German Council on Foreign Relations

No. 21
November 2021

DGAP REPORT

Strategic Compass

Promoting Technological Sovereignty and Innovation: Emerging and Disruptive Technologies

A Workshop Report

Dr. Christian Mölling
Research Director

Florence Schimmel
Research Fellow,
Security and Defense Program

1. INTRODUCTION

By Dr. Christian Mölling

1.1 Emerging and Disruptive Technologies and the Strategic Compass

The Strategic Compass (SC) seeks to adapt the EU to an ever faster-changing security environment. Based on a joint threat analysis, member states aim to agree on clear and achievable strategic objectives in four "baskets": crisis management, resilience, capabilities, and partnerships. These topics cover a broad spectrum of issues, and cannot be addressed comprehensively until the Strategic Compass's presentation date in early 2022. Leaving the mechanics of this EU process aside, there are several topics the SC cannot afford to ignore. One such topic is Emerging and Disruptive Technologies (EDT). As with any other large concept, the outer boundaries of the definition of EDT, that is, what exactly it entails, remains fuzzy. And like any other important concept, it has become politicized as actors with vested interests use the term to further their political or economic objectives.

Technology has always played a fascinating and important role in security and defense. Hence, emphasizing and sometimes exaggerating the role of technology in security has been common for centuries. However, contemporary circumstances differ from the past in two important ways. First, EDTs are mainly civilian or, more precisely, commercial technologies designed for broad consumer variety with a myriad of applications all the way down to entertainment and other everyday uses. Secondly, technology has become one of the main fields of geopolitical competition, especially between the US and China. This brings with it the question of what type of global order will govern global technology issues and international risk management. It is here where the functional perspective of technology collides with geopolitics and geoeconomics. For these reasons, it is now necessary to reassess the link between technology and security.[1]

1.2 The E, D, and T in EDT

While the term EDT is somewhat nebulous and, in fact, describes a rather heterogeneous family of technologies, some common ground on its definition can be found.

T is for Technology. Technologies are human made applications and (although this is often forgotten) procedures that aim to solve human problems.

E is for Emerging. EDTs are part of a wave of new technologies that will be ripe to be transferred into the field and into defense applications over course of the next 20 years. These technological areas are either currently at a promising stage of development or undergoing rapid, revolutionary advances. Examples of such broad technological fields are Data, Artificial Intelligence (AI), Autonomy, Space, Hypersonics, Quantum Computung, Biotechnology and Materials.

D is for Disruptive. Development in these areas will result in vastly improved defensive and offensive cyber capabilities; new generations of sensors, space-based capabilities, and autonomous weapon systems; and much-improved air and missile defense, drones, and long-range precision missiles. This will have a massive impact on security and defense, transforming the way armed forces are organized and equipped, as well as how they operate. Disruptive effects will most likely be produced by combinations of EDTs and the complex interactions between them.

1.3 The anticipated challenges of EDT for security and defense

Like all technologies, EDTs represent both opportunities and risks for the world in general, and security and defense in particular. However, in an environment of not only economic but also political competition where technologies are a key tool, what matters is exploiting them better and faster than competitors. This is especially true for EU member states, as well as the US. Western security and defense forces owe a significant proportion of their power and impact to technological superiority. In defense circles, this is often referred to as "quality over quantity" – having a technological edge against other, bigger armies. Current developments are fundamentally challenging this approach in terms of strategy, planning, and even military engagement. However, there is currently no prioritization to strategically guide investment, resulting in a fragmented landscape.

EDTs pose a serious challenge to EU and NATO states because other actors are challenging their technological superiority through independent innovation in strategically relevant EDT areas. This is more true of China than Russia as the latter has less capacity to systematically challenge technological superiority. Equally importantly, EDTs stem from civilian research, even if in some cases this is state-

1 I subsume the debate on a „Third offset strategy" under the current debate. This debate has been started in 2014 by the US DoD: U.S. Secretary of Defense, "Memorandum," November 15, 2014, http://www.defense.gov/Portals/1/Documents/pubs/OSD013411-14.pdf

owned. Competition for consumers between commercial enterprises has led to shorter innovation cycles, especially in the area of information technology, and to a geographical diversification of centers of innovation, with new hubs emerging particularly in Asia.

The ability of non-Western actors to identify promising civilian innovations and increasingly incorporate these into defense applications has led, inter alia, to the perception of a growing erosion of conventional deterrence and defense capabilities relative to rising powers and new international security actors. Moreover, the civilian origins of these technologies, and commercial interest in them, further limit the EU and NATO's ability to control their function and proliferation.

While Western states have started to integrate EDTs into their security and defense systems in an attempt to reclaim technological superiority, this task is also shaped by the need to meet legal and ethical standards, as can be seen in debates around the use of drones and the increasing autonomy of military systems. Moreover, as the coming years will be unlikely to see any significant increase in defense budgets, decisions on where investments in EDTs can make a difference, and to what extent cooperation is a solution, will be determined by short term business interests rather than the need to future-proof national and European security.

1.4 The Strategic Compass: How to think about EDTs and which technologies to prioritize

When thinking about EDTs, there are three important aspects that should be taken into account:

1. The growing importance of EDTs and their political and security implications;

2. The unclear scope of the term EDT and the lack of prioritization of key technologies;

3. The risk of prioritizing short-term wins over long-term strategic goals.

Given these factors, it makes sense to engage in collective, systematic, and analytical stakeholder discussions about the relationship between EDTs and the Strategic Compass. Only by doing so can the EU hope to outline a relevant and sustainable approach to the issues at hand.

