 3, 2020, https://digital-strategy.ec.europa.eu/en/news/new-strategic-research-agenda-quantum-technologies.

84 "Quantum Computing Governance Principles," Insight Report (World Economic Forum, January 2022), https://www3.weforum.org/docs/WEF_Quantum_Computing_2022.pdf.

85 "Quantum Technologies, Their Potential Impact on the Battlefield and Future Control," Stockholm International Peace Research Institute, November 9, 2021, https://www.sipri.org/events/2021/SSC21-quantum-technologies-battlefield-future-control.

86 Walter G. Johnson, "Quantum Supremacy and the Regulation of Quantum Technologies," The Regulatory Review, December 30, 2019, https://www.theregreview.org/2019/12/30/johnson-quantum-supremacy-regulation-quantum-technologies/.

87 "Kabinetsappreciatie Witboek over Kunstmatige Intelligentie" (Ministerie van Economische Zaken en Klimaat, February 19, 2020), https://open.overheid.nl/repository/ronl-e2e92d99-4d26-48a4-bae3-e49bfb6e542a/1/pdf/bijlage-kabinetsappreciatie-witboek-over-kunstmatige-intelligentie.pdf.

recognition database in 2012.[88] The right to data protection, privacy, and non-discrimination are guaranteed under the Union's Charter of Fundamental Rights,[89], though current requirements and constraints are insufficient to ensure freedom and fairness of consent by individuals, nor to prevent the massive collection of personal data. Laws such as the Data Protection Law and Target Advertising,[90] the GDPR, and the EC's ePrivacy Directive,[91] the Data Governance Act,[92] and the DSA[93] aim to tackle some of the negative impacts associated with echo chamber creation by limiting what data corporations can collect and by allowing consumers to manage their online footprints. The EU has also embarked on an initiative to legislate a coordinated European approach to implementing AI in a way that preserves human and ethical dignity.[94] More specifically, it has proposed an approach for "Fostering a European Approach to Artificial Intelligence"[95] and drafted guidelines for "Ethical and Trustworthy" AI in 2019.[96] These guidelines have since been transposed into a proposal for a legislative framework, commonly referred to as the Artificial Intelligence Act.[97]

- **International**. 193 countries adopted an agreement regulating the "Ethics of Artificial Intelligence" in 2020.[98] Diplomats have debated autonomous weapons issues under the United Nations Convention on Conventional Weapons Group of Governmental Experts on Lethal Autonomous Weapons since 2014.[99] While discussions have done little to facilitate the emergence of a new arms control regime, they *have* helped to clarify state positions regarding the topic,[100] with major military powers having argued that existing international law is sufficient to cover autonomous weapons.[101] Limiting the proliferation of autonomous weapons systems is therefore likely to remain dependent on activism and other norm-setting activities carried out by state and non-state actors alike. It is important to note that while autonomous weapons systems do not constitute the only military application of AI, the use

Corporations can collect and by allowing consumers to manage their online footprints. The EU has also embarked on an initiative to legislate a coordinated European approach to implementing AI in a way that preserves human and ethical dignity.

88 Eileen Li, "Europe's Next Steps in Regulating Facial Recognition Technology," Columbia Journal of Transnational Law, November 7, 2021, https://www.jtl.columbia.edu/bulletin-blog/europes-next-steps-in-regulating-facial-recognition-technology.

89 Tambiama Madiega and Hendrik Mildebrath, "Regulating Facial Recognition in the EU: In Depth Analysis." (Brussels: European Parliament. Directorate General for Parliamentary Research Services, September 2021), https://data.europa.eu/doi/10.2861/140928.

90 Giovanni Sartor, Francesca Lagioia, and Federico Galli, "Regulating Targeted and Behavioural Advertising in Digital Services: How to Ensure Users' Informed Consent," September 2021, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694680/IPOL_STU(2021)694680_EN.pdf.

91 Sartor, Lagioia, and Galli.

92 "European Data Governance Act," European Commission, n.d., https://digital-strategy.ec.europa.eu/en/policies/data-governance-act.

93 Noémi Bontridder and Yves Poullet, "The Role of Artificial Intelligence in Disinformation," Data & Policy 3 (ed 2021): e32.

94 European Commission, "Proposal for a 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."

95 "Communication on Fostering a European Approach to Artificial Intelligence," European Commission, July 21, 2022, https://digital-strategy.ec.europa.eu/en/library/communication-fostering-european-approach-artificial-intelligence.

96 "Ethics Guidelines for Trustworthy AI," European Commission, April 8, 2019, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

97 Eve Gaumond, "Artificial Intelligence Act: What Is the European Approach for AI?," Lawfare, June 4, 2021, https://www.lawfareblog.com/artificial-intelligence-act-what-european-approach-ai.

98 "193 Countries Adopt First-Ever Global Agreement on the Ethics of Artificial Intelligence," UN News, November 25, 2021, https://news.un.org/en/story/2021/11/1106612.

99 "Background on LAWS in the CCW," United Nations Office for Disarmament Affairs, n.d., https://www.un.org/disarmament/the-convention-on-certain-conventional-weapons/background-on-laws-in-the-ccw/.

100 Zachary Kallenborn, "Applying Arms-Control Frameworks to Autonomous Weapons," Brookings (blog), October 5, 2021, https://www.brookings.edu/techstream/applying-arms-control-frameworks-to-autonomous-weapons/.

101 U. S. Mission Geneva, "U.S. Statement at the GGE on LAWS During the Discussion of Agenda Item 5(d)," U.S. Mission to International Organizations in Geneva, August 5, 2021, https://geneva.usmission.gov/2021/08/05/u-s-statement-at-the-gge-on-laws-during-the-discussion-of-agenda-item-5d/.

case – which covers everything from highly manoeuvrable missiles to so-called "killer robots – does account for the lion's share of AI's negative impacts within the military domain.

- **Commercial**. There are currently 39 AI-related standards under development within the context of the International Standardisation Organisation (ISO).[102] Issues affected by these standards range from defining what AI is to ensuring those developing it are working with high-quality (inclusive) data, ensuring the ensuing product is "trustworthy", and ensuring it falls under a robust governance model. Despite the continued development of these standards, signs point towards private sector actors taking relatively limited steps to reduce the invasiveness of their data collection practices and algorithms. Google fired a prominent AI ethics researcher in 2020,[103] and Facebook – now Meta – has been accused of repressing the reach of internal research that shows Instagram contributed to teen depression, among others.[104]

4.5.3. **Semiconductors**

The semiconductor industry is one which is well-established, with the foremost challenges facing it being well-catalogued. As outlined in this publication, these (from the Dutch perspective) include the risks associated with manufacturing capacity being concentrated in Taiwan and the negative environmental and inequality-based implications of their production process. Domestic, regional, and commercial-level efforts at curtailing the negative impact of these challenges are outlined in the bullets below:

- **Domestic**. The Netherlands has not taken concrete steps towards introducing legislation aimed at reducing the environmental impact of semiconductor production specifically. It *has*, as previously outlined, introduced robust initiatives for reducing the Dutch dependence on 3rd countries for microchip supply.
- **Regional**. Much as is the case with the Netherlands, EU policymaking around microchips has put little emphasis on the environmental or societal impact of their production. This notwithstanding (and as previously outlined), initiatives such as the European Chips Act,[105] the European Alliance on Processors and Semiconductor Technologies,[106] and the European Digital Decade goals all speak to the EU's commitment to reducing dependence on foreign suppliers.[107]
- **Commercial**. Centralisation within the semiconductor supply chain means that standardisation initiatives are of limited utility. This notwithstanding, TSMC and Samsung have both committed to reducing the environmental footprints of their fabs.[108] The industry's environmental footprint is likely to grow as China's SMIC ramps up production and as additional fabs come online in the US and Europe.

102 "ISO - ISO/IEC JTC 1/SC 42 - Artificial Intelligence," International Organization for Standardization, accessed October 13, 2022, https://www.iso.org/committee/6794475/x/catalogue/.

103 Tom Simonite, "A Prominent AI Ethics Researcher Says Google Fired Her," Wired, December 3, 2020, https://www.wired.com/story/prominent-ai-ethics-researcher-says-google-fired-her/.

104 Georgia Wells, Jeff Horwitz, and Deepa Seetharaman, "Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show," Wall Street Journal, September 14, 2021, https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739.

105 "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Chips Act for Europe" (Brussels: European Commission, February 8, 2022), https://ec.europa.eu/newsroom/dae/redirection/document/83086.

106 "Alliance on Processors and Semiconductor Technologies," European Commission, n.d., https://digital-strategy.ec.europa.eu/en/policies/alliance-processors-and-semiconductor-technologies.

107 "Europe's Digital Decade: Digitally Empowered Europe by 2030," Text, European Commission, March 9, 2021, https://ec.europa.eu/commission/presscorner/detail/en/IP_21_983.

108 "How We Follow Eco-Regulations," Samsung Semiconductor Global, n.d., https://semiconductor.samsung.com/content/semiconductor/global/sustainability/environment/green-chip/in-compliance-with-international-environmental-regulations.html.

4.5.4. **Space-related technologies**

Much as is the case with semiconductors and (though to a lesser extent, AI), space-related technologies constitute an "established" technology type. Technological progress has reduced the cost of entering the space domain in recent years, resulting in a handful of challenges outlined in both this publication and in HCSS' *Strategic Alert: Towards a Space Security Strategy* (2021).[109] The established nature of space-related technologies means that a handful of domestic, regional, international, and commercial-level initiatives have emerged to regulate it over the years. These are shortly outlined in the bullets below:

Among other things, the Outer Space Treaty prohibits the placement of weapons of mass destruction in the Earth's orbit and on celestial bodies.

- **Domestic**. The Dutch efforts at regulating technological and other developments pertaining to the space domain are incomplete, something which prompted this institute to recommend the government draft up a Dutch space security strategy in 2021.[110] The most important pieces of domestic legislation include EZK's *Nota Ruimtevaartbeleid* (Space Policy Note) (2019)[111] and an official letter sent to parliament by the Dutch Ministry of Foreign Affairs in 2021.[112]
- **Regional**. At the European level, the regulatory framework pertaining to space and space-related technologies is fragmented, with most Member States having formulated their own laws. This notwithstanding, the EU has introduced several relevant initiatives and/or pieces of legislation. These include, but are not limited to, the External Action Service's (EEAS) "Strategic Compass," the EU Framework for Space Surveillance and Tracking Support (EUSST), PESCO, the EDF, the EDA, the European Cooperation for Space Standardisation,[113] the European Space Agency's (ESA) Mitigation Guidelines for Limiting Space Debris,[114] and the EEAS' Safety, Security and Sustainability of Outer Space (3SOS) protocol.[115]
- **International**. The most important piece of international legislation – and one whose scope has arguably lagged behind developments in the space domain – is the Outer Space Treaty (1967).[116] Among other things, the Outer Space Treaty prohibits the placement of weapons of mass destruction in the Earth's orbit and on celestial bodies.[117] It also aims to prohibit a new form of colonial competition by stipulating that outer space is the "province of all mankind".[118] The Rescue Agreement (1968), the Liability Convention (1972), the Registration Convention (1976) and the Moon Treaty (1984) form the remainder of the

109 Hugo van Manen, Tim Sweijs, and Patrick Bolder, "Strategic Alert: Towards a Space Security Strategy," Strategic Alert (The Hague: The Hague Centre for Strategic Studies, March 2021), https://hcss.nl/wp-content/uploads/2021/03/Strategic-Alert-Space-March-2021.pdf.

110 van Manen, Sweijs, and Bolder.

111 See "Nota Ruimtevaartbeleid 2019" (The Hague: Ministerie van Economische Zaken, 2019), https://open.overheid.nl/repository/ronl-57ade8f5-c87b-4d6d-887b-cde374fee2a5/1/pdf/bijlage-1-nota-ruimtevaartbeleid-2019.pdf.

112 See Stef Blok, "Betreft Introductie Ruimteveiligheidsbeleid" (The Hague: Ministerie van Buitenlandse Zaken, March 5, 2021), https://open.overheid.nl/repository/ronl-36c57cee-a2ae-480b-b3d7-466bc1d71caa/1/pdf/kamerbrief-inzake-introductie-ruimteveiligheidsbeleid.pdf.

113 "European Cooperation for Space Standardization," European Cooperation for Space Standardization, n.d., https://ecss.nl/.

114 "Mitigating Space Debris Generation," European Space Agency, n.d., https://www.esa.int/Space_Safety/Space_Debris/Mitigating_space_debris_generation.

115 "SOS SOS SOS : EU Calls for Ethical Conduct in Space to Avoid Collision and Orbital Debris," European Union External Action, September 19, 2019, https://www.eeas.europa.eu/eeas/sos-sos-sos-eu-calls-ethical-conduct-space-avoid-collision-and-orbital-debris_en.

116 Cassandra Steer and Matthew Hersch, War and Peace in Outer Space: Law, Policy, and Ethics, Ethics, National Security, and the Rule of Law (Oxford: University Press, Incorporated, 2021).

117 Jinyuan Su, "The Legal Challenge of Arms Control in Space," in War and Peace in Outer Space: Law, Policy, and Ethics, ed. Cassandra Steer and Matthew Hersch (Oxford University Press, 2020), 0.

118 Dave Webb, "The Ethical Use of Outer Space," in Ethical Engineering for International Development and Environmental Sustainability, ed. Marion Hersh (London: Springer, 2015), 16.

UN's foundational space treaties.[119] The United Nations Office for Outer Space Affairs (UNOOSA) was founded in 1958 to support governments in the creation of their legal, technical and political infrastructure to pursue space activities while also having a registry of objects launched into Outer Space.[120] The organisation published twenty-one guidelines for the long-term sustainability of outer space activities in 2019. These include everything from recommendations for revising regulatory frameworks for outer space activities at the national level to best practices for ensuring the safety of space operations.[121] The UN has also published a set of Space Debris Mitigation Guidelines (2010).[122] Importantly, space has been relatively absent in disarmament and arms control debates.[123]

- **Commercial**. There are no concrete, centralised efforts within the corporate sphere to mitigate the risks associated with space-related technologies. This notwithstanding, an industry norm against allowing defunct satellites to remain in orbit has taken hold in recent years. This is likely due to the orbital congestion that is set to follow the activation of constellations such as SpaceX's Starlink, which are set to be made up of tens of thousands of individual satellites.

