EUROPEAN
COMMISSION

Strasbourg, 15.2.2022
COM(2022) 61 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Roadmap on critical technologies for security and defence

1. Introduction

Remaining at the cutting edge of technological development is critical for ensuring Europe's prosperity, security and way of life. New technologies are transforming the security and defence sectors at a faster pace than ever before and blurring the dividing line between the civilian and military domain. Digital technologies in particular are affecting established balances of power within the global security landscape. It is thus essential to ensure that Europe's security and defence sectors remain technologically fit for purpose.

Many critical technologies for security and defence increasingly originate in the civilian domain and use critical components of a dual-use nature. To accelerate innovation across domains and foster technological sovereignty in the security and defence sectors, better exchange between civilian and defence research and innovation communities is needed. In light of its longstanding expertise in civilian technological development and its new defence cooperation instruments[1], the EU is well placed to take a lead role. However, this will require a more efficient use of resources and a readiness to explore the opportunities of dual use, while upholding the EU's fundamental values. It also means reducing strategic dependencies and vulnerabilities of the value and supply chains associated with these technologies.

The fragmentation of Europe's security and defence capabilities has led to economic inefficiencies, reduced operational capacity and increased strategic dependencies. The ongoing revolution in security and defence technologies and the new EU defence cooperation instruments give the EU an opportunity to avoid the mistakes of the past, to build on its existing capacities and preserve its economic prosperity and security. **The future European security and defence technological and innovation landscape should be developed under EU cooperative frameworks from the outset.**

In her 2021 State of the Union address[2], President von der Leyen recognised that while work on developing a European defence ecosystem had started, a European Defence Union was needed. The EU Strategic Compass for security and defence ('Strategic Compass'), to be adopted by Member States in March 2022, will set out a common strategic vision for the next decade and outline how the EU will enhance its capacity to act and respond to various crises and challenges; secure its interests and protect its citizens; invest and innovate to jointly develop the necessary capabilities and technologies; and deepen partnerships based on EU values and interests.

This roadmap on critical technologies for security and defence responds to a request from the European Council of 25-26 February 2021[3] to outline a path for boosting research, technology development and innovation (RTD&I) and reducing the EU's strategic dependencies in critical technologies and value chains for security and defence. The roadmap will be presented to the informal summit in Paris on 10-11 March 2022 and will feed into the Strategic Compass. The

[1] The European Defence Fund (EDF), the Coordinated Annual Review on Defence (CARD) and the Permanent Structured Cooperation on Defence (PESCO)

[2] 2021 State of the Union address of Commission President von der Leyen

[3] Statement of the members of the European Council of 26 February 2021

Roadmap proposes a way forward for the EU and Member States to jointly reach the above-mentioned goal, notably by:

- identifying technologies critical for EU security and defence, boosting them through European (RTD&I) programmes;
- ensuring that defence considerations are better taken into account in civilian European RTD&I programmes and industrial and trade policies, as appropriate, while possible civilian uses of technologies are also better considered in defence RTD&I programmes;
- promoting from the outset an EU-wide strategic and coordinated approach for critical technologies for security and defence, to make the best use of EU and Member States' RTD&I programmes, achieve synergies between civilian and defence RTD&I communities and mitigate strategic dependencies from external sources; and
- coordinating as much as possible with other like-minded partners, such as the United States and the North Atlantic Treaty Organization (NATO), under mutually beneficial conditions.

2. Critical technologies and strategic dependencies for security and defence

The update of the '2020 New Industrial Strategy: Building a stronger Single Market for Europe's recovery' ('updated industrial strategy')[4] of May 2021 confirms that technological leadership remains an essential driver of the EU's competitiveness and innovation, in particular for so-called 'critical technologies'[5]. It also underlines the importance of identifying and mitigating strategic dependencies in 'sensitive ecosystems', including those of 'proximity, social economy and civil security' and 'aerospace and defence', to ensure the EU's resilience.

The Commission action plan on synergies between civil, defence and space industries ('synergies action plan')[6] of February 2021 recognises the growing importance of disruptive and enabling technologies originating in the civilian domain for Europe's future security and defence and the need to promote cross-fertilisation and synergies between civilian and defence technologies. It sets out several key actions to encourage the exchange of information and cooperation between civilian and defence communities using EU RTD&I programmes and instruments as a starting point.