EDTs transcend the basket structure of the Strategic Compass because they touch on aspects of all issue areas. The following chapters look to further define the concept of EDTs, explain which technologies should be prioritized and why, and offer suggestions on how to incorporate EDTs into the Strategic Compass process in order to improve Europe's technological sovereignty and innovation. As a result, this paper aims to offer input that will help answer two overarching questions: How should EDT be treated in the final Strategic Compass document, and which technologies should be prioritized?

These two questions are addressed in chapters 3 and 4. The final chapter notes the key takeaways from the stakeholder discussion.

2. WORKSHOP RESULTS PAPER

Compiled by Dr. Christian Mölling & Florence Schimmel

Emerging and disruptive technologies (EDT) transcend the four-basket logic of the EU Strategic Compass as they touch on aspects of all issue areas. To break down this complex topic, the workshop was based on two input papers that focused on aspects of sovereignty and innovation. While the discussion cannot and should not be held exclusively in relation to the security and defence realm, participants were encouraged to highlight initiatives relevant for the scope of the Strategic Compass process.

Strategic Investment for Innovation

2.1. Participants agreed on the **importance of foresight exercises** to explore the potential developments and applications of EDTs, as well as the respective dependencies and weaknesses that might be implicated in the virtual and physical realms.

2.1.a. Such foresight should be informed by technology experts and policy makers alike, and conducted at the EU level to inform national institutions. Discussants concurred that **member states need to increase coherence and cooperation**, also regarding existing frameworks, to fully leverage European potential vis-à-vis other global players.

2.1.b. One speaker singled out the defence budget as the only multi-annual budget at the national level. This enables **longer-term planning**, but should not impede the ability to adjust it on a quarterly if not monthly basis, discussants agreed. Rapid developments, e.g. in quantum technologies demand **agile political steering.** The technology race was deemed real, but the speed of innovation was considered to be rendered useless if political action lags behind.

2.2. Such foresight exercises should translate into **concrete roadmaps that, inter alia, set priorities and focus investment**. Participants proposed clustering technologies in a family structure for a better overview, as well as clear and transparent communication.

2.2.a. There was consensus about the importance of the private sector. Consequentially, **a common understanding of the top priority breakthroughs needed at EU level should guide both public and private resources.**

2.2.b. Open communication about intents and goals was identified as an important part of signalling to the global partners and adversaries.

2.2.c. The **focus of investment** was rated even more important than increasing current investment levels. Precise, prescient, and long-term investment – financially and politically – is also what **recruits and keeps talented workers in the EU.** Some added that EU investment should ensure the results of the investment stay in the EU, and that the EU as a whole rather than single member states profits from the innovations derived from it.

2.2.d. So as to avoid costly and confining path dependencies, participants proposed **following a modular approach** in order to be able to "plug in and play" with innovations.

Institutional Set-Up for Sovereignty

2.3. Some participants regarded the notion of **dual use technologies as an unreliable concept.** Any emerging technology – that is, technology with a low technology readiness level (TRL) – is potentially dual use at that stage. This is why some discussants found trying to separate civilian and military uses to be unrealistic, or even misleading. As well as needing both public and private representatives to work together, expertise from civilian and military end users (with the industrial base) should be incorporated at all times.

2.3.a. In crisis management, likely future conflict theatres will include high-tech elements, and the need for interoperability is also likely to increase. In an inclusive approach, it is important to explore whether the modernization of existing platforms/systems or the development of new technologies is more cost effective.

2.4. Advocates of this approach also favoured **framing the discussion around political-strategic problems and challenges rather than on EDTs** (mission-based rather than tech-based). For example, access to verified and verifiable information is at the core of our democratic societies. With little cost or effort, adversaries such as Russia can inflict much damage.

2.4.a. This insight implicates the need for EU action beyond the Strategic Compass. In general, many participants brought up the potential of linking up all EU efforts in this area: efforts from the Commission, projects within PESCO, the EDA, the EDF, etc. An **appropriate support structure could bundle together**

insights and expertise from the Commission's scanning of raw material shortfalls to Green Deal implications and national military planning. Also, it could prevent security and defence implications from being overlooked or excluded like in the AI strategy.

2.4.b. In this context, discussants stressed the importance of not overlooking older technologies by fixating disproportionately on emerging technology in relation to their general disruptive character. This links back to the importance of foresight exercises.

2.4.c. One speaker emphasized the **need for a pragmatic 80/20 approach** so as not to counteract the initial prioritization derived from the foresight exercise. Some added that pragmatism should also entail preventing short-term cost-effectiveness from hindering the goal of gaining strategic advantages over other global players. This could include producing in the EU despite higher costs.

2.5. The fact that most EDTs are not stand-alone technologies was raised. Therefore, a **"system of systems" approach** is needed that brings together various related EDTs (e.g. AI, cloud computing, automation, quantum-resistant cryptography, synthetic biology, etc.), stakeholders from the public and private sector, both civilian and military, and insights from fundamental and applied research.