4.6. Strengthen Dutch and European legislation regulating social media platforms

The question of how, and if, to regulate speech on social media platforms is complicated for two reasons. First and foremost, taking a top-down approach to regulating what individuals *can* and *cannot* post on social media infringes on the right to free speech.[124] In instances where government regulations on speech do not infringe on rights guaranteed to citizens under national legislation, the introduction of such regulations risk being politicised, drawing negative attention to and fostering resentments against the sitting government. Second, moderation problems differ significantly by platform. The exact characteristics that shape and inform how mis and disinformation spread on a platform such as Facebook are different from the characteristics that shape and inform how they spread on Twitter, YouTube, TikTok, or Reddit.

Untangling the complexity brought on by these factors is problematised by the fact than in depth understanding of the subject area is necessary to craft policies capable of addressing the issue in a comprehensive manner. While implementing the policies outlined in Section

119 Sophie Goguichvili, Alan Linenberger, and Amber Gillette, "The Global Legal Landscape of Space: Who Writes the Rules on the Final Frontier?," Wilson Center, October 1, 2021, https://www.wilsoncenter.org/article/global-legal-landscape-space-who-writes-rules-final-frontier.

120 Goguichvili, Linenberger, and Gillette.

121 UN COPUOS has formulated a relatively comprehensive set of voluntary guidelines. For a full overview, see "Report of the Committee on the Peaceful Uses of Outer Space," General Assembly Official Records Seventy-Fourth Session Supplement No. 20 (United Nations General Assembly, June 21, 2019), https://www.unoosa.org/res/oosadoc/data/documents/2019/a/a7420_0_html/V1906077.pdf.

122 "Space Debris Mitigation Guidelines of the Committee on the Peaceful Uses of Outer Space" (Vienna: United Nations Office for Outer Space Affairs, 2010), https://www.unoosa.org/pdf/publications/st_space_49E.pdf.

123 John Lauder, Frank G. Klotz, and William Courtney, "How to Avoid a Space Arms Race," October 26, 2020, https://www.rand.org/blog/2020/10/how-to-avoid-a-space-arms-race.html.

124 The legalese surrounding this issue depends on jurisdiction. In the United States, where the right to free speech is guaranteed under the Constitution, the government has little to no tools for moderating speech online. In the Netherlands – and in much of Europe – laws against hate speech allow some leniency to regulators.

4.1, which outlines how to increase awareness and understanding of EDTs at the macro level, there are several steps the Dutch government can take towards reducing the degree to which the recommendation algorithms utilised by social media platforms contribute to the undermining of the democratic process through the proliferation of mis- and disinformation. These are outlined in the bullets below:

Refine regulation concerning social media. The problem of social media companies not doing enough to moderate speech on their platforms stems, in no small part, from the fact that these companies are averse to being accused of censoring free speech. In practice, this means that companies draft up community guidelines – often enshrined in the platform's terms of service – outlining what forms of speech are and are not allowed. It allows companies to avoid legal challenges when users are removed from their platforms as a result of engaging in hate speech. But there are steps that can be made to climb down on expressions on social media that are not in compliance with Dutch law pertaining to discrimination, hate speech, and violence incitement. First, the vast majority of major platforms (Facebook, Instagram, Discord, etc.) only take an active role in removing forms of political expression that amount to "hate speech" or calls to violence. This leaves the platforms open to the publication of reams of potentially damaging content, including racial slurs. Second, platforms view the implementation of more restrictive guidelines and the development of technologies capable of automating moderation in an effective way as amounting to a comparative disadvantage. As a result, they are unlikely to take these steps without their competitors being forced to do the same. This leaves an opportunity for state legislators to step in – an eventuality that platforms have frequently expressed openness for.[125] The Netherlands should introduce robust penalties for social media companies that fail to moderate their platforms in a way which aligns with articles 137c and 137d of the Dutch Penal Code pertaining to discrimination and violence incitation.[126]

Social media companies cannot, under current EU or Dutch law, be held liable for the content users place on their platforms.

Increase platform liability. In the United States, online platforms are – under Section 230 of the Communications Decency Act – absolved of liability for the content users place on their platforms. Intended to shield internet service providers (ISPs) from liability for providing consumers with access to the internet, Section 230 has also played a significant role in reducing social media platforms' commitment to moderating their platforms. Similarly to how they are treated in the US, social media platforms in the EU are treated differently from publishers. More specifically, unlike publishers, social media companies cannot, under current EU or Dutch law, be held liable for the content users place on their platforms. It is a missed opportunity. Algorithmic amplification is specifically geared towards making what are, in essence, editorial decisions about content and providing individual users with tailored experiences. This means that, while social media companies do not (unlike publishers) develop and publish content, they *are* responsible for determining what content their users do and do not interact with – often at a far larger scale. The EU's DSA and DMA will regulate social media platforms in a way that aligns more closely to how publishers are moderated, but will not come into effect until January of 2024. The Netherlands should put in place a law that emulates Germany's Network Enforcement Act (NEA) in the meantime.[127] This means formulating clear

125 "Why Facebook Wants To Be Regulated?," Management Study Guide, n.d., https://www.managementstudyguide.com/facebook-wants-to-be-regulated.htm.

126 "Criminal Code: Act of 3 March 1881," Criminal Code § (1881), https://www.ejtn.eu/PageFiles/6533/2014%20seminars/Omsenie/WetboekvanStrafrecht_ENG_PV.pdf.

127 "Germany: Network Enforcement Act Amended to Better Fight Online Hate Speech," web page, Library of Congress, Washington, D.C. 20540 USA, 2021, https://www.loc.gov/item/global-legal-monitor/2021-07-06/germany-network-enforcement-act-amended-to-better-fight-online-hate-speech/.

guidelines for what constitutes hate speech or not and fining companies in instances where they fail to take down hate speech.

Mandate explainability. A third avenue, through which to regulate algorithmic amplification's contribution to the spread of mis- and disinformation on online platforms involves the regulation of algorithmic explainability. Most online platforms – see for example Facebook, TikTok, or YouTube – treat the workings of their algorithms as trade secrets. Considering the fact that content recommendation algorithms play a central role in shaping their respective user experiences and engagement, this position is unsurprising. But treating amplification algorithms as trade secrets limits regulators' ability to review how they work and, more specifically, to critique what ends they are optimised towards achieving. Mandating that algorithms be "explainable" constitutes a middle ground towards open-sourcing them and maintaining the competitive advantages they provide to the companies that developed them. More concisely, Dutch regulators should put laws in place that require algorithms to be able to outline what variables contributed to specific decisions being made (i.e.: recommending a video or a group to thousands of people). This will allow Dutch policymakers to develop an insight into the "thinking" behind these algorithms' decision-making and, if appropriate, to craft policies to alter their behaviours.

Mandating that algorithms be "explainable" constitutes a middle ground towards open-sourcing them and maintaining the competitive advantages they provide to the companies that developed them.

Consider alternate "slowdown" options. Another option for reducing algorithmic amplification's (negative) impact on the democratic process is to, rather than removing all misinformation or hate speech from a platform, limit how far – and how quickly – these types of content can be disseminated. The options for achieving this end are extremely diverse, with many mechanisms having already been put in place by social media companies. As an example, Twitter registers whether users have opened a link to an outside source when the share button is pressed, prompting them to consider opening the link before sharing it with their networks if they have not. Several platforms, YouTube, Facebook, and Twitter included, have systems in place for reducing the reach of questionable content. In Twitter's case, the retweet and share options are disabled for tweets containing hate speech or other forms of borderline content. On YouTube, videos containing content that borderline infringes on the platform's community guidelines may be demonetised, limiting the financial incentives associated with developing such content in the first place. Virtually all platforms have been accused by opponents of algorithmically limiting the reach of borderline content, a practice that many pundits have lamented as "shadow banning" or "de-platforming". All of this speaks to the notion that there *are* options for reining in the spread of mis and disinformation that fall short of disallowing these forms of speech altogether.

Pursue antitrust options. A final solution for changing social media companies' approaches to algorithmic amplification is to pursue antitrust options. The Netherlands is something of a trailblazer as far as wielding antitrust is concerned, with a recent lawsuit having forced Apple to reconsider payment options for in-app purchases in Apps such as Tinder and OkCupid.[128] The EU has also taken a robust approach to antitrust, with companies such as Google and Facebook having been fined billions of Euros in recent years.[129] Pursuing antitrust cases and establishing legal precedents that increase the space for competition in the online space holds at least some potential for reducing the impact of algorithmic amplification.

128 Mitchell Clark, "Apple's Giving up Ground in Its App Store Fight with Dutch Regulators and Tinder," The Verge, June 11, 2022, https://www.theverge.com/2022/6/10/23163277/apple-third-party-payment-rules-update-acm-dutch-dating-apps-netherlands.

129 "Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service," Text, European Commission, June 27, 2017, https://ec.europa.eu/commission/presscorner/detail/es/MEMO_17_1785.

For one thing, it opens the door for the emergence and growth of new companies – and, quite possibly, the development of new types of recommendation algorithms. For another, it creates pressure on current market leaders to adjust how their platforms work, even if doing so is not explicitly mandated by law. Several potential antitrust cases could be pursued within the social media space today, including (but not limited to) Facebook's (now Meta's) acquisition of Instagram, Google's acquisition of YouTube, and Apple's and Google's control over iOS and Android through the App Store and the Google Play Store respectively.

Europe must leverage its strength as an economic powerhouse with a vast market, advanced knowledge sectors, and highly educated workforce, to create European champions that can globally compete in EDT sectors.

4.7. Facilitate the development of European champions and coalitions of the willing

The emergence of EDTs brings back to the fore the question whether states should take an active role in control over national enterprises. By taking a fully laissez-faire approach, the European markets suffer if their knowledge infrastructures simply lack either the know how or the resources to create and produce cutting edge technologies. The risk there is not just to prosperity but also to national and international security at large. At the same time, centralised planning and heavy state involvement have not always been conducive to the innovative and competitive edge of nations' economies, as twentieth century experience in both the Soviet Union and in Western Europe attest to.

European policymakers will need to approach this issue strategically but in a balanced manner . State engagement and direction must focus on vital sectors and utilise incentives and coordination rather than outright central planning.

Develop European champions. Size and scale matter, also in the 21st century innovation landscape. Europe must leverage its strength as an economic powerhouse with a vast market, advanced knowledge sectors, and highly educated workforce, to create European champions that can globally compete in EDT sectors. This will be a key pillar of European strategic autonomy going forward.

Leverage Dutch strengths in EDT and demand something in return. Policymakers are advised to recognise and wield the leverage stemming from their bottleneck role and their innovative edge in EDTs. For instance, the US' recent call to ASML to suspend China's access to high-end lithography machines is an opportunity for the Netherlands can be heeded but in return other benefits should be granted through issue linkage. For instance, the 2022 acquisition of a mere 96 Patriot Advanced Capability Guidance Enhanced Missiles (PAC-2 GEM-T) for $1.22B could have been negotiated on terms more advantageous to the Netherlands.[130] Within this domain, in the future it can include a greater role for Dutch corporations in EDT-intensive projects, for instance in the development of the F-35 Lightning II fighter jet (in which the Netherlands is currently a level two partner along with Italy), or the Transatlantic development of Raytheon manufacturing plants in the Netherlands (perhaps in cooperation with Thales).

130 DSCA, "Press Release - Netherlands 22-47 CN," accessed November 2, 2022, https://www.dsca.mil/sites/default/files/mas/Press%20Release%20-%20Netherlands%2022-47%20CN.pdf.

Subsidise deeper integration of the military and civilian sectors to enhance Dutch and European resilience. EDT-related challenges encompass all of society. That said, EDTs' implications are particularly pronounced within the defence sphere. The risks and opportunities pertaining to EDTs' impact on warfighting capabilities are far-reaching. The threat of foreign deployment of EDT-enhanced capabilities is one of the primary threats to national security within the EDT framework of analysis. However, wielding EDT-empowered capabilities in an ethical and refined manner may be the greatest leverage for safeguarding liberal democracies and corresponding practices. As such, cooperation between the military and civilian spheres must be incentivised. The rationale for this is multivariate. First, the military potential of EDTs may be harnessed to a higher degree. Second, given the strategic level threat posed by the deployment of foreign EDT-empowered technologies, their securitisation must be conducted in a societally holistic manner. Closer civil-military alignment and fusion through incentives and cooperative frameworks will enhance the integration of the military and civilian sectors when it comes to the challenges posed by EDTs.

4.8. **Final Remarks: Call for Action**

The EDTs covered in this study are associated with a wide range of threats and opportunities within the ethical, judicial, democratic, and military domains. As outlined in Chapter 3, this leads to a range of opportunities to enhance Dutch prosperity and security. At the same time, the threats also need to be addressed. More specifically, a range of initiatives need to be introduced to shield the Netherlands from the negative effects of competition over EDTs. National access to and control over EDTs is increasingly taking on the form of a zero-sum game. The weaponisation of access to EDTs will likely pervade in the coming years of instability and geopolitical competition. Some dimensions of the strategic rivalry, such as disinformation campaigns on social media platforms and pressures on ASML to restrict EDT exports to some countries have already been apparent. These phenomena will increasingly encompass EDTs in light of the Russian invasion of Ukraine and, most significantly, the increasing Sino-American competition over leadership in the next industrial revolution. As the barriers to developing and accessing sensitive technologies are exceptionally high, European policymakers should seek to reduce the European innovation ecosystem's vulnerability to techno-nationalist practices and improve Europe's ability to compete internationally. Additionally, addressing the challenges associated with EDTs will help to prevent these technologies from undermining the democratic legal order, infringing on basic (ethics-based) norms and values, violating judicial processes, and exposing it to the negative effects of a race-to-the-bottom within the military domain. Fulfilling the aforementioned guidelines and recommendations formulated in this report should remain a key priority. Although some significant steps have been made since 2021 toward this end, much remains to be done. The time to act is now.