2.1. The specific features of the security and defence sectors

The EU defence industry has a diverse structure, with large multinationals and small to medium-sized players. Demand comes almost exclusively from national governments, which also control all acquisition of defence-related products and technologies, as well as their export. Different national requirements and national public spending and investment continue to fragment the EU defence market, at times risking to impede interoperability between Member States' national armed forces. The defence sector therefore does not follow the conventional rules and business models that govern more traditional markets, and has thus limited room to influence related

4 COM(2021) 350 final

5 The Commission in the context of its work on the Observatory of critical technologies is in the process of defining 'criticality' for the purposes of space, defence and related civil sectors (including security).

6 COM(2021) 70 final

investments and market choices. This makes it difficult for industry to undertake substantial self-funded defence RTD&I projects.

The EU security industry faces similar challenges, as markets are also predominantly national but even more fragmented. Its customers are diverse (e.g. police forces, internal security agencies, custom agencies, border authorities, private security services), activities take place at different levels (local, regional, national), and organisation varies from one Member State to another. **The Commission will present a study on the EU security market in 2022 providing further insights into this complex sector**. In addition, Commission services in the first half of 2022 will summarise the proposals for fostering the adoption of capability-driven approaches to be applied across security sectors. These proposals will strengthen the early and forward-looking identification of needs and solutions for security and law enforcement.

The space and cyber are strategic 'enablers' for the security and defence sectors. The space sector shares many of their specific features, with its small market volumes and limited leverage on the private market for components. The resilience of the space programmes and of the space value chains are critical for the EU security and defence objectives. Cyber also plays an increasingly important role across defence capabilities, requiring attention and investment. With fast-increasing cyber-attacks targeting both civilian and defence assets and networks, and the growing role of the civilian sector in cyber innovation and standardisation, closer links between cybersecurity and cyber defence are needed. The Commission contribution to European defence in the context of the Strategic Compass ('defence communication'), which is part of this defence package, outlines further measures for these two sectors.

2.2. Mapping critical technologies and strategic dependencies for security and defence

The updated industrial strategy provides a broad-based mapping and analysis of the EU's strategic dependencies and capacities, based on a first round of in-depth reviews of sensitive ecosystems[7]. While this work has provided a basis for policy action in support of better EU resilience, it also acknowledges that more work is needed to enhance further our understanding of the EU's strategic dependencies, and how they may develop and lead to further vulnerabilities. This work includes a second round of in-depth reviews of sensitive ecosystems and a monitoring system through the Observatory of critical technologies ('Observatory'), see Section 2.3.

Commission services have started working on in-depth reviews of defence and security technology areas, including in the area of cybersecurity, to support the updated industrial strategy and the development of the Observatory. Two preliminary case studies have been carried out so far on the defence technology areas of autonomous systems and semiconductors, which were considered to be representative samples, because of their cross-cutting relevance for military capabilities in different domains, see Box 1. The aim was to identify common patterns between these defence technology areas, in particular as regards the causes of dependencies and associated risks, as well as initial avenues to mitigate them.

[7] SWD(2021) 352 final

The case studies confirm that the defence sector broadly shares the same strategic dependencies and vulnerabilities as other sensitive ecosystems, notably as regards technology gaps, (critical) raw materials, skills, low RTD&I investment, and extra-territorial regulations by non-EU countries. They also indicate that the sector's vulnerabilities are generally exacerbated by the strategic and sensitive nature of its activities (e.g. higher standards of security of information and security of supply) and its comparatively marginal market size.

The case studies further show that some of the EU's global competitors take more offensive and defensive actions to promote critical technologies and address strategic dependencies than the EU has done up to now. For example, they tie national defence considerations more systematically into civil technological development, invest heavily in their indigenous RTD&I and industrial capacity, attract outside investors and at times deploy aggressive takeover strategies in third countries. They also protect their own industrial expertise and influence by leveraging interdependencies or using tight extra-territorial regulations to limit third country access to technologies.