2.5.a. The foresight exercise should also reveal the skill sets needed by European personnel as well as the wider population, and help with prioritization within the system of systems approach. Participants underlined that skill sets are not necessarily about very specialized expertise, but also include cyber hygiene skills, especially in strategic sectors.

2.5.b. Many believed that the EU wants to and should employ ethical standards, regardless of whether the its adversaries observe them or not. During the discussion it remained unclear at which stage ethical considerations would be best placed. This could especially touch upon the dilemma of proliferation, which is desirable in the civilian sector but not in the military sphere.

On the Global Stage

2.6. Participants identified two major fields for potential **cooperation with NATO: joint foresight** and agreeing on matters of **standardization**. As the alliance and the union have many similar security interests, conducting foresight exercises together could both pool expertise and improve robustness of outcomes. Regarding standardization, the EU could profit from NATO's capacity to harmonize and capitalize on its own strength of organizing implementation. Eventually, both initiatives serve the alignment of strategic and tactical behaviour.

2.6.a. Discussants highlighted the importance of being able to keep up with and exceed Chinese and Russian capabilities. However, the necessity of cooperation was also labelled a reality. Some participants proposed exploring climate change mitigation technology as an area for cooperation.

2.6.b. Some participants identified intellectual property rights (IPRs) as a potential roadblock for EU-NATO cooperation and it remained unclear how this could be mitigated.

2.7. One participant raised the UK Integrated Review as an example of putting scientific advancement and technological evolution at the centre. EDTs could therefore be a promising issue area to catalyse joint approaches with the UK in security and defence cooperation.

2.8. One expert remarked that standardization (how tech fits together and works) is not the same as regulation (how tech can or should be used). Even more than regarding innovation, the players who dominate these areas of EDTs set the pace on a geopolitical level. The participants concluded that the EU needs strategies for cooperation and competition with both partners and adversaries: in good cases for leveraging synergy effects, in difficult cases for dealing with inadequacy and ethical approaches the EU does not agree with, but which are being employed by adversaries.

The workshop took place on 4th May 2021 with support from the German Federal Foreign Office. This paper sums up the main points of the discussion as perceived by the rapporteurs. It does not necessarily reflect their opinion. Participants included representatives from member state ministries and the European Union, as well as from the European think tank community. We thank all participants and especially our excellent speakers for their valuable input. Any comment is welcome and may be sent to schimmel@dgap.org.

3. INPUT PAPER

PROMOTING TECHNOLOGICAL SOVEREIGNTY AND INNOVATION: EMERGING AND DISRUPTIVE TECHNOLOGIES

By Dr. Daniel Fiott, Security and Defence Editor, European Union Institute of Security Studies[1]

3.1. What do "emerging and disruptive technologies" mean in security and defense?

Any discussion about emerging and disruptive technologies (EDTs) must first interrogate overused and unclear concepts. First, the terms "disruptive technologies" and "disruptive innovation" refer to processes or products that up-end a well-established market by fundamentally changing the way the market functions. It is also assumed that disruptive innovation revolutionizes a market by introducing widely accessible and cost-effective products or services. Examples of disruptive innovation include the way that video streaming services displaced rental video shops. Obviously, in the defense sector such a definition only takes us so far as the costs of innovation are not low, and, ideally, proliferation of defense technologies is to be avoided in order to maintain a military-technological edge and contribute to arms control. Furthermore, examples of genuine innovation in the defense sector can be hard to come by. Unmanned aerial vehicles are often touted as disruptive technologies, but most of the technologies they integrate rely on past innovations related to propulsion, sensoring and radio communications.

3.2. How best to conduct EDT horizon scanning, analysis and assessment?

To be clear, in the defense sector the related terms "emerging" and "disruptive" technologies usually refer to a series of trends and challenges: (1) those future technologies that have not yet been developed, but which may have a profound effect on the conduct of military operations, defense planning, and innovation and acquisition; (2) civil innovation and technology trends that threaten to outpace and outperform defense innovation patterns and fundamentally alter defense procurement cycles; and (3) those technologies that can be utilized to enhance the performance and endurance of existing legacy platforms. It should be apparent that strategic foresight and trend scanning are critical components of any viable and effective EDT strategy. Horizon scanning allows for the identification of technological obsolescence, as well as future technological trends.

3.3. How to shift risk perceptions in defense for the development of EDTs?

Additionally, EDTs imply a shortening of research and development timeframes, even if defense innovation and procurement cycles embody long-term processes. In this respect, there is a need to think about how the defense sector can benefit from sporadic and quick innovation lead times in the commercial sector. Being able to profit from and include civil innovation patterns in defense calls for a mindset change and new strategies. This begins by casting a wide net for potential stakeholders including commercial firms, SMEs, research institutes, start-ups, universities, etc. Additionally, EDTs require different risk, investment perceptions, and strategies ("high risk, high return"), but these approaches are relatively alien to the defense sector. Consider that the integration of EDTs into legacy platforms may not lead to greater performance and it is not a given that the modernization of legacy platforms is cheaper than integrating EDTs into new platforms and systems.