The Hague Centre
for Strategic Studies

Annex

Emerging Disruptive Technologies in an Era of Great Power Competition

Hugo van Manen, Stella Kim, Adam Meszaros and Michal Gorecki
Contributions by: Rob de Wijk, Frank Bekkers, Joris Teer and Tim Sweijs

As competition over access to and control over emerging (and) disruptive technologies (EDTs) intensifies, these technologies' (negative) impact on society is likely to increase. The intensified competition will probably result in, among other things, an uptick in the rate at which EDTs are developed and iterated. It is also likely to contribute to a tendency to treat their development as a race to the bottom. It will plausibly result in the developers of these technologies being largely unconcerned with foreseeing and taking steps to mitigate the risks associated with their use. In the case of some EDTs – and artificial intelligence (AI) most prominently – race-to-the-bottom dynamics' contribution to the manifestation of negative externalities in our daily lives can already be observed. The Cambridge Analytica scandal and the polarisation that has come to characterise the United States and other liberal democracies' political systems in recent years can, in no small part, be attributed to Meta's decision to optimise for engagement on Facebook, with the platform's ability to automate auditorial decisions being the likely culprit. In the case of other EDTs, their impact has yet to manifest in earnest, though the contours of what is likely to occur in the future can be observed in the present.

Table 4: Summary of threats and opportunities associated with EDTs

Access to EDTs			
Threat #	**Threat description**	**Opportunity #**	**Opportunity description**
1	Intensification of technology theft	1	Increase in policymaker awareness and understanding
2	Uptick in issue linkage	2	Increase in demand for highly educated individuals
3	Acceleration of China's semiconductor capabilities	3	Support for bolstering applied research capacity
4	Increases in the cost of consumer goods	4	Increases in government funding
5	Tech market fragmentation	5	Increase in amiability for international cooperation
Warfighting Capabilities and EDTs			
Threat #	**Threat description**	**Opportunity #**	**Opportunity description**
6	Overdependence on 3rd countries	6	Increased pressure opens the door to new legislation
7	Adversarial states are likely to gain access independently	7	EDTs offer pathways to cost reductions for military operators
8	Increases in demand for semiconductors	8	Significant operational benefits enabled by EDTs
9	Risk of conflict escalation		
10	Competition incentivises corner cutting during development		
Societal Impacts of EDTs			
Threat #	**Threat description**	**Opportunity #**	**Opportunity description**
11	Alienation and disillusionment on social media	9	Automation of content moderation and "deep fake" detection
12	Democratisation and proliferation of convincing "deep fakes"		
13	Cementing of authoritarian governance models abroad	10	Judicial cost reductions as a result of automation
14	Biases in judicial automation processes		

This publication catalogues EDTs' negative impact within the ethical, judicial, democratic, and military domains. The choice of these domains, and the exclusion of the economic domain, can, first and foremost, be attributed to the research goals formulated by the Dutch Ministries of Foreign Affairs and Defence. Another factor informing the authors' adherence to the ethical, judicial, democratic, and military domains is that EDTs' impact within them is set to be significant in the medium-short term. The democratic and ethical domains, in particular, face significant challenges as a result of the introduction of EDTs, with AI and, in the longer run, quantum computing posing the most significant threats to these domains' integrity. A final consideration worth noting is that, in the case of many EDTs, the technology-specific impacts within the

(omitted) economic domain are too numerous to address them feasibly in this publication. For instance, AI's economic impacts can be observed across industries and differ significantly by the industry and the use case the technology is employed to fulfil. Covering a technology such as AI's economic impact within a single industry in a comprehensive manner would likely require a full report. Covering the economic impact of four technologies, in addition to those technologies' impacts within the ethical, judicial, democratic, and military domains within a single publication, is simply unfeasible. A short description of the factors considered within each domain is provided below:[1]

- **Ethical.** The ethical domain spans occurrences across a wide range of societal issues, including (but not limited to) human rights and individual-level privacy. The domain centres around exploring how use cases associated with covered EDTs might infringe on the norms and values that are upheld or championed by or within the Netherlands.
- **Democratic.** The democratic domain explores covered EDTs' impact on the democratic process. More specifically, it outlines how EDTs can disrupt the electoral process itself, how they can contribute to polarising and disillusioning voters at the individual level, and through what mechanisms they provide opportunities to foreign or domestic actors to exacerbate these processes.
- **Judicial.** The judicial domain explores EDTs' impact on the judicial process. It can manifest in two ways. First, EDTs can impact the day-to-day activities of law enforcement organisations in negative ways, providing officers with bad incentives or resulting in damaging forms of ethnic or other profiling. Second, they can impact the sentencing process.
- **Military.** The military domain explores EDTs' impact on warfighting capabilities. More specifically, it outlines how EDTs are, and are likely to continue, changing the character of war (read: how wars are fought) on the one hand and how they are set to continue impacting warfighting strategies going forward.

The authors acknowledge EDTs' likely impact on the economic domain and societal prosperity. To correct for their omission in this chapter and to allow for the formulation of policy recommendations that address – as outlined in Chapter 3 – the problem of techno-nationalist measures undermining the Dutch strategic autonomy, an in-depth description of the economic and strategic implications of losing access to EDTs is offered in Chapters 3 and 4.

The EDTs covered in this section are quantum computing, AI, semiconductors, and space-related technologies. As is the case with the choice of impact domains (outlined above), this choice of technologies has been informed, first and foremost, by research goals formulated by the Dutch Ministries of Foreign Affairs and Defence. The omission of (for example) bio or nanotechnologies constitutes, from the authors' perspective, a significant oversight – particularly given the study's domain choices. This notwithstanding, quantum computing, AI, semiconductors, and space-related technologies constitute EDTs that are topical to shaping international competition – something which makes them highly relevant to the policy recommendations offered in later chapters. They are among the most relevant to driving negative forms of interstate competition. It means that they are likely to be most affected by race-to-the-bottom dynamics, that their negative impacts can generally be conceptualised as being more likely to manifest, and that they are likely disproportionately affected by

1 Because EDTs' impacts within these domains differs a.) by specific sub-technology and/or application, and b.) by the timeframe within which they are likely to manifest, the per-technology (negative) externalities described within this section should not interpreted as comprehensive. Unless otherwise specified, the authors have generally prioritized the inclusion of externalities which are unfolding – and, therefore, require attention – in the here and now, or which are expected to unfold within the next five to ten (5-10) years. Externalities which are expected to manifest beyond the aforementioned 5-10 year timeframe have generally only been included because the authors deem them worrisome enough to warrant immediate attention and/or awareness.

techno-nationalist practices in the near future. Not insignificantly, the Netherlands possesses a robust infrastructure for pushing forward – and, in the case of semiconductors, arguably even for shaping – how these technologies and the international discussions around them develop.[2] Added to the fact that the Netherlands is likely to remain a net consumer of each of these technologies going forward, these factors mean that the Netherlands has a vested interest in mitigating their (negative) impact on the foreign and domestic fronts. In addition, their use and continued development also have the potential to profoundly impact the ethical, democratic, judicial, and military domains, despite the degree to which each of these technologies are likely to impact all covered domains is somewhat uneven.

This section provides a short, per-technology (quantum computing, AI, semiconductors, space-related technologies) and per-domain (ethical, judicial, democratic, and military) description of the negative impacts associated with their most reported-on current (and, where applicable, future) use cases. Each subsection provides a short description of the technology, outlines its high-level findings in a Table, and provides a short description of per-domain externalities.

Quantum Computing

A quantum computer performs computation by influencing specific characteristics detailed by quantum mechanics.[3] Whereas current-gen computers work by transforming information into binary digits (bits) which have either the value 0 or 1, the information transformed by quantum computers can be in a state of being both 0 and 1 at the same time.[4] It allows quantum computers to conduct computations at significantly higher speeds than current-gen computers.[5] These improved operational abilities are evident in the numbers: Google in 2019 stated its quantum computer, Sycamore, is 158 million times faster than its classical computers. The company designed a calculation that would have taken IBM's supercomputer – the world's most powerful supercomputer – 10.000 years to complete.[6] Sycamore completed the calculation in 200 seconds.[7]

2 The exceptions to this rule are arguably quantum computing and AI, both of which are technologies that Dutch institutions have contributed to through theoretical (but not applied) research.

3 Jack D. Hidary, Quantum Computing: An Applied Approach, 2021.

4 Engineering National Academies of Sciences et al., Quantum Computing: Progress and Prospects, A Consensus Study Report of the National Academies of Sciences, Engineering, Medicine (Washington, D.C: National Academies Press, 2019).

5 Harrison Brooks, "Quantum Computers: Opportunities, Risks, and Challenges for Policymakers," American University, November 16, 2021, https://www.american.edu/sis/centers/security-technology/quantum-computers.cfm.

6 Bernard Marr, "What Is The Impact of Artificial Intelligence (AI) On Society?," Bernard Marr & Co., accessed April 4, 2022, https://bernardmarr.com/what-is-the-impact-of-artificial-intelligence-ai-on-society/#:~:text=Artificial%20intelligence%20can%20dramatically%20improve,creativity%20and%20empathy%20among%20others.; Vidar, "Google's Quantum Computer Is About 158 Million Times Faster Than the World's Fastest Supercomputer," February 28, 2021, https://medium.com/predict/googles-quantum-computer-is-about-158-million-times-faster-than-the-world-s-fastest-supercomputer-36df56747f7f.

7 Annarita Giani and Zachary Eldredge, "Quantum Computing Opportunities in Renewable Energy," SN Computer Science 2, no. 5 (September 2021): 393.

Table 5: Summary: risks associated with quantum computing

Judicial[8]

- Quantum computers' acceleration of AI-based workflows is likely to require regulation, with algorithms requiring large datasets are certain to grow more robust – and more invasive – as a result of quantum acceleration. Examples include:
  - o User databases of social media companies used for targeted advertising
  - o Patient databases of hospitals documenting medical history
  - o Credit and debit card purchase histories
  - o Users' visitation history on websites documented by cookies (online footprint)
- Quantum computing will enable new forms of cybercrime due to its ability to break through various encryption techniques. For instance, quantum computers pose dangers within the following types of cybercrime:
  - o Blockchain technology and crypto-wallet decryption
  - o Hacking into traditional financial systems, such as:
    - Trading via the stock market
    - Bank accounts
    - Credit scores
  - o Infringing on privacy and online anonymity
  - o Copyright infringement and intellectual property theft
  - o Abuse of facial recognition technology
  - o Hacking into social engineering experiments, such as the social credit system in China
  - o Decrypting even computer-generated passwords
  - o Developing more advanced ransomware
  - o Making the Dark Web inaccessible to authorities, who do not themselves possess quantum technology
- There remains legal uncertainty around the patentability of quantum computing systems.
- Social media companies may harness the power of quantum computing unethically without regulation from the state.

Ethical[9]

- Development of and access to quantum computers is shaping up to be extremely unequally distributed, meaning that the computing technology is likely to widen existing power gaps between rich and poor countries.
- Quantum computers require – among other materials – hexagonal boron nitride and niobium diselenide to operate. The resulting ethical risks are two-fold:
  - o Environmental – given the pollution related to mining operations
  - o Human rights-related – given the poor track record of countries with major deposits
- Research into quantum computing is commonly targeted for theft through student exchange programmes, raising concerns about whether universities should continue to accept foreign students into relevant programmes.
- During data mining operations that use quantum computing technology the individual's rights to privacy may be harmed, given the invasive practices of some actors – mainly social media and advertising companies – being potentially exacerbated by quantum computing capabilities.

Democratic[10]

- Quantum computing's capacity to process large sets of data will pose considerable risks to democratic processes. For instance:
  - o The 'echo chamber' effect will grow more prominent on social media platforms due to more efficient content recommendations based on pre-existing identity patterns.
  - o Political actors may adjust their communications to social media trends more accurately, thereby increasing populism.
  - o Propaganda will resonate better with popular sentiments, as AI capabilities and quantum technology together will generate such content en masse.
  - o Totalitarian regimes, such as China, will further develop their societal surveillance and credit systems.
  - o Due to rising extremism in democracies, such alternatives may garner support as a legitimate model.
  - o 'Deep fakes' produced about prominent figures may contribute to the trend of 'fake news', thereby eroding trust in public institutions and increasing hyper normalisation.
- The above processes may accelerate democratic backsliding in young democracies and hybrid regimes.
- They may also undermine social cohesion and the integrity of democratic processes in liberal democracies by exacerbating pre-existing issues.
- They may solidify the grip of autocratic and totalitarian regimes (such as Russia or China) on their populations, especially in ethnic minority regions via mandatory DNA samples, Wi-Fi network monitoring and facial recognition cameras.

Military[11]

- Quantum technologies allow for substantially improved measurement, sensing, stealth detection and other positioning, and precision capabilities. These may entail:
  - o Integrated Air and Missile Defence (IAMD)
- Autocannons, CWAS, and air defence systems will improve their accuracy
- Improved early warning capabilities
- Improved fire control and generally C2 capabilities
  - o Sixth-generation fighters (such as the NGAD programme) and self-propelled air defence systems may serve as command centres in their own right.
- Quantum technologies will likely impact navigation and timing (PNT)-related objectives. Quantum sensing is the most mature quantum technology available to military operators. These may entail:
  - o Automated formation flying between sixth generation fighters and their surrounding UACVs
  - o General improvements in interoperability and capability enhancement between weapon systems (such as the F-35 improving the on-board computer of surrounding fourth-generation fighters, just by flying in the same formation).
- As secure communication and information sharing are crucial to military operators, the interception of quantum computers is likely to require an overhaul of military digital infrastructures. In particular:
  - o Infrastructure relying on cryptography will need to be upgraded to be quantum resistant through either quantum cryptography or post-quantum cryptography.
  - o Jamming technology of enemy communications and sensors will have to become more sophisticated.