While the EU has tools of its own to strengthen its industrial capacity in compliance with EU rules, it is hampered by the still largely fragmented EU defence market demand, its historically strict separation of civilian and defence RTD&I at EU level, and comparative underinvestment by Member States in the European Defence Technological and Industrial Base (EDTIB). Indeed, the collective spending on defence innovation by Member States (EUR 2.5 billion or 1.2% of defence expenditure) continues to lag behind a 15-year old EDA target of 2%.

While market forces have led to a situation where no single country can achieve full technological sovereignty in a technology domain, there is a global race for technological leadership and the associated economic and military advantages. This could exacerbate the EU's existing strategic dependencies and generate new ones, if it does not take action. A structured approach is needed for the EU to stay at the forefront of critical technologies and to identify and mitigate strategic dependencies in the domain of security and defence. This roadmap aims to provide such an approach, to be integrated in the EU Strategic Compass.

Box 1: Case studies – Autonomous systems and semiconductors for defence

The Commission's analytical work on autonomous systems for defence, with specific attention to artificial intelligence (AI) and machine learning, identified relevant critical technologies and four main areas where the EU is lagging behind, namely: skills, data, hardware, and testing. Possible measures to address them would build on the existing EU AI strategy[8] and associated policy initiatives, as well as Member States' national AI strategies. They include RTD&I activities (e.g. increased availability of data and AI training, link to the European Processor Initiative), infrastructure (e.g. cloud computing capacity for defence purposes, domestic testing facilities) and the protection of existing critical assets (e.g. foreign direct investment screening).

The analytical work on semiconductors for defence underlined the ubiquitous presence of semiconductors in defence equipment, and existing and future dependencies caused in

[8] COM(2018) 237 final

particular by the lack of indigenous EU capacities (foundries) for the most advanced nodes. The Commission has included mitigating measures in the proposal for a European Chips Act adopted on 8 February 2022[9], which aims to create a state-of-the-art European chip ecosystem to improve EU capabilities in this area, thereby also addressing defence needs.

2.3. The Observatory of critical technologies

Lack of foresight on the future importance of technologies is in part to blame for some of the EU's existing strategic dependencies on third countries (e.g. remotely piloted systems, semiconductors). The EU needs more structured foresight and strategic reflection on critical technologies for security and defence in order to identify priority areas to boost research and innovation, reduce existing strategic dependencies and avoid the emergence of new ones.

The Observatory of critical technologies, currently being set up by the Commission in line with the synergies action plan (action 4), will contribute to this reflection. Its working methods will take into account other similar initiatives[10] to avoid duplication. This will enable the fine-tuning of the list of critical technologies from the synergies action plan to reflect the evolving technology landscape and capability needs.

The Observatory will identify, monitor and assess critical technologies for the space, defence and related civil sectors, their potential application and related value and supply chains. It will also identify, monitor and analyse existing and predictable technology gaps, root causes of strategic dependencies and vulnerabilities.

It will be essential to agree with Member States on a meaningful level of detail to discuss these issues at EU level and on the need to share relevant data among Member States and with the Commission. A mechanism will be established within the Observatory, in the form of a dedicated expert group, for exchanging and discussing in a classified environment with Member States. This will include discussions on the emergence of new and disruptive technologies to avoid new dependencies for the security, defence and space industries. The High Representative and his services will be associated with this process.

The Commission, based on data of the Observatory, will present to Member States a classified report on critical technologies and risks associated with strategic dependencies affecting security, space and defence by end of 2022 and every two years thereafter. The Commission will prepare technology roadmaps based on these reports, which will include mitigating measures to boost RTD&I and reduce strategic dependencies affecting security and defence.

Once the Observatory's operations are well-established, the scope of its work could be extended to other industries, as indicated in the updated industrial strategy.

---

9 COM(2022) 45 final

10 For example, the Advanced Technologies for Industry (ATI) support and tools, the monitoring of critical technologies for space, the Overarching Strategic Research Agenda (OSRA), the Technology Building Blocks (TBB) and Key Strategic Activities (KSA) of the European Defence Agency (EDA).