3.4. How to achieve an EDT "system of systems" approach with finite resources?

EDTs should not be thought of as stand-alone technologies and systems. They are, in fact, part of a system of systems. The vast majority of EDTs are worthless without data collection, management, and use. Data powers Artificial Intelligence(AI)-enabled systems, but data is vital for blockchain and automation. Any sound EDT strategy should seek mastery of the system of systems of EDTs, but this is challenging with a finite level of financial resources. Skills and training are vital for the development of EDTs too, and there is under-investment in the skills and personnel required to digitalize armed forces. EDTs give the impression that automation and AI can reduce the need for human involvement, but actually the reverse is true as skills, training and personnel retention are crucial ingredients for innovation and strategic effect. A finite level of resources also implies that technological prioritization is required, but this could undermine a system of systems strategy.

1 The views in this note do not necessarily reflect the views of the EU Institute for Security Studies or the European Union.

3.1 3.5. How to safeguard against non-European EDT strategies and uses?

AI is a specific EDT that requires a "whole of society" approach. AI raises questions of ethics and law, and questions of human responsibility and liability are important. There are calls to ensure that EDTs respect European values and rules, but there is less clarity about how actual and potential adversaries will employ EDTs in a military context. This places a strategic burden on Europe: EDTs may be applied to enhance the effectiveness and performance of military operations, but there is a need to also invest in EDTs that provide a deterrence effect and countermeasures against adversaries that may not "play by our rules". Such developments are already visible in the area of cyberdefense and the use of predictive AI. Greater intellectual investment is needed in understanding the balance between the control and development of EDTs.

3.6. How to achieve a credible overarching EU strategy for EDTs and defense?

An overarching strategy for EDTs and defense in the EU is absent. What exists today is a patchwork of different strategies (i.e. industrial strategy, digital services/markets acts, data strategy and AI strategy) that do not comprehensively address the defense angle of EDTs. In the context of the European Defence Fund, both DG DEFIS and the European Defence Agency are engaged in investments in EDTs for military purposes, and the European Commission has developed a synergies action plan for civil, space and defense industries in order to capitalize on EDTs. Without an overarching and coherent EU strategic vision for EDTs and defense, however, industry and military planners alike will be sent mixed and possibly lukewarm signals. Financial resources and investment are the bedrock of technological sovereignty, but an ambitious strategy that prioritizes investments and challenges political taboos is sorely needed today. The EU's added value is in connecting various policy domains and this should be the case for EDTs and defense.

3.7. How can EU defense capability development processes integrate EDTs?

The emergence of EDTs poses questions for the EU's current system of defense capability development. The European Defence Fund offers financial incentives to invest in disruptive technologies, but only a handful of PESCO projects address EDTs directly. The European Defence Agency has developed new initiatives to give greater clarity to the Capability Development Plan, including the Strategic Context Cases and the Overarching Strategic Research Agenda. However, there is a need to consider how EDT scanning and assessment can be better hardwired into EU processes. The development of technology roadmaps could help provide greater clarity, prioritization and strategic direction for the development of EDTs in defense. Beyond roadmaps, however, there is also a need to better connect discussions about EDTs with the operational needs of military planners and operators – there can be a gap between technology-centric and capability-centric understandings of capability development. There could also be scope to better integrate EDT considerations within military scenario planning and exercises: EDTs can be threats in their own right or aggravate/alleviate existing crisis and conflict trends.

3.2 What role for defense in protecting critical digital and physical supply/infrastructures?

The development of EDTs also connects to critical supply and critical infrastructure protection – without a secure infrastructure, certain EDTs cannot function properly or are open to hostile manipulation. If technological sovereignty means anything, it implies Europe's ability to master and control critical economic and industrial interdependences. Achieving technological autarky may be impossible or undesirable, but critical supplies (e.g. rare earth minerals) and sophisticated EDT enablers (e.g. semiconductors) are a key vulnerability for Europe. There is a strong case for lowering Europe's dependences in these key critical domains by boosting manufacturing capacity and know-how in Europe. Additionally, the digitalization of the European economy is dependent on the safe and proper functioning of key physical infrastructure such as space systems, submarine cables or supercomputing and data processing locations. A challenging question is what role (if any) armed forces could play in protecting critical physical infrastructure.

3.8. How to enhance EU-NATO complementarity on EDTs?

The NATO alliance increasingly sees itself as a "transatlantic forum" on EDTs. This aim has been stressed during the NATO 2030 reflection process. NATO fears that EDTs are proliferating into the hands of adversaries, and this is eroding the alliance's military-technological superiority. NATO also recognizes that the growth of EDTs poses a risk with regard to alliance cohesion because unequal development and ownership of EDTs can lead to lower interoperability and higher technology gaps. While the alliance has a proven track record of developing standards, NATO has neither the financial resources nor regulatory power to take a comprehensive lead on the question of EDTs. This situation has even given rise to new ideas such as a NATO Innovation Fund and the Defense Innovation Accelerator for the North Atlantic (DIANA).[2] There is certainly scope for more EU-NA-

2 NATO Advisory Group on Emerging and Disruptive Technologies, "Annual Report 2020", 2021, p. 20, <https://www.digitaleurope.org/wp/wp-content/uploads/2021/02/

TO common engagement with the strategic challenges and opportunities that could emerge due to EDTs. In fact, the EU's Political and Security Committee and the North Atlantic Council met in March 2021 to discuss EDTs.