8 Ronald de Wolf, "The Potential Impact of Quantum Computers on Society," Ethics and Information Technology 19, no. 4 (December 2017): 271–76; Vikas Hassija et al., "Present Landscape of Quantum Computing," IET Quantum Communication 1, no. 2 (2020): 42–48; Mauritz Kop, "Quantum Computing and Intellectual Property Law," n.d., 10.

9 Elsa B. Kania and John K. Costello, "The Second Quantum Revolution" (Center for a New American Security, 2018), JSTOR; Kania and Costello, "The Strategic Implications of China's Quantum Leaps"; Hassija et al., "Present Landscape of Quantum Computing"; Rahul Matthan, "Prepare for a World of Quantum Haves and Have-Nots," mint, February 4, 2020, https://www.livemint.com/opinion/columns/opinion-prepare-for-a-world-of-quantum-haves-and-have-nots-11580833439895.html; Adam Zewe, "Tiny Materials Lead to a Big Advance in Quantum Computing," Massachusetts Institute of Technology, January 27, 2022, https://news.mit.edu/2022/tiny-materials-quibits-quantum-computing-0128; King Alexander, "This Is Not New - A Short History of Materials Criticality and Supply-Chain Challenges," in Critical Materials (Elsevier, 2021); Michael Raska, "Strategic Competition for Emerging Military Technologies," PRISM 8, no. 3 (2019): 64–81; Danah Zohar, "Governing a Quantum Society: Two Models," in Zero Distance, by Danah Zohar (Singapore: Springer Singapore, 2022), 229–41.

10 Anupama Chadha et al., "Deep fake: An Overview," in Proceedings of Second International Conference on Computing, Communications, and Cyber-Security, ed. Pradeep Kumar Singh et al., Lecture Notes in Networks and Systems (Singapore: Springer, 2021), 557–66; Mika Westerlund, "The Emergence of Deep fake Technology: A Review," Technology Innovation Management Review 9, no. 11 (January 1, 2019): 39–52; Andrei Kwok and Sharon Koh, "Deep fake: A Social Construction of Technology Perspective," Current Issues in Tourism, March 14, 2020, 1–5; Elsa B. Kania and John K. Costello, "The Strategic Implications of China's Quantum Leaps" (Center for a New American Security, 2018), JSTOR; Nicholas D Wright, "Artificial Intelligence and Democratic Norms: Meeting the Authoritarian Challange," Sharp Power and Democratic Resilience (National Endowment for Democracy, August 2020), https://www.ned.org/wp-content/uploads/2020/07/Artificial-Intelligence-Democratic-Norms-Meeting-Authoritarian-Challenge-Wright.pdf.

11 Andrew Davies and Patrick Kennedy, "Quantum Sensing," From Little Things (Australian Strategic Policy Institute, 2017), JSTOR; Kania and Costello, "The Strategic Implications of China's Quantum Leaps"; Raska, "Strategic Competition for Emerging Military Technologies"; Stew Magnuson, "Quantum Technology," National Defense 103, no. 784 (2019): 20–25; Michal Krelina, "Quantum Technology for Military Applications," EPJ Quantum Technology 8, no. 1 (December 2021): 24; Michiel van Amerongen, "Quantum Technologies in Defence & Security," NATO Review, June 3, 2021, https://www.nato.int/docu/review/articles/2021/06/03/quantum-technologies-in-defence-security/index.html.

The computing power unlocked by future quantum computers – though dependent on industry-wide changes in application architecture and widespread adoption – will bring major societal, economic, and military advantages. It will also supercharge existing (hybrid) threats and facilitate the introduction of new ones. In addition, as with many cutting-edge technologies. Ethical and judicial dilemmas associated with sourcing the raw materials needed for manufacturing and operating quantum computers appear. The hardware is highly unstable and is extremely sensitive to outside disturbances. Current quantum computers require an environment which offers a temperature of -273°C, barely any atmospheric pressure, and isolation from the Earth's magnetic field.[12]

Perhaps the most important ethical challenge associated with quantum computing is that, as with virtually all cutting-edge technologies, the development of and access to this technology is shaping up to be extremely unequally distributed. Most of the companies investing in quantum computing are American. Google, IBM, Microsoft and Intel arguably lead the world in developing and conceiving use cases for quantum computing. Because quantum research is exorbitantly expensive, this dynamic is unlikely to change soon.[13] American (or, quite possibly, Chinese) companies are set to dictate what workflows quantum computers are likely to be employed in, at least in the near future. In the case of Chinese quantum computing projects, quantum computers' use within societal control mechanisms – and the export thereof – is likely, at least from an EU perspective, to top the list of ethical concerns. It is particularly true within quantum computing's ability to overcome classical cryptography – something which is certain to transpose into a significant reduction in online privacy.[14] At the international level, quantum computing is likely to widen existing power gaps between rich and poor countries. Developing countries will inevitably lag behind in adopting advanced cryptographic approaches and securing access to quantum computers.[15] Another ethical challenge associated with quantum computers centres around sourcing materials required to develop quantum computing. Specifically, quantum computers require – among other materials – hexagonal boron nitride and niobium diselenide to operate.[16] The top 5 hexagonal boron nitride exporters are 3M (US), Denka Company (Japan), HC Starck (Vietnam), Saint-Gobain (France) and Showa Denko (Japan).[17] Brazil currently produces around 85% of the world's needs in niobium.[18] Another important material is helium-3, an element which is used to achieve the extremely low temperatures and to reduce noise or interference.[19] US, Qatar, Algeria, Australia, Russia, Poland, and Canada are the leading helium-exporting countries.[20]

The technology also faces challenges on the judicial front. Because they remain decidedly emerging as a technology area, quantum computers are currently subjected to very little

12 BBVA, "Quantum Computing: How It Differs from Classical Computing?," NEWS BBVA (blog), December 10, 2019, https://www.bbva.com/en/quantum-computing-how-it-differs-from-classical-computing/.

13 de Wolf, "The Potential Impact of Quantum Computers on Society."

14 de Wolf.

15 Matthan, "Prepare for a World of Quantum Haves and Have-Nots."

16 Zewe, "Tiny Materials Lead to a Big Advance in Quantum Computing."

17 "Top 5 Vendors in the Hexagonal Boron Nitride Market from 2017 to 2021: Technavio," Business Wire, July 18, 2017, https://www.businesswire.com/news/home/20170718005835/en/Top-5-Vendors-in-the-Hexagonal-Boron-Nitride-Market-from-2017-to-2021-Technavio.

18 King Alexander, "This Is Not New - A Short History of Materials Criticality and Supply-Chain Challenges."

19 "Laurentis's Production of Helium-3 Supports Research, Security, Health Care and High-Tech Industries," Laurentis Energy Partners, September 13, 2021, https://laurentisenergy.com/story/laurentiss-production-of-helium-3-supports-high-tech-research-security-and-health-care/.

20 Ty Haqqi, "7 Largest Helium Producing Countries in the World," Insider Monkey, September 14, 2020, https://www.insidermonkey.com/blog/7-largest-helium-producing-countries-in-the-world-847075/.

in terms of regulation.[21] The first area in which quantum-related regulations are likely to be necessary is within the field of AI. AI use cases will likely continue blurring the lines between legal and illegal. Algorithms requiring large datasets are certain to grow more robust – and more invasive – as a result of quantum acceleration. One area in which it is likely to have a direct impact on existing judicial frameworks is predictive policing. Another area where quantum technologies are likely to have a significant judicial impact is cybercrime. Even if a working quantum computer does not become available in the short term, enemy spies (or anyone willing to secure access to previously stored information) could gather encrypted communication *today* and use a future quantum computer to decrypt them.[22] Pursuing this type of cybercrime would require a whole new set of legal domestic, international, and legal frameworks.[23]

Quantum technologies' impact on democratic processes will be informed first and foremost by the AI-enabled use cases they are used to accelerate. It means that, as with AI, quantum technologies' impact on democratic processes is entirely dependent on how their operators choose to utilise them. Based on current trends, the most likely (negative) use cases will centre around the consolidation of autocracy in autocratic countries, the export of autocratic governance models abroad, and the acceleration of democratic backsliding. China is currently very prominently constructing a digital authoritarian system and also propagating this abroad, begging the question of how liberal democracies can utilise the immense benefits of AI-related technologies without violating fundamental rights and risking a shift towards authoritarianism.[24] China has been successfully using digital technologies for its government's repressive activities and to maintain societal control: an example being its internet filtration system the "Great Firewall" for selective censorship,[25] as well as its much reported-on social credit system. The erosion of democratic processes can be attributed, in no small part, to the business models pursued by social media giants such as Facebook, YouTube, and (though to a lesser extent) Twitter. These companies utilise AI to cluster users into categories, which allows them to serve relevant ads to them on the one hand and recommend content that aligns with their world interests and/or world views on the other. Though the automation of what can fundamentally be understood as an editorial process is not inherently negative, it pays to note that companies such as Facebook and YouTube have been accused of optimising for engagement (read: time spent on their platforms). It increases ad revenues, but also creates an incentive for the creation of algorithmically-perpetuated "echo chambers" that favour the presentation of content which enrages.

Within the military realm, quantum technologies allow for substantially improved measurement, sensing, and precision capabilities.[26] The improvement of existing weapons through quantum computing enhances capabilities by reducing the time needed for executing an offensive and helping to optimise military logistics through the acceleration of current and future AI workflows.[27] It also bolsters warning and decision-making dynamics which – though

21 Ibrahim Almosallam, "Why Quantum Computing Needs Proper Governance," World Economic Forum, February 28, 2022, https://www.weforum.org/agenda/2022/02/quantum-computing-governance-regulation/.

22 de Wolf, "The Potential Impact of Quantum Computers on Society."

23 Walter G. Johnson, "Governance Tools for the Second Quantum Revolution Comment," Jurimetrics 59, no. 4 (2019 2018): 487–522.

24 Wright, "Artificial Intelligence and Democratic Norms: Meeting the Authoritarian Challange."

25 Wright.

26 Krelina, "Quantum Technology for Military Applications."

27 Yasmin Tadjdeh, "Spending on Quantum Tech on the Upswing," National Defense Magazine, February 26, 2021, https://www.nationaldefensemagazine.org/articles/2021/2/26/spending-on-quantum-tech-on-the-upswing.

beneficial from an operator perspective – ultimately serve to increase the "pace" of decision-making, increasing the risk of an unwanted escalation.[28] Quantum technologies will likely impact military areas, such as stealth detection and other PNT-related objectives. Quantum sensing is the most mature quantum technology available to military operators.[29] The technology is likely to grow, with quantum sensors likely being applicable to detecting submarines and stealth aircraft and increasing the reliability of PNT.[30] Another – and one in which the technology's impact goes far beyond the acceleration of existing AI-based workflows – is in (the breaking of) military encryption.

AI

AI is a term used to describe a wide range of learning-based use cases in computing. In extremely general terms, it describes a machine's ability to copy human intelligence (learning, logic, reasoning, perception, creativity, etc.).[31] Compared to classical computing, which is based on exact inputs, outputs and logic, AI workflows are based on providing a machine with the inputs, and the favoured outcome.[32] Depending on the data it is trained on, AI allows computers to understand their environments, handle, solve problems, and act to achieve specific goals.[33] In its current incarnation, the technology enables the advancement of existing applications; it is rarely stand-alone. Examples include Siri's (a smart assistant trained on voice data) introduction into Apple's product line and YouTube's use of an algorithm to automate content recommendations.

28 Krelina, "Quantum Technology for Military Applications."

29 van Amerongen, "Quantum Technologies in Defence & Security."

30 van Amerongen.

31 "Artificial Intelligence News: Latest Advancements in AI Technology," Business Insider, n.d., https://www.businessinsider.com/artificial-intelligence; "What Is Artificial Intelligence and How Is It Used?," European Parliament, April 9, 2020, https://www.europarl.europa.eu/news/en/headlines/society/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used.

32 "Artificial Intelligence News."

33 "What Is Artificial Intelligence and How Is It Used?"

Table 6: Summary: risks associated with AI

Judicial[34]	Democratic[35]
• A key (judicial) challenge in the AI space has to do with liability. Specifically, there remains a significant amount of uncertainty around who is liable for damage caused by AI-based systems, such as: o Driverless cars o 'Smart' household appliances o Autonomous Unmanned Aerial Vehicles (UAVs) o Autonomous harvesters o 'Robot staff' at hotels and restaurants • Another judicial challenge associated with AI has to do with how it has been used in law enforcement. AI has been used in predictive policing tools, including location-based algorithms that link location, event and past crime rate data to predict where and when crimes are most likely to occur. The implications include: o Racial profiling o Negative bias against working-class neighbourhoods o Going against the principle of presumption of innocence • AI is also seeing increased use in the judicial system to automate certain types of sentencing. It may have negative implications for cases where a human judge may recognise extenuating circumstances, such as: o Emotional state at the time of committing the crime o Socio-economic background o Misunderstandings rooted in cultural differences • The Geneva Convention does not regulate the deployment of AI-based military capabilities. The conventions of war will have to adapt to the new technological environment.	• The possibility of AI being weaponised in the corruption of elections and destruction of trust in democratic institutions remains a very current threat, with voter manipulation being just one example of a threat the technology poses to democratic processes. Similar risks to quantum computers apply here as well due to the interlinked nature of the two technologies: o The 'echo chamber' effect will grow more prominent on social media platforms due to more efficient content recommendations based on pre-existing identity patterns. o Political actors may adjust their communications to social media trends more accurately, thereby increasing populism. o Propaganda will resonate better with popular sentiments, as AI capabilities and quantum technology together generate such content *en masse*. o Totalitarian regimes, such as China, will further develop their societal surveillance and credit systems. o Due to rising extremism in democracies, such alternatives may garner support as a legitimate model. • Another (arguably underappreciated) threat to democracy comes from deep fake-based AI use cases. Deep fakes are synthetically generated images or videos of a person. They can be used to misrepresent the speeches of politicians, create false narratives, lower people's trust in media, and facilitate the spread of disinformation. • In authoritarian countries, AI systems are commonly abused to support domestic control and surveillance. It can be clearly observed in China, where the government has utilised AI in wide-scale crackdowns of regions with ethnic minorities, which include mandatory DNA samples, Wi-Fi network monitoring and facial recognition cameras.