Way forward:

- In 2022, the Commission will establish an expert group to facilitate exchanges with Member States on critical technologies, value and supply chains. It will be part of the Observatory of critical technologies for defence, space and related civil industries. The aim would be to:
  - conduct a regular consultation with Member State authorities to prepare the classified report;
  - ensure appropriate handling of sensitive and classified information that may be exchanged in the context of the Observatory of critical technologies, related reports and roadmaps.
- By mid-2022 the Commission will present a study on the EU security market, which will serve to better understand the specific features of the civil security market, to support the identification of critical technologies and strategic dependencies, and to underpin the new capability driven approach for security and other RTD&I activities.
- By mid-2022, Commission services will produce a paper summarising the proposals for fostering the adoption of capability-driven approaches to be applied across security sectors.

3. Boosting RTD&I on critical technologies for security and defence

The technology roadmaps that the Commission will prepare, based on the assessments from the Observatory, will underpin activities ranging from programming RTD&I on critical technologies to developing larger flagship initiatives that will contribute to strengthening the EU's competitiveness and resilience in the security and defence sectors. In order to deliver on these objectives, a more efficient use will need to be made of available financial resources through better coordination of existing EU and national RTD&I programmes and instruments.

3.1. Overcoming the separation between EU civilian and defence RTD&I

The Commission under its synergies action plan (action 2) committed to enhancing by 2022 internal coordination between EU programmes and instruments, see Box 2, in order to unlock the huge benefits arising from synergies between civilian and defence RTD&I for economic growth, the single market and the security of European citizens.

While the implementation of this objective can be taken further also in 2023 (e.g. through improved planning and synchronisation, guidance to managing authorities in Member States, etc.), some obstacles will be harder to tackle in the short- and medium term and may require involving other stakeholders. This is notably the case where legal provisions in the basic acts of EU programmes and instruments set practical constraints. For example, while dual use activities can be funded under the Connecting Europe Facility (CEF) and European Structural Investment Funds (ESIF), activities carried out under Horizon Europe[11] focus on civilian applications; there is no framework for direct support for such activities under RTD&I programmes and

[11] The term 'Horizon Europe' in this document refers to the specific programme implementing Horizon Europe and the European Institute of Innovation and Technology, activities carried out under these have an exclusive focus on civilian applications.

instruments. Similarly, the European Investment Bank's lending policy still has restrictions for the defence sector.

In order to facilitate exchanges between civilian and defence communities, especially in the area of critical technologies, the Commission will prepare in 2023 an approach for encouraging dual-use RTD&I at EU level to be fully implemented in the medium to long term across EU programmes and instruments. This work will also feed into the mid-term evaluation of relevant sectoral programmes, such as the funds under the Common Provisions Regulation, including funds for health emergency preparedness.

Box 2: EU programmes and instruments supporting RTD&I on critical technologies relevant to security and defence and their infrastructure deployment under the Multiannual Financial Programme (2021-2027)

- EDF dedicates EUR 8 billion to defence research and development. 4-8% of the EDF research and development budget will be allocated to disruptive technologies, i.e. up to EUR 100 million per year.
- Horizon Europe under pillar II 'Global Challenges and European Industrial Competitiveness' allocates EUR 1.6 billion to civilian security research and innovation under the cluster 'Civil security for society', whereas critical technologies are supported under clusters 'Digital, Industry and Space', 'Climate, Energy and Mobility' and 'Food, Bioeconomy, Natural Resources, Agriculture and Environment'. Complementary activities are funded under pillar I 'Excellent Science', the European Innovation Council (EIC) and European Institute of Innovation and Technology (EIT) in pillar III 'Innovative Europe', as well as European partnerships, which pool and mobilise resources to ensure the EU's technological leadership and open strategic autonomy in critical areas;
- the Digital Europe Programme (DEP) will foster deployment activities relevant to critical technologies in the priority areas of cybersecurity, AI and supercomputing;
- the Cybersecurity Industrial, Technology and Research Competence Centre and Network of Coordination Centres in 2022 will adopt a strategic agenda on cyber investments feeding into Horizon Europe and DEP. Synergies between civilian and defence technologies and dual use applications may be explored through links to EDF in line with applicable rules.
- ESIF (in particular for European Regional Development Fund and the European Social Fund+) can be used in support of EDTIB;
- other relevant EU programmes, funds and instruments include the Space Programme, CEF, InvestEU Programme, the Recovery and Resilience Facility (RRF), LIFE Programme, public-private partnerships, blending facilities.