3.9. Technological sovereignty in a transatlantic context

The development of EDTs touches on the sensitive issue of industrial competitiveness. Technological sovereignty implies mastery and control of technology. This is certainly the case in the United States, where two early Executive Orders under the Biden administration target domestic technological competitiveness ("Buy America") and global critical supply chains. There is a fear that promoting EDT uptake within NATO is a way to enhance the competitiveness of American firms that develop EDTs; the US already has a comparative advantage in many critical technology sectors. A key question for the EU then, is how to engage in a transatlantic dialogue on EDTs without harming its own industrial competitiveness or control over critical technology sectors. Proposals such as the EU-US Trade and Technology Council or the EU-US Defense Dialogue could help to work out differences over regulations, standards, extraterritorial measures, forced transfers of technology, and intellectual property rights.[3]

4. INPUT PAPER

WHAT TECHNOLOGICAL PRIORITIES FOR EUROPE'S STRATEGIC AUTONOMY?

By Andre Loeskrug-Pietri, Executive Chairman, Joint European Disruptive Initiative (JEDI)[4]

New technologies are steadily changing the way we work, travel, communicate and relate to each other. They also exert a major influence on the strategic autonomy of state actors – that is, the ability to freely take decisions and actions in an interdependent world without being subject to foreign interference.[5] We need to recognize the radical challenges posed by the adoption of emerging technologies by organizations or states trying to undermine or threaten the European Union, its citizens, or its way of life, and their ability to have an asymmetrical and highly destabilizing impact.

In a world characterized by a high level of global economic interdependence and by the importance of scale, the countries of the old continent can only prevent these emerging threats by working at the European level. European strategic autonomy in critical technologies refers to the ability of European actors to own a degree of control over strategic technologies, i.e. technologies that already or soon will play a critical role in the functioning and resilience of our economies and societies. This also includes technologies that may have a significant impact on our political models, institutions, and values.

Owning a degree of control does not automatically imply that Europe should replicate and develop a whole industry around each of these technologies. Nor should strategic autonomy in critical technologies be understood in absolute terms. Rather, it should be understood as a flexible concept, as a capability that actors can and must extend as far as they can to increase their freedom of decision and action.

European strategic autonomy in critical technologies starts with identifying them. The following selection of three technological categories on which Europe should focus its efforts is proposed: **(1)** critical infrastructures, **(2)** strategic technological sectors, and **(3)** selected key technological bricks ("pillars") without which a sufficient degree of control over infrastructures and technological sectors cannot be achieved.[6]

4.1 Critical infrastructures

The first fundamental pillar of strategic autonomy is the control, protection, and strengthening of our critical technological infrastructures.

EDT-Advisory-Group-Annual-Report-2020.pdf>.

3 European Commission, "Joint Communication to the European Parliament, the European Council and the Council: A New EU-US Agenda for Global Change", JOIN(2020) 22 final,12 December, 2020: <https://ec.europa.eu/info/sites/default/files/joint-communication-eu-us-agenda_en.pdf>.

4 JEDI is the most advanced initiative to build a European counterpart to the US's Defence Advanced Research Projects Agency (DARPA).

5 L. Poirier, Essais sur la stratégie théorique [Essays on Theoretical Strategy], Paris, Foundation for National Defense Studies Fondation pour les études de défense nationale , 1982.

6 A. Loesekrug-Pietri, "Technology Strategies in China and the US, and the Challenges for European Companies", French Institute of International Relations, 2020

Submarine cables: Submarine cables use fiber-optic technology, whereby information is encoded in waves of light transmitted by lasers across thin glass. Carrying more than 90% of international communications traffic and, as of 2017, transporting $10trn of financial transfers every day,[7] submarine cables are critical to our information and communications infrastructure. Any damage to these cables would have major consequences for telecommunications and therefore for the economies of countries affected by a breakdown. Increasingly, non-state actors such as Google and Facebook are exerting control over these cables.

5G & 6G networks: The shift of cellular communication networks from the 4th to the 5th (and later 6th) generations of cellular network standards (that is, to 5G and 6G) will have a major impact on our societies. It is estimated that 5G alone will contribute to roughly 5.3% of global GDP growth over the next 15 years[8] and reduce energy consumption across industrial sectors by 15%.[9] 5G and 6G networks will be a game changer for the competitiveness of European industries, but will also play a critical role in healthcare, energy management, and the military. Their disruptive character makes them a strategic asset that Europe cannot afford to not control.

Satellites: The proliferation of devices using satellite positioning systems such as GPS or Galileo, the development of space imagery services for defense and industrial use, and the vital role of telecommunications are increasing our dependence on satellites. Thus, their protection is of great strategic importance. Europe faces two main security challenges related to satellites. The first relates to protecting them from the growing risks of collision with space debris, while the second relates to potential crisis situations in space. By successfully conducting an anti-satellite missile test on 27 March 2019, India became the fourth country capable of destroying an enemy satellite, after the US, Russia and China.[10] Other coercive actions that could be conducted in space include blinding or obscuring the sensors of an observation satellite, jamming or intercepting a communication satellite, using a space maintenance device to damage satellite equipment, or blinding it from the ground with a laser.

Data centers & cloud computing: The amount of data generated by human activity is growing at an ever-increasing rate. The International Data Corporation (IDC) estimates that the global volume of data generated by both individuals and companies will grow from 59 zettabytes (ZB)[11] in 2020 to 175 ZB by 2025.[12] For now, 90% of data generated globally is stored and managed in data centers, with the remaining 10% stored in devices such as smartphones and personal computers. While the growth of the Internet of Things and of "edge computing" will decrease the importance of centralized data centers,[13] an issue of particular importance for European strategic autonomy is their location, which determines the legal regime that applies to the data they store and thus our degree of control over them.