34 John Charles, "AI and Law Enforcement," IEEE Intelligent Systems and Their Applications 13, no. 1 (1998): 77–80; Nicolas Petit, "Artificial Intelligence and Automated Law Enforcement: A Review Paper," 2018; Timo Rademacher, "Artificial Intelligence and Law Enforcement," in Regulating Artificial Intelligence (Springer, 2020), 225–54; Stephan Raaijmakers, "Artificial Intelligence for Law Enforcement: Challenges and Opportunities," IEEE Security & Privacy 17, no. 5 (2019): 74–77; Suhaib Alzou'bi, Haitham Alshibl, and Mohammad Al-Ma'aitah, "Artificial Intelligence in Law Enforcement, a Review," International Journal of Advanced Information Technology 4, no. 4 (2014): 1; "Artificial Intelligence: Threats and Opportunities," European Parliament, March 29, 2021, https://www.europarl.europa.eu/news/en/headlines/society/20200918STO87404/artificial-intelligence-threats-and-opportunities; Elizabeth Fernandez, "Who Is Responsible In A Crash With A Self-Driving Car?," Forbes, February 6, 2020, https://www.forbes.com/sites/fernandezelizabeth/2020/02/06/who-is-responsible-in-a-crash-with-a-self-driving-car/; Kathleen Walch, "The Growth Of AI Adoption In Law Enforcement," Forbes, July 26, 2019, https://www.forbes.com/sites/cognitiveworld/2019/07/26/the-growth-of-ai-adoption-in-law-enforcement/; Hope Reese, "What Happens When Police Use AI to Predict and Prevent Crime," Jstor Daily, February 23, 2022, https://daily.jstor.org/what-happens-when-police-use-ai-to-predict-and-prevent-crime/; Dawn Lo, "Can AI Replace a Judge in the Courtroom?," UNSW, October 26, 2021, https://www.unsw.edu.au/news/2021/10/can-ai-replace-a-judge-in-the-courtroom; Georg Stawa, "Artificial Intelligence: How Is Austria Approaching AI Integration into Judicial Policies" (Vienna: Bundesministerium Verfassung, Reformen, Deregulierung und Justiz, June 22, 2018), https://rm.coe.int/how-is-austria-approaching-ai-integration-into-judicial-policies-/16808e4d81.

35 Chadha et al., "Deep fake"; Kwok and Koh, "Deep fake"; Westerlund, "The Emergence of Deep fake Technology"; Karl Manheim and Lyric Kaplan, "Artificial Intelligence: Risks to Privacy and Democracy" 21 (2019): 83; Lisanne Fridsma et al., "The Misuse of Artificial Intelligence Can Be a Threat to Democracy," RPA Human(e) AI, n.d., https://humane-ai.nl/students-corner/the-misuse-of-artificial-intelligence-can-be-a-threat-to-democracy/; Cem Dilmengani, "Top 9 Ethical Dilemmas of AI and How to Navigate Them in 2022," Research AI Multiple, February 9, 2022, https://research.aimultiple.com/ai-ethics/; Feldstein, "How Artificial Intelligence Systems Could Threaten Democracy"; Kashmir Hill and Jeremy White, "Designed to Deceive: Do These People Look Real to You?," The New York Times, November 21, 2020, sec. Science, https://www.nytimes.com/interactive/2020/11/21/science/artificial-intelligence-fake-people-faces.html; Kathleen Walch, "Ethical Concerns of AI," Forbes, December 29, 2019, https://www.forbes.com/sites/cognitiveworld/2020/12/29/ethical-concerns-of-ai/; Christian Djeffal, "AI, Democracy and the Law," in The Democratization of Artificial Intelligence, ed. Andreas Sudmann, vol. 1 (Bielefeld, 2020), 255–284; Oggie Arandelovic, "AI, Democracy, and the Importance of Asking the Right Questions," AI & Ethics Journal, 2021; Paul Nemitz, "Constitutional Democracy and Technology in the Age of Artificial Intelligence," Philosophical Transactions of the Royal Society 376 (August 14, 2018): 1–14; Eleni Christodoulou and Kalypso Iordanou, "Democracy Under Attack: Challenges of Addressing Ethical Issues of AI and Big Data for More Democratic Digital Media and Societies," Frontiers in Political Science 3 (2021); Fernando Filgueiras, "The Politics of AI: Democracy and Authoritarianism in Developing Countries," Journal of Information Technology & Politics 19, no. 4 (October 2, 2022): 449–64.; Christian Djeffal, "AI, Democracy and the Law," AI Critique| Volume, 2019, 255; Oggie Arandelovic, "AI, Democracy, and the Importance of Asking the Right Questions," AI & Ethics Journal, 2021; Paul Nemitz, "Constitutional Democracy and Technology in the Age of Artificial Intelligence," Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 376, no. 2133 (2018): 20180089; Eleni Christodoulou and Kalypso Iordanou, "Democracy under Attack: Challenges of Addressing Ethical Issues of AI and Big Data for More Democratic Digital Media and Societies," Frontiers in Political Science 3 (2021): 682945; Fernando Filgueiras, "The Politics of AI: Democracy and Authoritarianism in Developing Countries," Journal of Information Technology & Politics 19, no. 4 (2022): 449–64.

Ethical[36]	Military[37]
• The ethical implications of AI are two-fold: o The short-term impacts of AI revolve around privacy protection and civil rights issues. o Long-term impacts extend to questions surrounding the protection of vulnerable populations. • A key ethical question about the use of AI has to do with its likely impact on the job market. AI-supported use cases are likely to continue prompting changes in the nature of work, meaning the technology's use will result in layoffs and unemployment. • There are also ethical questions about AI's use in law enforcement. Facial recognition is commonly used for identifying criminals in public spaces and crowds. Predictive policing uses AI to forecast likely crime affinity in individuals. • The military implications of AI also raise concerns in the ethical realm. AI may enhance conventional military capabilities in ways that would be too brutal for the conventions of war in ways similar to white phosphorus or expanding ordnance.	• Defence organisations primarily use AI to optimise certain tasks, such as: o logistics o vehicle automation o drone servicing o target acquisition • AI has already started to change military planning and operations, especially in the fields of o early warning, o intelligence analysis, o battlefield analysis, o target acquisition and analysis, o drone swarming, command and control o semi-autonomous decision-making • AI has significant advantages over traditional technologies and/or methods. These include, but are not limited to: o improved threat sensing o reduced human labour o recruitment improvement o better preparedness o enhanced cyber security o optimisations in logistics and transportation • The technology's downsides include: o its high implementation cost, o its inability to fully replace human operators, o its inability to learn from experience, o and its inability to benefit from creative thought. • These above are all factors which undermine its operational utility and fungibility.

AI is a transformative technology that will have significant ethical, judicial, and democratic impacts in the near future. Regulating AI will be a challenge for policymakers, and balancing the positive and negative effects will be a thin line. This section limits its discussion of the technology to impacts which are likely to manifest in the short-medium term (5-15 years), as anything beyond this time frame amounts to speculation. It is important to note that, due to – among others – AI and machine learning technologies growing increasingly accessible and being utilised more commonly across industries, the ethical, judicial, and democratic impacts outlined in this section are unlikely to be comprehensive in their scope.

AI's ethical impact – as with many transformative agencies – is ultimately a product of human agency. The short-term (ethical) impacts of AI revolve around privacy protection and civil rights issues. Long-term impacts extend to questions surrounding the protection of vulnerable populations.[38] A key ethical question to be raised around the use of AI has to do with its likely impact on the job market. AI-supported use cases are likely to continue prompting changes in the nature of work, with a common – and increasingly well-corroborated fear –that the technology's use will result in layoffs and unemployment. Estimates project that AI will result in the elimination of 7 million existing (low-skilled) jobs. They also stipulate that

36 Yi Zeng, "Near-Term and Long-Term Challenges for Creating Ethical AI," Institute for Ethics in Artificial Intelligence, May 12, 2021, https://www.ieai.sot.tum.de/near-term-and-long-term-challenges-for-creating-ethical-ai/; Bernard Marr, "What Is The Impact Of Artificial Intelligence (AI) On Society?," Bernard Marr & Co. (blog), July 2, 2021, https://bernardmarr.com/what-is-the-impact-of-artificial-intelligence-ai-on-society/; "Artificial Intelligence: Threats and Opportunities"; Cem Dilmegani, "Top 9 Ethical Dilemmas of AI and How to Navigate Them in 2022," AI Multiple, January 23, 2021, https://research.aimultiple.com/ai-ethics/; Kambria, "The 7 Most Pressing Ethical Issues in Artificial Intelligence," Kambria, August 13, 2019, https://kambria.io/blog/the-7-most-pressing-ethical-issues-in-artificial-intelligence/.

37 Pragya Soni, "AI in Military Sector - Advantages and Disadvantages," Analytics Steps, November 5, 2021, https://www.analyticssteps.com/blogs/ai-military-sector-advantages-and-disadvantages; "The Militarization of Artificial Intelligence" (New York: Stanley Center for Peace and Security, August 2019), https://stanley-center.org/wp-content/uploads/2020/06/TheMilitarization-ArtificialIntelligence.pdf; van Manen et al., "Taming Techno-Nationalism: A Policy Agenda.".

38 Yi Zeng, "Near-Term and Long-Term Challenges for Creating Ethical AI," Institute for Ethics in Artificial Intelligence, May 12, 2021, https://www.ieai.sot.tum.de/near-term-and-long-term-challenges-for-creating-ethical-ai/.

the technology will create 7.2 million *new* (high-skilled) jobs in the same period.[39] Not unrelated to job loss, another ethical question surrounding AI is the question of wealth inequality. Specifically, by allowing companies to replace human workers, AI is set to exacerbate a pre-existing trend; namely, the concentration of wealth in the shareholder / C-suite class.[40] Another ethical concern is the overlap of data privacy in society, the need of the private sector to stay competitive, and government regulation.

On the judicial front, a key challenge in the AI space –one which complicates both its use & regulation and its utility to law enforcement agencies – has to do with liability. Specifically, there remains significant uncertainty around who is liable for damage caused by A. In the case of an accident involving a self-driving car, for example, existing legislation offers (relatively) little guidance as to whether liability lies with the owner of the car, the car's manufacturer, or (if the car is using a 3rd party software solution to enable self-driving) the software developed.[41] In a 2018 accident, when a self-driving Volvo which was part of an autonomous driving test by Uber in Arizona, killed a pedestrian, the blame was divided between the safety driver, Uber, the self-driving car, the victim, and the state of Arizona.[42] There are also ethical questions to be raised around AI's use in law enforcement. Facial recognition is commonly used for identifying criminals in public spaces and crowds.[43] Predictive policing uses AI to forecast likely crime affinity in individuals. The technology uses past information about a crime to make predictions about future crimes, which are inherently biased and only reinforce inequality.[44] AI is also seeing increased use in the judicial system to automate certain types of sentencing. The Estonian government uses an AI judge for small claim disputes of contract claims under €7000 of clear case backlog.[45] AI is also applied within the judicial system on a much lower level. As an example, it is used to anonymise court documents and for the analysis and preparation of investigation data in Austria.[46]

The possibility of AI being weaponised in the corruption of elections and destruction of trust in democratic institutions remains a very current threat.[47] Voter manipulation is just one example of a threat posed to democracy, though it is one which – due, in no small part, to the media attention Cambridge Analytica garnered for its use of psychographic profiling of Facebook users during the 2016 UK and US elections – is growing increasingly widely recognised.[48] The 2020 US election was one of the most digitised campaigns ever and the usage of AI in political microtargeting and bots emerged as new powerful ways for online advertising.[49] Another (arguably underappreciated) threat to democracy comes from deep fake-based AI use cases. Deep fakes are synthetically generated images or videos of a person. They can be used to misrepresent the speeches of politicians, create false narratives, lower people's trust

39 Marr, "What Is The Impact of Artificial Intelligence (AI) On Society?"

40 Kambria, "The 7 Most Pressing Ethical Issues in Artificial Intelligence," Kambria, August 13, 2019, https://kambria.io/blog/the-7-most-pressing-ethical-issues-in-artificial-intelligence/.

41 "Artificial Intelligence: Threats and Opportunities," European Parliament, September 23, 2020, https://www.europarl.europa.eu/news/en/headlines/society/20200918STO87404/artificial-intelligence-threats-and-opportunities.

42 Fernandez, "Who Is Responsible In A Crash With A Self-Driving Car?"

43 Walch, "The Growth Of AI Adoption In Law Enforcement."

44 Reese Hope, "What Happens When Police Use AI to Predict and Prevent Crime?," JSTOR Daily, February 23, 2022, https://daily.jstor.org/what-happens-when-police-use-ai-to-predict-and-prevent-crime/.