3.2. Linking EU and national programmes and instruments supporting RTD&I on critical technologies for security and defence

While EU programmes and instruments provide significant funding to RTD&I activities for security and defence in the EU, the majority of funding for such activities still lies with Member States, and the fragmentation of security and defence markets remains a serious problem. As a consequence, achieving technological sovereignty in some critical technology areas and mitigating strategic dependencies in others will require EU-wide coordination.

Member States are invited to commit in the Strategic Compass to developing together with the Commission an EU-wide strategic coordinated approach for critical technologies relevant for security and defence from the outset, in full respect of the variety and complexity of the governance of EU and national programmes and instruments. This approach would also take into account other coordinating structures, such as the new EU Innovation Hub for Internal Security chaired by the Standing Committee on Operational Cooperation on Internal Security (COSI), and the new EU Innovation Hub for Defence to be set up by the EDA.

The approach would use the classified reports on critical technologies and the technology roadmaps prepared by the Commission as a starting point for discussions between Member States authorities and the Commission. The objective would be to identify on the basis of the technology roadmaps those areas requiring the most urgent action and to mobilise EU and Member States' programmes, instruments and policies to address them in a coordinated manner, in compliance with EU State aid rules. This would ensure that investments are focused on those areas that matter the most to the security of EU citizens. Priorities would be regularly updated to ensure that they remain relevant and that spending is efficient.

The Commission will work with Member States to identify the best mechanism for facilitating this coordination work (e.g. expert group of the Observatory).

3.3. Supporting security and defence innovation and entrepreneurship – Creating an EU Defence Innovation Scheme

The EU needs to make better use of the full potential of its innovation community in support of security and defence. This will require assisting non-traditional players and existing innovative start-ups and small and medium-sized enterprises (SMEs)) in the two sectors with overcoming their high technological, administrative, regulatory and market-entry hurdles, complying with the high security standards, and accessing financing. The defence market is often structured around a few large players supported by a set of specialised SMEs that have limited direct access to this market. As a result, it can be difficult for innovative defence SMEs to access finance, which can make them more likely to turn to or be targeted by foreign investors. The situation is similar for innovative security SMEs, which face similar challenges in approaching potential customers or accessing tailored finance[12].

The Commission has been supporting innovative security start-ups and SMEs under Horizon 2020, where the allocated funding and overall success rates under the societal challenge 7 'Civil security for society' have been above average for small innovators. While this support will continue under Horizon Europe, security start-ups and SMEs will still need additional tailored support to accelerate their road to the market. Exploring new instruments for dual-use innovation could boost their production capacity, competitiveness and sustainability.

[12] Challenges and opportunities for SMEs and start-ups in EU security R&I, CERIS SSRI virtual event, 30 April 2021

The Commission has started setting up similar activities under EDF to develop a toolbox on defence and dual-use innovation covering technology readiness levels (TRLs)[13] 1-9. Work is ongoing on the following tools covering defence, new technologies and dual use:

a) *Defence innovation through EDF* – Specific actions are being explored to better support projects on disruptive technologies, and innovative and future-oriented defence solutions, encouraging in particular the participation of innovative SMEs, innovative laboratories and research and technology organisations (RTOs). These actions may take different forms, for example business coaching (WP2021); technology challenges (WP2022), hackathons or prizes (WP2023 or later). They will also draw on relevant experience from the EIC and may link to the new CASSINI for defence.

b) *A defence investment blending facility under InvestEU* – The creation of such a facility would allow the Commission to guarantee investments made by financial intermediaries across the EU in innovative or strategic defence SMEs. This would ease problems linked with the limited access to finance for SMEs developing promising technologies for European defence, while providing trusted capital and avoiding hostile takeovers from third countries' entities. Enabling a better access to equity funding for innovative defence SMEs and mid-caps would support their growth and finally benefit to the innovativeness of the EDTIB. The Commission will also explore the need for further instruments in support of key market actors in the value chain.

c) *CASSINI for defence* – This initiative would be inspired by the existing CASSINI initiative to support the SMEs and start-ups in the space industry. It would provide them with services like: business development and networks (e.g. matchmaking, business accelerator), and prizes and competitions (including hackathons, mentoring, etc.), complementing the defence investment blending facility above.