High Performance Computing: Increasingly, supercomputers are needed to harness big data and facilitate scientific discoveries that need large computational efforts, such as cryptography, materials science, artificial intelligence technologies, and climate modelling. Thus, they can be considered a strategic resource for research performances and competitiveness.

Critical energy grids: Energy grids are critical for the daily functioning and resilience of our societies. As the 2015 hacking of the Ukrainian power distribution grid clearly demonstrated, the main concern for this type of infrastructure relates to the cybersecurity threats that arise from the increasing digitalization of European energy systems.

4.2 Strategic technological sectors

Technologies are evolving at an ever-faster pace. It is therefore critical to identify the main sectors where disruption and technological acceleration are most likely to occur and to have a major societal, economic and strategic impact.

Artificial intelligence (AI) systems: AI systems technology, [14]specially deep learning, is undoubtedly the field that has

7 Wayne Nielsen et al., "Submarine Telecoms Industry Report, 7th Edition", Submarine Telecoms Forum, October 2019. https://subtelforum.com/products/submarine-telecoms-industry-report/.

8 "Mobile Industry Generates $565 Billion in Additional Global GDP by unlocking the Right 5G Spectrum: GSMA Study", GSMA, 12 December, 2018: <http://www.gsma.com/newsroom/press-release/mobile-industry-could-generate-565-billion-in-additional-global-gdp> (accessed 9 September, 2020).

9 Börje Ekholm, "3 ways to boost innovation in the 5G digital economy", World Economic Forum, 15 January, 2020: <http://www.weforum.org/agenda/2020/01/3-ways-to-boost-innovation-in-the-5g-enabled-digital-economy> (accessed 9 September, 2020).

10 Ashley J. Tellis, "India's ASAT Test: An Incomplete Success", Carnegie Endowment for International Peace, 15 April, 2019: <https://carnegieendowment.org/2019/04/15/india-s-asat-test-incomplete-success-pub-78884> (accessed11 September 2019).

11 One zettabyte is equivalent to 10^{21} bytes.

12 David Reinsel, John Gantz and John Rydning, "Worldwide Global DataSphere Forecast, 2020–2024: The COVID-19 Data Bump and the Future of Data Growth", The International Data Corporation, April, 2020.

13 IRDS, "International Roadmap for Devices and Systems – Systems and Architecture", 2020 edition, p. 3-4

14 Artificial intelligence systems are defined by the EU panel of experts on AI as "software – and possibly also hardware systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions". Using the classification of Goodfellow

seen the most substantial advances in recent years, mainly thanks to the increase in data and computing capacities, and the improvement of algorithmic and learning techniques. Due to their consequences and pervasiveness, AI systems and related technologies are critical for the strategic autonomy of Europe. They have met the conditions for a qualitative leap in many areas of human activity. By 2030, for instance, AI-powered technologies could increase labor productivity by an average of 30% compared with 2015,[15] and contribute $15.700 trillion to the global economy.[16]

Information and communication platforms: Information and communication platforms, and more specifically social networks, have fundamentally transformed the way we interact with others and inform ourselves, as well as our consumer behavior. A 2019 survey conducted by Eurobarometer in 34 countries (including all 28 EU member states) indicated that 64% of Europeans used social networks once a week, and 48% used them every day or almost every day. This number rose to 87% for the 15–24 age group, suggesting that the importance of these communication platforms will rise in the near future.[17] As highlighted by the Cambridge Analytica affair, the impact of these platforms on citizens' perceptions, on the formation of public opinion, and on our democratic life should not be underestimated.

Face recognition and contact-tracing systems: While European societies are understandably anxious about surveillance technologies, they may also have societal benefits. These benefits will not be restricted to law enforcement, but spread to other sectors such as healthcare. Contact-tracing applications, for example, are considered to have played an important role in limiting the Covid-19 epidemic in South Korea.[18] Face recognition can also be used to track a patient's use of medication, support pain management procedures, detect genetic diseases and support impaired individuals. State actors have expressed growing interest in these technologies. The AI Surveillance Index developed by the Carnegie Endowment for International Peace identifies at least sixty-four countries that are incorporating facial-recognition systems into their AI surveillance programs, the majority of them being advanced democracies, including seven EU member states.[19]

Quantum technologies: Quantum technologies will revolutionize the way we perform information computing activities, which are currently based on the binary logic of Boolean algebra. The quantic paradigm is expected to produce exponentially more efficient algorithms for solving important classes of problems,[20] to enable the development of very accurate sensors, and, together with quantum cryptography, to improve the security of our communications.[21]

Genomic technologies: So-called living technologies may have the greatest impact of all over the next century. Gene-editing technologies such as CRISPR/Cas9, whose developers were recently awarded a Nobel Prize in Chemistry, is particularly powerful, as are gene drives. Each of these tools can dramatically modify a gene pool, including genes responsible for malformations and serious diseases.[22] The potential of RNA messengers has been highlighted by the Covid-19 pandemic, and may disrupt the way and the speed with which we develop new vaccines.[23] Genomic technologies will significantly change health management, disease diagnosis, and treatment. Their high disruptive potential and the bioethical questions arising from their use mean they are of strategic interest to Europe and its populations.