45 Lo, "Can AI Replace a Judge in the Courtroom?"

46 Stawa, "Artificial Intelligence: How Is Austria Approaching AI Integration into Judicial Policies."

47 Manheim and Kaplan, "Artificial Intelligence: Risks to Privacy and Democracy."

48 Manheim and Kaplan.

49 Fridsma et al., "The Misuse of Artificial Intelligence Can Be a Threat to Democracy."

in media, and facilitate the spread of disinformation.[50] AI can create "fake people," a person that does not exist, but has a real face, which allows i.e. right-wing propagandists to hide behind fake profiles.[51] As AI systems are improving its capabilities of creating fake images, videos, conversations and all kinds of content, it becomes increasingly difficult to differentiate whether something is AI-generated or real.[52] The role of bots spreading political propaganda in the 2016 US Presidential elections is already heavily debated, questioning whether AI will make fake media and disinformation worse.[53] Finally, in authoritarian countries, AI systems are commonly abused to support domestic control and surveillance. It can be clearly observed in China, where the government has utilised AI in wide-scale crackdowns of regions, with ethnic minorities which include mandatory DNA samples, Wi-Fi network monitoring and widespread facial recognition cameras which are connected to integrated data analysis platforms.[54] Chinese companies are further building smart cities with built-in surveillance technology in Pakistan, the Philippines, and Kenya; and Chinese companies are supplying Singapore with facial recognition cameras.[55]

Today, defence organisations primarily use AI to optimise logistics, vehicle automation, drone servicing, and target acquisition.[56] AI has already started to change military planning and operations, especially in the fields of early warning, intelligence analysis, battlefield analysis, target acquisition and analysis, drone swarming, command and control and semi-autonomous decision-making[57]. AI has significant advantages over traditional technologies and/or methods. These include, but are not limited to, improved threat sensing, reduced human labour, recruitment improvement, better preparedness, enhanced cyber security, and optimisations in logistics and transportation.[58] The technology also runs into several limitations. It has a high implementation cost, is not (yet) able to fully replace, lacks (in its current iterations) the ability to learn from experience, and is unable to benefit from creative thought – all factors which undermine its operational utility and fungibility.[59] In the short term, the army is most likely to use AI to support decision making.[60] Because the technology offers opportunities to avoid putting human lives at risk, can reduce costs in logistics and sensing, and can improve communication and transparency in a complex system, it could especially benefit the peacekeeping agenda.[61]

50 Cem Dilmegani, "Top 9 Ethical Dilemmas of AI and How to Navigate Them in 2022," AI Multiple, January 23, 2021, https://research.aimultiple.com/ai-ethics/; Feldstein, "How Artificial Intelligence Systems Could Threaten Democracy."

51 Hill and White, "Designed to Deceive."

52 Walch, "Ethical Concerns of AI."

53 Walch.

54 Feldstein, "How Artificial Intelligence Systems Could Threaten Democracy."

55 Feldstein.

56 Soni, "AI in Military Sector - Advantages and Disadvantages."

57 van Manen et al., "Taming Techno-Nationalism: A Policy Agenda."

58 Soni, "AI in Military Sector - Advantages and Disadvantages."

59 Soni.

60 "The Militarization of Artificial Intelligence."

61 "The Militarization of Artificial Intelligence."

Semiconductors

Semiconductors form the basic building blocks of modern computers. More specifically, semiconductors are made up of transistors capable of regulating the flow of electrons through integrated circuits.[62] A transistor can be made of pure elements (such as silicon or germanium), or of compounds (such as gallium arsenide).[63] Small impurities are introduced during production in a procedure dubbed doping, allowing for significant changes in the conductivity of the material.[64] Silicon, which makes up 90% of the Earth's crust, is utilised in virtually all semiconductors. The purest silicon is found in quartz rock; the purest quartz comes from a quarry in North Carolina.[65] Silicon powder is melted in a furnace at 1400 degrees Celsius, shaped into cylindrical ingots, and then sliced into discs called wafers. Several dozen rectangular circuits are then printed onto each wafer to synthesise the final chip.[66] This manufacturing process requires giant factories, dust-free rooms, multi-million-dollar machines, molten tin, and lasers. From start to finish, the creation of a "batch" of chips takes around three months.[67] Because chips are very sensitive to external variables such as static electricity, temperature variations, and even tiny specks of dusk, the manufacturing process requires the construction of highly controlled environments. As a result, just the fabrication of the facilities in which microchips are produced (commonly referred to as foundries) takes between two to five years.[68]

62 Douglas Heaven, "Made on Earth: The Humble Mineral That Transformed the World," BBC, n.d., https://www.bbc.com/future/bespoke/made-on-earth/how-the-chip-changed-everything/.

63 "What Is a Semiconductor?," Semiconductor Industry Association, January 22, 2018, https://www.semiconductors.org/semiconductors-101/what-is-a-semiconductor/.

64 "What Is a Semiconductor?"

65 Heaven, "Made on Earth: The Humble Mineral That Transformed the World."

66 Heaven.

67 Ian King, Adrian Leung, and Demetrios Pogkas, "Chip Shortage Keeps Getting Worse. Why Can't We Just Make More?," Bloomberg.Com, May 6, 2021, https://www.bloomberg.com/graphics/2021-chip-production-why-hard-to-make-semiconductors/.

68 "What You Need to Know About the Chip Shortage," Planet Technology USA, May 18, 2021, https://planetechusa.com/chip-and-semiconductor-shortage/.

Table 7: Summary: risks associated with semiconductors

Judicial[69]	Democratic[70]
• A significant judicial concern plaguing the semiconductor industry is corporate espionage, with TSMC claiming to have been the victim of several cyber-attacks aimed at scouring its networks and sourcing code and chip-related software and other company trade secrets. • The structure of the supply chain of semiconductor manufacturing leaves access of countries to semiconductors vulnerable. It poses a two-fold judicial risk: o No international treaty regulates cutting off access to these crucial components, o And multilateral binding sanctions can undermine the semiconductor supply chain altogether. • In addition, there are very few judicial checks on the consolidation of this strategically vital activity in the hands of very few (nations and companies), leading to monopolisation, which harms the principles of the free market. For instance: o The Taiwan Semiconductor Manufacturing Company (TSMC) o Intel Corporation o Qualcomm o Micron Technology Inc. o Broadcom Inc. • Insurance schemes are yet to be adapted to the unparalleled high financial barrier of entry into the semiconductor sector. For instance, if an earthquake shatters a several-billion-dollar fabrication cleanroom, the economic fallout ripples across the supply chain, with no legal framework for mitigating the damage. Solutions may be as follows, among others: o A degree of government presence, akin to reimbursement of banking clients upon the financial institution abdicating leverage o Multi-layered reinsurance schemes, akin to the British government's ability to turn a profit from being blockaded during WWI	• Access to semiconductors can be used and weaponised as a political tool. As an example, semiconductors have emerged as a crucial bargaining chip in: o The current Russian invasion of Ukraine, with the US having cut off 49 Russian and two Belarusian entities from accessing US technology, including semiconductors. o The Chinese threat over Taiwan, with a large portion of the world's semiconductors made by TSMC o The US-China trade war's underlying motives were both economic and ideological (liberal democracy as opposed to autocracy) • The above calamities may, in the medium term, undermine democratic nations' strategic posture against their autocratic adversaries, thereby forcing the appeasement of the latter by the former. • Domestic voices advocating for said appeasement may also adopt autocratic ideas, thereby: o deepening the societal rift in democratic societies and causing a democratic deficit o accelerating democratic backsliding in young democracies and hybrid regimes o solidifying the grip of autocratic regimes over their domestic populations • Geopolitical concerns have also increasingly contributed to nations wanting to reduce their dependence on Chinese manufacturers. While this in itself may be good for democratic processes, it poses risks: o Domestic opposition to this endeavour may start propagating the Chinese model of statecraft more openly o China may rely on more proactive methods of power projection once economic interconnectivity becomes less significant, such as: • Espionage (such as the Fudan University campus in Budapest or breaches into TSMC) • Social media influencing (still soft power projection, but globally present via platforms such as TikTok) • Military sabre rattling (against East Asian democracies) • Moore's Law also amplifies the worrisome effects of AI (and, to some extent, quantum computing), as well as in terms of democratic concerns.

69 Yen Nee Lee, "2 Charts Show How Much the World Depends on Taiwan for Semiconductors," CNBC, March 15, 2021, https://www.cnbc.com/2021/03/16/2-charts-show-how-much-the-world-depends-on-taiwan-for-semiconductors.html; Alan Crawford et al., "The World Is Dangerously Dependent on Taiwan for Semiconductors," Bloomberg.Com, January 25, 2021, https://www.bloomberg.com/news/features/2021-01-25/the-world-is-dangerously-dependent-on-taiwan-for-semiconductors; Sean Lyngaas, "Hacking Group Has Hit Taiwan's Prized Semiconductor Industry, Taiwanese Firm Says," CyberScoop, August 6, 2020, https://www.cyberscoop.com/cycraft-taiwan-semiconductor-espionage-black-hat/; Toby Sterling and Anthony Deutsch, "ASML Says It Suffered Intellectual Property Theft, Rejects 'Chinese' Label," Reuters, April 11, 2019, https://www.reuters.com/article/us-asml-china-spying-idUSKCN1RN0DK; "An Insurance Take on Global Telecoms," The Advanced Semiconductor Magazine, III-Vs Review, 18, no. 5 (2005): 6–6; Kochun Mou and Guang-Hann Chen, "Risk Management in Semiconductor Industry," in 2004 Semiconductor Manufacturing Technology Workshop Proceedings (IEEE Cat. No.04EX846), 2004, 197–200; "Semiconductor Secrets: Taiwan's Government Propose a Law to Prevent China from Stealing Its Chip Technology," The Economic Times, February 17, 2022, https://economictimes.indiatimes.com/news/international/business/semiconductor-secrets-taiwans-government-propose-a-law-to-prevent-china-from-stealing-its-chip-technology/articleshow/89633337.cms.

70 "How Will New Export Controls Impact the Global Semiconductor Shortage?," Foreign Policy Magazine, n.d., https://foreignpolicy.com/2022/03/17/russia-us-china-semiconductors-export-controls-sanctions-eu/; Amar Diwakar, "'Chip Wars': US, China and the Battle for Semiconductor Supremacy," TRT World, March 16, 2021, https://www.trtworld.com/magazine/chip-wars-us-china-and-the-battle-for-semiconductor-supremacy-45052; Assif Shameen, "Tech: Why TSMC Is the World's Most Underestimated Tech Giant," The Edge Markets, February 17, 2021, http://www.theedgemarkets.com/article/tech-why-tsmc-worlds-most-underestimated-tech-giant; Jillian Deutsch, Debby Wu, and Jenny Leonard, "The Global Fight Over Chips Is About to Get Even Worse," Bloomberg, March 16, 2022, https://www.bloomberg.com/news/features/2022-03-16/when-will-the-chip-shortage-end-u-s-eu-spend-billions-in-race-to-beat-china; Wynand Lambrechts et al., Extending Moore's Law through Advanced Semiconductor Design and Processing Techniques (Boca Raton: CRC Press, 2018); Stephen Ezell, "Moore's Law Under Attack: The Impact of China's Policies on Global Semiconductor Innovation," Washington International Trade Association (blog), October 2, 2021, https://www.wita.org/atp-research/moores-law-chinas-policies/; Robin Herberg, Semiconductors and the Promotion of Democracy in Southeast Asia, 2022; James Lee, "Taiwan and the 'New Cold War,'" Network for Strategic Analysis (NSA) (blog), August 29, 2022, https://ras-nsa.ca/taiwan-and-the-new-cold-war/; John Shalf, "The Future of Computing beyond Moore's Law," Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 378, no. 2166 (January 20, 2020); Jared Cohen and Richard Fontaine, "Uniting the Techno-Democracies: How to Build Digital Cooperation," December 2020, https://www.foreignaffairs.com/articles/united-states/2020-10-13/uniting-techno-democracies; Nurul Aulia Rahmawati and Fristian Hadinata, "Computational Propaganda on TikTok as the 21st Century Propaganda Model," International Review of Humanities Studies 7, no. 1 (2022); Federica Cristani, "Economic Cyber-Espionage in the Visegrád Four Countries: A Hungarian Perspective," Politics in Central Europe 17, no. 4 (2021): 697–721; Oxford Analytica, "Hungary's Law Change Admits China's Fudan University," Emerald Expert Briefings, no. oxan-es (2021); Gabriela Pleschová, "Identifying with Someone Other than the West: Hungarians Belonging and Orbans Unique China Policy," in China in Central Europe (Edward Elgar Publishing, 2022), 43–60; Fergus Ryan, Audrey Fritz, and Daria Impiombato, "TikTok and WeChat: Curating and Controlling Global Information Flows," 2020.

Ethical[71]

- A key ethical question surrounding semiconductors has to do with the health risks posed to workers during the manufacturing process. Despite having a somewhat 'clean' image, there are various health risks associated with the three steps:
  - Wafer cutting
  - Fabrication
  - And packaging/testing
- Supply chain centralisation means that open market mechanisms result in an extremely uneven distribution of semiconductors at the global (and, in some cases, even domestic) levels. For instance:
  - Nearly all deposits of rare earth materials needed for semiconductor production are located in China, Russia, or the Democratic republic of the Congo (DRC).
  - The Netherlands has de facto exclusive control over advanced lithography machines.
  - Over half of the world's semiconductors are manufactured in TSMC foundries.
  - Much of the world's chip designs are patented in the US.
- Increases in the computing power of semiconductors amplify the ethical concerns revolving around AI (and, to some extent, quantum technology) as well. The more powerful semiconductors get (see: Moore's Law, i.e. the idea that computing power doubles every two years), the more pronounced the implications of AI become.

Military[72]

- Semiconductors are essential for military and defence technology, weaponry, and equipment – but the critical dependencies within the industry, with the maintenance of US leadership and the resilience and security of the industry's supply chains, making them a national security imperative.
- Disruptions from malware in the defence sector are a growing concern due to the globalisation of the semiconductor market.
- The global chip shortage is detrimental to military access to semiconductors.
- National security cannot be seen as separate from commercial applications due to the dual use of semiconductors.
- Unforeseen breakthroughs in semiconductor development, on the part, of rival powers, may pose a significant increase in the level of military threat said powers pose to NATO.