d) *Innovation incubator* – The Commission will set up in 2022 an innovation incubator to support the development of new technologies and shape dual-use innovation in line with the synergies action plan (action 6), which could play an important role in bridging the gap between civilian- and defence-focused RTD&I programmes. Following a systematic analysis of results of early stage technology development, the incubator would flag projects and/or technologies that would exhibit potential security, space or defence applications to relevant services in the Commission and Member States for potential uptake. The Commission would assess how these flagged projects could be directed to further funding opportunities, as appropriate, such as the Transition funding scheme of the EIC or the EDF.

e) *Support to innovation networks* – Cross-border defence innovation networks could play the role of innovation brokers and encourage collaborative projects to incorporate innovative

[13] The EU has widely adopted the use of a Technology Readiness Level (TRL) scale under its RTD&I programmes and instruments since 2014. The scale distinguishes nine levels of technological maturity, ranging from fundamental research under TRL 1 to a final product ready for entry into the market under TRL 9. Since the application and thus dual use potential of a technology is typically revealed at TRLs 5-6, it can be considered that a technology is 'neutral' at TRLs 1-4.

solutions. Technology scouting would detect and identify new innovative solutions and technologies with potential benefits for defence applications. Research centres and technical test facilities would then test relevance of such technologies from the civil domain and exchange best practices. EDA would be a core partner of the Commission for the implementation of another part of action 6 under the synergies action plan.

The Commission will identify how to link the toolbox to instruments supporting innovation in the domains of security (e.g. Horizon Europe) or cybersecurity (e.g. the network of National Cybersecurity Coordination Centres in cooperation with European Digital Innovation Hubs).

The complementary strengths of the Commission and the EDA should be brought together under an **'EU Defence Innovation Scheme'.** Under the scheme, the Commission, based on its experience in implementing the EU budget in support of defence, civil and dual-use RTD&I, will play a central role in stimulating innovation for the EDTIB. Given its defence expertise, including in bringing together emerging and disruptive technologies and military capability requirements, EDA will further connect and support Member States efforts through its Defence Innovation Hub. By cooperating closely, the Commission and the EDA will in synergy accelerate security and defence innovation for the EU and its Member States.

3.4. Skills

Lack of skills and work-force shortages, especially of skilled employees with a background in science, technology, engineering and mathematics, are major challenges for the defence and security industry, which rely heavily on them like many other high-tech industries. As technologies and the threat landscape are rapidly evolving, it is important that the industry reaches out more to new and young researchers and entrepreneurs, including women, taking an inclusive and accessible approach of all talents, skills and available work force.

In November 2020, the Commission launched the Pact for Skills with a first wave of skills partnerships in the three key industrial ecosystems of microelectronics, automotive and the aerospace & defence industries. Pact members (industry, universities and training organisations, social partners) committed to ensuring a continuous and sustainable supply of skills in most needed areas by upskilling 200 000 employees and reskilling 300 000 people, with a public and private investment of EUR 1 billion by 2030.

Way forward:

- The Commission invites Member States to commit in the Strategic Compass to developing an EU-wide strategic coordinated approach for critical technologies relevant for security and defence from the outset.
- In 2023 the Commission will review existing EU instruments and propose further ways to encourage dual-use RTD&I at EU level.
- The Commission will support innovation and entrepreneurship on critical technologies for security and defence based on the following tools: a) dedicated EDF actions; b) a new defence investment blending facility under InvestEU; c) a new CASSINI for defence; d) a new innovation incubator on new technologies and dual-use innovation in 2022; and e) increased support to innovation networks.

- The Commission together with the EDA and its Defence Innovation Hub will set up an EU Defence Innovation Scheme to accelerate security and defence innovation for the EU and its Member States.

4. Reducing strategic dependencies in critical technologies and value chains for security and defence

The EU has several policy tools beyond its RTD&I programmes and instruments that can contribute to reducing its strategic dependencies in critical technologies and value chains in the security and defence sectors. These contribute to strengthening the EU's industrial capacity, competitiveness, technological sovereignty and resilience, but also to protecting current and future technological developments and capabilities.

The Commission, based on the work of the Observatory of critical technologies and under the updated industrial strategy, will systematically assess security and defence considerations, as appropriate, when implementing and reviewing existing, or designing new, EU industrial and trade instruments to ensure that they are fit for purpose.