Clean energy: One of the most pressing challenges faced by our societies today is to limit global warming. To achieve this goal, the production, transportation, distribution, and use of clean energies – that is, energies that do not emit greenhouse gases (GHG) when in use, and which are produced through non-polluting methods – will be absolutely critical. Beyond their immediate interest for decarboniza-

et al., there are four main types of AI systems: (1) rule-based systems, (2) machine learning systems, (3) representation learning systems and (4) deep learning systems. See: EU Commission High-Level Expert Group on Artificial Intelligence, "A definition of AI: Main capabilities and scientific disciplines", 8 April, 2019, p.6: <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56341> (accessed 7 July, 2020);Ian Goodfellow, Yoshua Bengio and Aaron Courville, Deep Learning (MIT Press, USA, 2016), p.2-5.

15 James Manyika et al., "Jobs Lost, Jobs Gained: What the Future of Work Will Mean for Jobs, Skills, and Wages", McKinsey Global Institute report, November, 2017: <http://www.mckinsey.com/global-themes/future-of-organizations-and-work/what-the-future-of-work-will-mean-for-jobs-skills-and-wages>.

16 "The Mobile Economy 2019", GSMA Intelligence Report, 2019, p. 43: http://www.gsmaintelligence.com/research/?file=b9a6e6202ee1d5f787cfebb95d3639c5&download>.

17 "Media use in the European Union", Standard Eurobarometer 92 (survey requested and coordinated by the European Commission's Directorate-General for Communications), Autumn 2019, pp. 6, 21: https://op.europa.eu/en/publication-detail/-/publication/c2fb9fad-db78-11ea-adf7-01aa75ed71a1/language-en/format-PDF/source-164536003.

18 Heesu Lee, "These Elite Contact Tracers Show the World How to Beat Covid-19", Bloomberg, 27 July, 2020: <http://www.bloomberg.com/news/articles/2020-07-25/these-elite-contact-tracers-show-the-world-how-to-beat-covid-19> (accessed 7 September, 2020).

19 "AI Global Surveillance Technology", Carnegie Endowment for International Peace: <https://carnegieendowment.org/publications/interactive/ai-surveillance> (accessed 7 September, 2020); Steven Feldstein, "The Global Expansion of AI Surveillance", Carnegie Endowment for International Peace, September, 2019 <https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847>.

20 International Roadmap for Devices and Systems , "International Roadmap for Devices and Systems – Executive Summary", 2018 edition, p. 16.

21 "Science & Technology Trends 2020-2040 – Exploring the S&T Edge", NATO Science & Technology Organization, 2020, p.19.

22 Xu Xun, "We are witnessing a revolution in genomics – and it's only just begun", World Economic Forum, 24 June, 2019: <http://www.weforum.org/agenda/2019/06/today-you-can-have-your-genome-sequenced-at-the-supermarket/> (accessed 7 September, 2020).

23 See Willy Shih, "Could COVID-19 Spur a Revolution in Vaccine Development?", Forbes, 16 February, 2020: <http://www.forbes.com/sites/willyshih/2020/02/16/could-the-covid-19-spur-a-revolution-in-vaccine-development/#5f30b3b07c8c> (accessed 11 September, 2020).

tion, clean energies can also be a strategic asset, an opportunity to increase European energy autonomy.

4.3 Technological pillars

Not all technologies have the same importance. In order to remain technologically sovereign, Europe will need to master the most critical technologies, those which are at the core of several sectors and have the biggest strategic and economic impact. Focus and significant investments will be required.

<10 nm semiconductors: Semiconductor-based devices are the components of our information-processing systems. They are used everywhere, from high-performance computing systems, connected devices, cars, and smartphones to the infrastructure of our communication systems.

AI accelerators: One of the essential technological pillars of AI development is an AI-specific class of computing hardware known as AI accelerators. The last decade has seen the rise of these devices, especially Graphics Processing Units (GPUs) and Application Specific Integrated Circuits (ASICs) such as Google's Tensor Processing Unit (TPU).[24]

5G antennas: 5G antennas, known as small cells, are critical for the effective deployment of the 5G network. They act as the low-powered access point connecting mobile devices to broader cellular networks. One of the advantages of these small antennas that, unlike 4G macro cells, they enable the densification of the radio access network. This leads to increased performance in terms of coverage, capacity and quality of service, especially in dense urban areas.[25]

Natural-language processing (NLP): Natural language processing (NLP) refers to a set of tools which use AI to enable information-processing systems such as computers to automatically recognize, understand, interpret and alter human language. This has enormous implications in terms of development of autonomous systems and decision-making, be it in healthcare, industry, energy, or the defense sector. Through its ability to automatically extract information or to recognize what is expressed in a comment or sentence, NLP will bring about a strategic shift in the ability of actors to take informed, real-time decisions and understand situations.[26]

AI-powered cybersecurity protocols: AI algorithms can greatly benefit the cybersecurity of information and communication networks on four levels: (1) the use of biometric log-ins instead of passwords; (2) earlier and faster detection of cyberthreats and malicious activities; (3) continuous updates on the evolution of threats through monitoring and analyzing cyberspace; (4) strengthening cybersecurity capabilities by adapting the authentication framework and blocking access for users exhibiting suspicious behavior.[27]