Centralisation of supply chains and production processes plays an important role in defining the ethical, judicial, democratic, and – to a lesser extent – military threats and opportunities that might reasonably be associated with semiconductors. The US maintains a dominant position in chip design and electronic software tools, while Japan is a key supplier of equipment, chemicals and wafers.[73] Taiwan's chip factories could potentially become collateral damage if China chooses to invade Taiwan, with many analysts already identifying Taiwan as a focal point of Chinese security policy.[74] Because the semiconductor industry is widespread and diversified, no one country or company is truly independent in its value chain.[75] Many major tech companies (Apple, Qualcomm, Nvidia, etc.) are TSMC's clients.[76] All of this

71 Lambrechts et al., Extending Moore's Law through Advanced Semiconductor Design and Processing Techniques; Ezell, "Moore's Law Under Attack"; Shalf, "The Future of Computing beyond Moore's Law"; Kim, Kim, and Paek, "The Health Impacts of Semiconductor Production"; Alan Crawford, Ian King, and Debby Wu, "The Chip Industry Has a Problem With Its Giant Carbon Footprint," Bloomberg, April 8, 2021, https://www.bloomberg.com/news/articles/2021-04-08/the-chip-industry-has-a-problem-with-its-giant-carbon-footprint; Gooding, "The Environmental Impact of Chip Making Needs Closer Scrutiny"; Pádraig Belton, "The Computer Chip Industry Has a Dirty Climate Secret," The Guardian, September 18, 2021, sec. Environment, https://www.theguardian.com/environment/2021/sep/18/semiconductor-silicon-chips-carbon-footprint-climate; Jeanny Kao and Yimou Lee, "Exclusive: Taiwan Ministry Says TSMC Will Prioritise Auto Chips If Possible," Reuters, January 25, 2021, https://www.reuters.com/article/us-taiwan-autos-chips-exclusive-idUSKBN29U091; Banjamin Mayo, "TSMC to Prioritize Apple and Automaker Silicon Orders as Global Semiconductor Shortage Continues," 9to5Mac, June 22, 2021, https://9to5mac.com/2021/06/22/tsmc-to-prioritize-apple-and-automaker-silicon-orders-as-global-semiconductor-shortage-continues/.

72 Lee, "Taiwan and the 'New Cold War'"; Che-Jen Wang, "China's Semiconductor Breakthrough," The Diplomat, August 20, 2022, https://thediplomat.com/2022/08/chinas-semiconductor-breakthrough/; Melissa K. Griffith and Sophie Goguichvili, "The U.S. Needs a Sustained, Comprehensive, and Cohesive Semiconductor National Security Effort," Wilson Center, March 23, 2021, https://www.wilsoncenter.org/blog-post/us-needs-sustained-comprehensive-and-cohesive-semiconductor-national-security-effort; Gordon Feller, "Facing Down Semiconductor Supply Chain Threats," Air & Space Forces Magazine (blog), January 4, 2022, https://www.airandspaceforces.com/article/facing-down-semiconductor-supply-chain-threats/; John Adams, "America's Semiconductors Supply Chain Faces Big Cybersecurity Risks," Alliance for American Manufacturing, March 23, 2017, https://www.americanmanufacturing.org/blog/americas-semiconductors-supply-chain-faces-big-cybersecurity-risks.

73 Crawford et al., "The World Is Dangerously Dependent on Taiwan for Semiconductors."

74 Crawford et al.

75 Ahsan Nisar, "Threat of Semiconductor Chips Shortage Is Real," Pakistan & Gulf Economist, September 5, 2021, https://www.pakistangulfeconomist.com/2021/09/06/threat-of-semiconductor-chips-shortage-is-real/.

76 Lee, "2 Charts Show How Much the World Depends on Taiwan for Semiconductors."

raises questions regarding the ethics of sourcing and diversifying, the judicial pathways that might help to alleviate supply chain bottlenecks, and the (democratic) implications of high dependence.

A key ethical question surrounding semiconductors concerns the health risks posed to workers during the manufacturing process. Despite having a somewhat 'clean' image, there are various health risks associated with the three steps of wafer manufacturing, fabrication, and packaging/testing.[77] For example, during wafer fabrication, the material deposition, photolithography, etching, and doping all make use of hazardous materials, such as organic solvents, acids, and heavy metals. While some of those materials do no more than irritate the skin or respiratory organs, others are carcinogenic, damage the reproductive system, or are classified as neurotoxins.[78] In 2019, Intel's fabs used three times as much water as Ford's plants, while also creating twice as much hazardous waste.[79] TSMC has also not met its key sustainability targets in 2020; the company's water waste has increased with its revenue.[80] This trend is unlikely to abate; as the world continues to digitalise, semiconductors – and the reliable supply and production thereof – are set to continue to grow in relevance.[81] The industry also has a huge carbon footprint. Despite semiconductors contributing to meeting global climate goals by being part of (among others) electric vehicles, solar arrays and wind turbines, their manufacturing process is extremely energy intensive.[82] In addition, supply chain centralisation means that open market mechanisms result in an extremely uneven distribution of semiconductors at the global levels. TSMC's client relations are defined – in no small part – by order size, meaning that the company can (and frequently does) choose to prioritise some clients over others when allocating limited fab capacity. While the company has announced that it will prioritise the production of car chips in the short term,[83] analysts have long observed that affluent partners – such as Apple – have generally been able to secure outsized fab capacities in the past.[84]

A significant judicial concern plaguing the semiconductor industry is corporate espionage. TSMC claims to have been a victim of several cyber-attacks aimed at scouring its networks and sourcing code and chip-related software and other company trade secrets.[85] The company also reported intellectual property theft in 2015.[86] In response, Taiwan proposed a new law targeted at preventing China from stealing its chip technology.[87] The cabinet intends to introduce new offences for economic espionage, even introducing a sentence of up to 12 years of imprisonment for anyone leaking core technologies to China or foreign enemy forces.[88]

On the democratic front, it pays to note that semiconductors have grown increasingly central to geopolitical competition between liberal democracies and autocracies. Semiconductors have emerged as a crucial bargaining chip in the current Russian invasion of Ukraine, with

77 Kim, Kim, and Paek, "The Health Impacts of Semiconductor Production."

78 Kim, Kim, and Paek.

79 Crawford, King, and Wu, "The Chip Industry Has a Problem With Its Giant Carbon Footprint," April 8, 2021.

80 Gooding, "The Environmental Impact of Chip Making Needs Closer Scrutiny."

81 Crawford, King, and Wu, "The Chip Industry Has a Problem With Its Giant Carbon Footprint," April 8, 2021.

82 Belton, "The Computer Chip Industry Has a Dirty Climate Secret."

83 Kao and Lee, "Exclusive."

84 Mayo, "TSMC to Prioritize Apple and Automaker Silicon Orders as Global Semiconductor Shortage Continues."

85 Lyngaas, "Hacking Group Has Hit Taiwan's Prized Semiconductor Industry, Taiwanese Firm Says."

86 Sterling and Deutsch, "ASML Says It Suffered Intellectual Property Theft, Rejects 'Chinese' Label."

87 "Semiconductor Secrets."

88 "Semiconductor Secrets."

the US having cut off 49 Russian and two Belarusian entities from accessing US technology, including semiconductors.[89] They have also played a central role in the US-China trade war, where they are at the core of the Sino-American rivalry for tech supremacy,[90] showcasing how a battle for ideology (liberal democracy vs an authoritarian state) can spill over into other dimensions. The US sanctioned SMIC, the largest Chinese chip manufacturer, in September 2020 due to supposed military end-use in China.[91] In the wake of the US-China tech war, TSMC has been forced to take sides with Washington. Before the tech war, mainland China accounted for around 22% of total revenues.[92] After TSMC stopped supplying to Huawei, the number dropped to 6%.[93] The US has also pressured ASML not to sell its EUV machines to China,[94] clearly highlighting the US' commitment to curtailing Chinese influence and independence through tech-related mechanisms, and through mechanisms affecting semiconductor production specifically.

Besides the direct impact of semiconductors on military equipment, their development can pose a national security risk. Semiconductors are essential for military and defence technology, weaponry, and equipment – but the critical dependencies within the industry with the maintenance of US leadership and the resilience and security of the industry's supply chains, making them national security imperative.[95] However, national security cannot be seen separate from commercial applications, as high-performance computing tools are dual-use technologies: the same technologies building better bombers can also build better transport planes[96]. The global chip shortage severely impacted military supply chains.[97] Moreover, the increasingly globalised semiconductor supply chain threatens the vulnerability of the American semiconductor industry, leaving it increasingly exposed to disruption from malware and other production defects.[98]

89 "How Will New Export Controls Impact the Global Semiconductor Shortage?"

90 Diwakar, "'Chip Wars.'"

91 Diwakar.

92 Shameen, "Tech."

93 Shameen.

94 Jillian Deutsch, Debby Wu, and Jenny Leonard, "The Global Fight Over Chips Is About to Get Even Worse," Bloomberg.Com, March 16, 2022, https://www.bloomberg.com/news/features/2022-03-16/when-will-the-chip-shortage-end-u-s-eu-spend-billions-in-race-to-beat-china.

95 Griffith and Goguichvili, "The U.S. Needs a Sustained, Comprehensive, and Cohesive Semiconductor National Security Effort."

96 Griffith and Goguichvili.

97 Feller, "Facing Down Semiconductor Supply Chain Threats."

98 Adams, "America's Semiconductors Supply Chain Faces Big Cybersecurity Risks."

Space-related Technologies

Spurred on by innovations pioneered by private entities such as Elon Musk's SpaceX, Jeff Bezos' Blue Origin, and the United Launch Alliance (ULA), the per-kilo cost of launching objects into Low-Earth Orbit (LEO) has decreased over 700-fold from close to $1,000,000 in the mid-late 1950s to $1,400 today.[99] Costs are set to further decline in the coming years. The development of platforms such as Starship, a reusable SpaceX-developed launch vehicle with an ascent payload capacity of more than 100 tons, is expected to further reduce the per-kilo cost of launching objects into LEO to around $10 sometime within the next decade. The democratisation of space has created huge opportunities for state and corporate actors. The number of spacecraft launched more than tripled since 2008, with private-sector actors accounting for the bulk of this growth.[100] It has also highlighted and exacerbated the potential impact of several threats and vulnerabilities. As the number of satellites in orbit around the Earth has increased, so has a risk of a disruptive collision. An increasing number of states – including the United States,[101] Russia,[102] China,[103] India,[104] and Israel[105] – have moved to militarise the domain. Guidelines put forward by the United Nations Committee on the Peaceful Uses of Outer Space (UN COPUOS – 2020) and by the University of Adelaide's Woomera Manual (2018) have sought to regulate these activities,[106] but the existing body of rules and regulations is nonetheless growing long in the tooth and need of a refresh.

99 van Manen, Sweijs, and Bolder, "Strategic Alert: Towards a Space Security Strategy."

100 Claude Lafleur, "The Spacecrafts Encyclopedia - A Comprehensive Census of All the Spacecraft Ever Launched," 2017, http://claudelafleur.qc.ca/Spacecrafts-index.html.

101 The US Navy successfully destroyed a nonfunctional National Reconnaissance Office satellite using a single modified tactical Standard Missile-3 launched from an AEGIS-class cruiser in 2008. See Jim Wolf, "U.S. Shot Raises Tensions and Worries over Satellites," Reuters, 2008, https://www.reuters.com/article/us-satellite-intercept-vulnerability-idUSN2144210520080222.

102 Russia carried out the first successful flight test of its anti-satellite missile, the Nudol, in 2015. See Bill Gertz, "Russia Flight Tests Anti-Satellite Missile," Washington Free Beacon (blog), December 2, 2015, https://freebeacon.com/national-security/russia-conducts-successful-flight-test-of-anti-satellite-missile/.

103 China carried out a test of its SC-19 ASAT missile in 2007, during which the missile successfully intercepted and destroyed the FY-IC polar orbit satellite. See Brendan Nicholson, "World Fury at Satellite Destruction," The Age, January 20, 2007, https://www.theage.com.au/national/world-fury-at-satellite-destruction-20070120-ge416d.html.

104 The Indian Ballistic Missile Defense Programme tested its Prithvi Defense Vehicle Mark-II in 2019, successfully destroying a Defense Research and Development Organization Microsat-r satellite. See Marco Langbroek, "Why India's ASAT Test Was Reckless," The Diplomat, 2019, https://thediplomat.com/2019/05/why-indias-asat-test-was-reckless/.

105 Israel hasn't truly demonstrated is ASAT capability. However, it has the Arrow 3 or Hetz 3 anti-ballistic missile in service that provides exo-atmospheric interception of ballistic missiles. The Israeli Space Agency reported in 2009 that its Arrow-3 interceptor missile would be adapted to also fulfill an ASAT role. See Barbara Opall-Rome, "Israeli Experts: Arrow-3 Could Be Adapted for Anti-Satellite Role," SpaceNews, 2009, https://spacenews.com/israeli-experts-arrow-3-could-be-adapted-anti-satellite role/.

106 "The Woomera Manual on the International Law of Military Space Operations" (The University of Adelaide, 2018), https://law.adelaide.edu.au/woomera/system/files/docs/Woomera%20Manual.pdf.

Table 8: Summary: risks associated with space-related technologies

Judicial[107]	Democratic[108]
• The 1967 Outer Space Treaty lays the legal foundation for regulating (state) behaviour in space, stipulating that space is used exclusively for peaceful purposes and that all activities in space have to be in accordance with international law. Several treaties have expanded on it since its inception. • New challenges lack adequate legal regulation: o Increasing space debris and overpopulated orbits are not addressed on a legal level and have serious implications for the accessibility of space in the future o Radio frequency interferences and spectrum allocation issues are yet to be codified by any legal regulation o Developing counter-space capabilities and space-based weapon systems is yet to be regulated by the conventions of warfare o Asteroid mining: the anti-trust checks against the consolidation of massive deposits of rare earth elements in the hands of a few conglomerates o Conventional space exploration by actors in the private sector underlines the need for anti-trust regulation o The colonisation of celestial bodies in the solar system also requires legal assurances for granting equal access to various actors. It is particularly urgent in the case of bodies such as: • Mars • Venus • Europa • Titan • The legislative landscape is fragmented even at the EU level, with the various Member States having their own national space laws. • As of 2022, existing international regulations on space-based and space-related activities mostly focus on human activity in outer space, while contingencies about the defence of earth from outer space are relegated to niche departments of national defence sectors. • Low-to-middle-income countries have been excluded from the development of legislation, as they lack their own space agility, allowing for an emerging gap between high- and low-income countries in the potential for space capabilities, which is then further reflected in space law.	• With many social systems (including the internet, payment platforms, etc.) being dependent on space-based infrastructure, some aspects of the continued functioning of the digital democratic infrastructure in the Netherlands are vulnerable to disruption by o Satellite collisions o Space debris strikes o Anti-satellite (ASAT) weapons. • The consolidation of wealth as exacerbated by space-related activities such as asteroid mining or private space exploration ventures has the potential to deepen the societal rift between political extremes. • The same process also has a negative bearing on the process of disillusionment and alienation among the population, which exposes societal groups to populism. • Given the extremely high financial barrier of entry when it comes to the space exploration sector, early actors who exploit the profits of activities such as asteroid mining may accumulate wealth and influence the democratic infrastructure in liberal democracies is not prepared for. Effects of this presently observable include: o Unique media presence and influencing of these individuals' following o Conventional media presence and control of narratives in social discourse o Political lobbying • The lack of emphasis on space exploration and astrophysics concepts in education may make populist claims by political adventurers related to space more resonant with societal groups. This process may accelerate with further developments in space-related activities. • China's increasing space activity may give them a strategic edge in space-based warfare, potentially undermining NATO's ability to defend democratic systems on military grounds • China's potential achievements in space-related activities may yield perceived legitimacy to autocratic systems as a seemingly legitimate alternative in the eyes of domestic populations. The effects of this may lead to: o Democratic deficit and populism in liberal democracies o Accelerated democratic backsliding in young democracies and hybrid regimes o The solidification of autocratic rule in rival regimes.

107 Lafleur, "The Spacecrafts Encyclopedia - A Comprehensive Census of All the Spacecraft Ever Launched"; "The Woomera Manual on the International Law of Military Space Operations" (The University of Adelaide, 2018), https://law.adelaide.edu.au/woomera/system/files/docs/Woomera%20Manual.pdf; Niklas Nienass, "Needed: A European Space Strategy," The Parliament Magazine, February 3, 2022, https://www.theparliamentmagazine.eu/news/article/needed-a-european-space-strategy; Steer and Hersch, War and Peace in Outer Space; Su, "The Legal Challenge of Arms Control in Space"; Dave Webb, "The Ethical Use of Outer Space," in Ethical Engineering for International Development and Environmental Sustainability, ed. Marion Hersh (London: Springer, 2015), 103–38; Goguichvili, Linenberger, and Gillette, "The Global Legal Landscape of Space"; King James Nkum and Beida Onivehu Julius, "Emerging Legal Issues in Sub-Orbital Flight and Colonization under International Air and Space Law," Groningen Journal of International Law 7, no. 1 (August 27, 2019): 37–45; Melissa J Durkee, "Interstitial Space Law," Wash. UL Rev. 97 (2019): 423; Igor Levchenko et al., "Mars Colonization: Beyond Getting There," in Terraforming Mars, ed. Martin Beech, Joseph Seckbach, and Richard Gordon, 1st ed. (Wiley, 2021), 73–98; Marko Kovic, "Risks of Space Colonization," Futures 126 (February 1, 2021): 102638, https://doi.org/10.1016/j.futures.2020.102638; Luisa María Lara et al., White Paper 12: Our Future? Space Colonization and Exploration (Consejo Superior de Investigaciones Científicas (España), 2021).

108 Lafleur, "The Spacecrafts Encyclopedia - A Comprehensive Census of All the Spacecraft Ever Launched"; Lucas Porto de Souza Fontão, "'Make Space Great Again': The Populist Nationalism of the US Space Program Under Donald Trump," Encontro Nacional de Associacao Brasileira de Estudios de Defesa, n.d.; Lucian Vesalon and Vlad Botgros, "'The World's Shortest Highway': Entrepreneurial Populism and the Making of a Personal Campaign," European Journal of Cultural Studies 25, no. 1 (January 11, 2022); George Tyler, Billionaire Democracy: The Hijacking of the American Political System (BenBella Books, 2018); Benjamin I Page, Jason Seawright, and Matthew J Lacombe, Billionaires and Stealth Politics (University of Chicago Press, 2018); Brian Patrick Green, "Convergences in the Ethics of Space Exploration," Social and Conceptual Issues in Astrobiology, 2020, 179–96; Martin Karlsson, "Digital Democracy and the European Union," in The European Union and the Technology Shift (Springer, 2021), 237–61; Ronak Gopaldas, "Digital Dictatorship versus Digital Democracy in Africa," 2019; Nkum and Julius, "Emerging Legal Issues in Sub-Orbital Flight and Colonization under International Air and Space Law"; Tony Milligan and Shin-ichiro Inaba, "Ethical Problems of Life Extension for Space Exploration," in Human Enhancements for Space Missions (Springer, 2020), 183–200; Ryan Bourne, "Has Wealth Inequality Eroded US Democracy?," 2019; Levchenko et al., "Mars Colonization"; Lara et al., White Paper 12; Sutirtha Bagchi and Matthew J Fagerstrom, "Wealth Inequality and Democracy," vol. 112 (Proceedings. Annual Conference on Taxation and Minutes of the Annual Meeting of the National Tax Association, JSTOR, 2019), 1–40; Namrata Goswami, "China in Space: Ambitions and Possible Conflict," Strategic Studies Quarterly 12, no. 1 (2018): 74–97; Baohui Zhang, "The Security Dilemma in the US-China Military Space Relationship: The Prospects for Arms Control," Asian Survey 51, no. 2 (2011): 311–32.

Ethical[109]	Military[110]
• Social inequality may be exacerbated by current billionaires growing even richer due to space-related activities, stemming from the high financial barrier of entry into the sector. • Long-term space missions may be volunteered for without meaningful prior knowledge about the psychological and physical damage these may pose. • The environmental effects of space exploration are challenging to plan for in a responsible manner. • Speculative ethics about potential first contact with extra-terrestrial life are yet to enter the mainstream, despite 30+ years of scholarship on the subject. • Some scholars argue that space exploration is essential for the survival of the human species for various reasons: o Planetary defence against extra-terrestrial threats, such as: • Asteroid strikes • Gamma-ray bursts (GRBs) • Volatile solar activity o Sustainability of population growth rates o New applied technological innovations o Development of fundamental science o Development of astrobiology	• With terrestrial warfighting increasingly dependent on space-based technologies, military satellites constitute increasingly more high-value targets. It opens the door to space-based conflict escalation. • Several countries have demonstrated anti-satellite (ASAT) capabilities, such as: o The US o China o Russia o India • The development of certain capabilities shows both the military potential of the domain and also the depth of states' dependence on space: o Space military command and control systems o Early missile warning and tracking o Intelligence, surveillance, and reconnaissance (ISR) • The focus of rival powers on space exploration may put NATO and its Allies at a strategic disadvantage in the space domain should investment in such endeavours lag behind. • More and more countries are expected to designate their 'Space Force' as a standalone branch of their armed forces in its own right. • In the medium- and long-term, space vessels are expected to adopt certain military capabilities.

The judicial and military domains contain, by far, the most significant (short-term) externalities within the space domain. Within the judicial domain, as is the case with all emerging technologies, the rapid development of space-related technology means that international regulation has lagged behind real-world applications.[111] Currently, the 1967 Outer Space Treaty lays the foundation for regulating (state) conduct in space, stipulating that the domain is to be used exclusively for peaceful purposes and that all activities in space should occur in accordance

109 Andrew F Cheng et al., "AIDA DART Asteroid Deflection Test: Planetary Defense and Science Objectives," Planetary and Space Science 157 (2018): 104–15; Green, "Convergences in the Ethics of Space Exploration"; Milligan and Inaba, "Ethical Problems of Life Extension for Space Exploration"; David Griffin and Natasha Acimovic, "How Academia Processes the ET Contact Issue and Some Implications for the UFO Community," n.d.; Patrick K King et al., "Late-Time Small Body Disruptions for Planetary Defense," Acta Astronautica 188 (2021): 367–86; Nikola Schmidt, Planetary Defense: Global Collaboration for Defending Earth from Asteroids and Comets (Springer, 2018); Linda Billings, "Public Engagement With Planetary Science: Experiences With Astrobiology and Planetary Defense," in Space Science and Public Engagement (Elsevier, 2021), 121–42; Kovic, "Risks of Space Colonization"; Andrew S Rivkin et al., "The Double Asteroid Redirection Test (DART): Planetary Defense Investigations and Requirements," The Planetary Science Journal 2, no. 5 (2021): 173; P Schouten, "Theory Talk# 3: Alexander Wendt on UFO's, Black Swans and Constructivist International Relations Theory', Theory Talks," 2008; Lara et al., White Paper 12; Lauren Blackwell Landon, Kelley J Slack, and Eduardo Salas, Psychology and Human Performance in Space Programs: Research at the Frontier (CRC Press, 2020); Steven Abood, "Martian Environmental Psychology: The Choice Architecture of a Mars Mission and Colony," in The Human Factor in a Mission to Mars (Springer, 2019), 3–34; Jan Thimo Grundmann et al., "Solar Sails for Planetary Defense & High-Energy Missions" (2019 IEEE Aerospace Conference, IEEE, 2019), 1–21.

110 Marco Langbroek, "Why India's ASAT Test Was Reckless," April 30, 2019, https://thediplomat.com/2019/05/why-indias-asat-test-was-reckless/; Nicholson, "World Fury at Satellite Destruction"; Gertz, "Russia Flight Tests Anti-Satellite Missile"; Jim Wolf, "U.S. Shot Raises Tensions and Worries over Satellites," Reuters, February 22, 2008, sec. Science & Space, https://www.reuters.com/article/us-satellite-intercept-vulnerability-idUSN2144210520080222; Steer and Hersch, War and Peace in Outer Space; Jana Robinson, "Prominent Security Threats Stemming from Space Hybrid Operations," in War and Peace in Outer Space: Law, Policy, and Ethics, Ethics, National Security, and the Rule of Law (Oxford, New York: Oxford University Press, 2021); Sa'id Mosteshar, "Space Law and Weapons in Space," Oxford Research Encyclopedia of Planetary Science, May 23, 2019; Todd Harrison, "Why We Need a Space Force," Center for Strategic and International Studies (CSIS) 3 (2018); Rachel S Karas, "USAF Launches New ISR Flight Plan to Shape Next-Gen Enterprise," Inside the Air Force 29, no. 31 (2018): 1–5; Zhang, "The Security Dilemma in the US-China Military Space Relationship: The Prospects for Arms Control"; Kaitlyn Johnson, "Space Force or Space Corps?," The Center for Strategic and International Studies, 2019; John Mazz, "Modeling Space-Based Intelligence, Surveillance, and Reconnaissance (ISR) in Combat Simulations" (US Army Combat Capabilities Development Command, Analysis Center, 2022); Sitong Liu, Zhanyue Zhang, and Sichen Liu, "Construction and Capability Analysis of Air-Space-Ground Integrated Early Warning and Detection System," vol. 12332 (International Conference on Intelligent Systems, Communications, and Computer Networks (ISCCN 2022), SPIE, 2022), 155–65; Goswami, "China in Space: Ambitions and Possible Conflict."

111 Nienass, "Needed."

with international law.[112] The Outer Space Treaty does prohibit the placement of weapons of mass destruction in the Earth's orbit and on celestial bodies and stationing in space in any other matter[113]. Furthermore, the Outer Space Treaty intends to prohibit a new form of colonial competition as outer space is the "province of all mankind".[114] There is also the 1968 Rescue Agreement, the 1972 Liability Convention, the 1976 Registration Convention and the 1984 Moon Treaty which form the UN foundational space treaties.[115] New challenges, including space debris, overpopulated orbits, radio frequency interferences, spectrum allocation issues and developing counter-space capabilities lack adequate legal regulation,[116] incentivising states to develop their own regulations. This phenomenon can be observed even at the European level, where the legislative landscape is fragmented due to the various Member States having adopted their own national space laws.[117] Shortcomings in the legislative framework governing space – which, in its current incarnation, favour states with the resources to operate within the domain – pose significant negative ethical externalities, too. Low-to-middle-income countries have found themselves largely excluded from the development of legislation.[118]

Increased activity within the space domain also poses several risks within the military domain. With terrestrial warfighting being increasingly dependent on space-based technologies, military satellites pose high-value, vulnerable targets.[119] Space is essential for strategic and conventional operations, facilitating the collection of intelligence, early warning against nuclear attacks, effective weapon deliveries, and the provision of environmental data to support military missions.[120] Space systems have found military purposes through reconnaissance, meteorological, communication, navigation satellites, ballistic missile defence and ASAT weapons.[121] The fact that many space objects are dual-use and can be utilised for both military and civilian goals makes it difficult for states to distinguish between the two, meaning that any conflict with a space-based component risks the disruption of critical civilian infrastructure.[122]

112 Steer and Hersch, War and Peace in Outer Space.

113 Su, "The Legal Challenge of Arms Control in Space."

114 Webb, "The Ethical Use of Outer Space," 2015.

115 Goguichvili, Linenberger, and Gillette, "The Global Legal Landscape of Space."

116 Goguichvili, Linenberger, and Gillette.

117 Nienass, "Needed."

118 Goguichvili, Linenberger, and Gillette, "The Global Legal Landscape of Space."

119 Steer and Hersch, War and Peace in Outer Space.

120 Robinson, "Prominent Security Threats Stemming from Space Hybrid Operations."

121 Mosteshar, "Space Law and Weapons in Space."

122 Mosteshar.

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