Next-generation batteries and green hydrogen-related technologies: Electricity and hydrogen produced by renewable energy sources are considered by many observers to be among the best solutions for decarbonizing our societies. Both batteries and hydrogen offer means of storing, transporting and even using the energy produced by renewable sources. Indeed, one of the shortcomings of wind and solar energy is that they are intermittent, making energy storage solutions such as hydrogen and batteries necessary for their wider adoption. In terms of transport and end-uses, both electric batteries and green hydrogen – that is, hydrogen produced by electrolysis powered by renewables – are considered to be important and complementary solutions to decarbonize hard-to-abate sectors. Green hydrogen and its derivatives (ammoniac or synthetic fuels), are also considered powerful alternatives to fossil fuels in several industries, as well as in the heavy aerial, maritime and terrestrial transportation sectors.[28]

4.4 Conclusion

The concept of "critical technologies" is pervasive, covering a wide range of technologies used in sectors from healthcare to industry, and even in the decarbonization of our societies. It is also a concept in constant evolution; the technological sector is evolving at an ever-faster pace, generating new ideas and paradigms that we could not have imagined.

Europe has a great number of assets, and true potential in several of the strategic technologies discussed above. It has

24 International Roadmap for Devices and Systems, "International Roadmap for Devices and Systems – Application Benchmarking", 2020 edition, p.10: Li Du and Yuan Du, "Hardware Accelerator Design for Machine Learning", in Machine Learning – Advanced Techniques and Emerging Application (ed. Hamed Fahradi), IntechOpen, 2018: <http://www.intechopen.com/books/machine-learning-advanced-techniques-and-emerging-applications/hardware-accelerator-design-for-machine-learning>.

25 "Setting the scene for 5G: opportunities and challenges", International Telecommunications Union, 2018, p.10: <http://www.itu.int/pub/D-PREF-BB.5G_01-2018>.

26 William D. Eggers, Neha Malik, Matt Gracie, "Using AI to unleash the power of unstructured government data", Deloitte Insights, 16 January 2019:. <http://www2.deloitte.com/us/en/insights/focus/cognitive-technologies/natural-language-processing-examples-in-government-data.html> (accessed 10 September 2020).

27 Naveen Joshi, "Can AI Become Our New Cybersecurity Sheriff?", Forbes, 4 February, 2019, https://www.forbes.com/sites/cognitiveworld/2019/02/04/can-ai-become-our-new-cybersecurity-sheriff (accessed 10 September, 2020).

28 See: International Energy Agency, "The Future of Hydrogen – Seizing Today's Opportunities," report prepared for the G20, Japan, June, 2019: <https://www.iea.org/reports/the-future-of-hydrogen>; Cédric Philibert, "Perspectives on a Hydrogen Strategy for the European Union", Etudes de l'Ifri [IFRI Studies], Center for Energy & Climate, French Institute for International Reations, April, 2020: <http://www.ifri.org/sites/default/files/atoms/files/philibert_hydrogen_strategy_2020.pdf>.

very strong research and development activity in the quantum and green energy technological sectors, is the home of world leaders in 5G, is the most advanced continent in the field of robotics, and is a global space power. But despite these advantages, it remains significantly dependent on the United States and, increasingly, on China for most of its critical digital infrastructure, be it data centers, cloud computing, information and communication platforms, or even supercomputers, AI and autonomous systems, synthetic biology, or submarine cables.

In order to tap into its full potential, protect its assets, and gain true geopolitical influence, Europe needs a significant political push, and a revolution in terms of its mindset. Progress cannot be achieved without the adoption of a strategic perspective on the technological sector. Acknowledging the urgency of the situation, the new Commission has made several steps in this direction. While these efforts have been appreciated, they remain too small or too slow relative to the "warp speed" with which technology is evolving.

The true challenge for Europe lies in the need to achieve significant progress to reach scale through the completion of digital single markets in technology and the digital space, as well as dealing with inefficient funding mechanisms that sometimes rely more on the logic of "spray and pray" than on focused and result-driven approaches. This is compounded by an overall absence of independent impact assessments for policies, preventing agility and improvements

A lack of cohesion and cooperation among EU member states, as highlighted in the fields of AI, quantum or hydrogen, where most member states have their own strategies, hinders the EU's capacity to anticipate at a time when it is imperative for it to focus on the next big things: on the strategic issues of the near- and medium-term future rather than the battles of the past. Cutting-edge technologies based in Europe cannot be developed without the scale of the Single Market. And European strategic autonomy cannot be achieved without strong capabilities in the cutting-edge technologies that will shape the future.

Innovation means moving fast, and its key success factors are foresight, agility and speed. This is what the EU will need if it wants to keep up in the technological race of the 21st century.

DGAP
Advancing foreign policy. Since 1955.

Rauchstraße 17/18
10787 Berlin

Tel. +49 30 254231-0

info@dgap.org
www.dgap.org
@dgapev

The German Council on Foreign Relations (DGAP) is committed to fostering impactful foreign and security policy on a German and European level that promotes democracy, peace, and the rule of law. It is nonpartisan and nonprofit. The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the German Council on Foreign Relations (DGAP).

Publisher
Deutsche Gesellschaft für
Auswärtige Politik e.V.

ISSN 1866-9182

Editing Mark McQuay

Layout Mark McQuay

Design Concept WeDo

Autho Picturer