– *Industrial alliances* – Industrial alliances engage a wide range of partners (e.g. public and private players, civil society) in joint action on key EU policy objectives in specific industries or value chains. They are based on the principles of openness, transparency, diversity and inclusiveness, and operate in full compliance with competition rules. Industrial alliances can include, where appropriate, specific work strands to reduce strategic dependencies for the security and defence sectors. This is being considered in the European Alliance for Industrial Data, Edge and Cloud and in the Industrial Alliance on Processors and Semiconductor Technologies.

– *Important Projects of Common European Interest (IPCEI)* – IPCEIs are initiated by Member States and subject to EU State aid rules. They are designed to bring together knowledge, expertise, financial resources and economic players throughout the EU with the aim of overcoming market or systemic failures and societal challenges that could not be addressed by private actors alone, in particular in the area of breakthrough innovation and key infrastructure. IPCEIs can take into account security and defence aspects. This could be the case in the upcoming second IPCEI on microelectronics announced in the Chips Act.

– *EU funding programmes* – The EU has always had an open research and innovation policy. It is guided by the principle of open strategic autonomy and aims at ensuring a level playing field and reciprocity. The EU's global approach on research and innovation encourages strategic partnerships with like-minded partners in line with the EU's international obligations (e.g. NATO, United States, Canada Japan, South Korea, etc.)[14].

  At the same time, it is necessary for Europe to make sure that its strategic interest are preserved. For 2021-2027 the Commission has clarified and harmonised the rules of participation for non-EU countries, and eligibility of entities, across EU programmes and

[14] It must be noted, however, that the defence-related research and development programmes of most of our partners are not open to EU companies.

instruments. Specific eligibility conditions for security sensitive activities have been established for certain programmes (Horizon Europe, DEP, EDF, Space Programme, CEF) and further refined in the relevant work programmes to protect the EU's essential security interests. The ongoing review of the Commission Financial Regulation will also provide more clarity on how to maintain the EU's open strategic autonomy approach, i.e. fully preserving the EU's essential security interests while respecting its international obligations.

- *Standards* – Under the synergies action plan the Commission is promoting the use of existing hybrid civil/defence standards and the development of new ones by the end of 2022 (action 5) and the consideration of defence in the Commission's standardisation policy and actions. While the EU strategy on standardisation[15] aims to ensure EU leadership in setting civilian standards, it will be highly relevant for the defence sector, since almost 80% of standards used in defence come from civilian sectors. The Commission, together will stakeholders (e.g. EDA), will explore the possibility of including defence requirements in the future standardisation efforts it supports to enhance their compatibility with defence needs.
- *Foreign Direct Investment screening* – The EU is one of the world's most open environments for foreign investment and one of the main destinations for foreign direct investment (FDI) in the world. However, specific investments can also undermine the EU's essential security interests. To prevent such risks, the EU has put in place a framework for FDI screening that has been operational since October 2020. The first annual report on FDI screening confirms the importance of effective FDI screening at Member State level and close cooperation at EU level, focusing on potential risks for security or public order. Member States are encouraged to set up national FDI screening mechanisms; 18 Member States already have one in place with another six in the pipeline. The Commission will evaluate the Regulation and present a report to the European Parliament and to the Council by October 2023.
- *Critical infrastructures* – The increasingly rapid emergence of new and disruptive technologies has had a significant impact on security of equipment, infrastructure, services, value and supply chains of strategic sectors, including those of security and defence. The EU and Member States need to factor in more comprehensively such vulnerabilities in relevant risk assessments and monitoring, and implementation of resilience-enhancing measures against security threats, e.g. of a hybrid or cyber nature. EU coordination will be needed to ensure that Member States maintain a future-proof level of resilience and consistent security standards at EU level in order to avoid vulnerabilities.
- *Smart and circular use of materials* –The new Circular Economy Action Plan of March 2020 is one of the main building blocks of the European Green Deal, Europe's new agenda for sustainable growth. Innovation and new business models based on increased resource efficiency, development of new materials, promotion of secondary raw materials and more sustainable public procurement, will not only preserve the environment but also secure access to materials for the industry. Additive manufacturing techniques, green procurement

[15] COM(2022) 31 final

and the recycling of materials, if well implemented, could also contribute to strengthening the competitiveness of the EU's security and defence industries, and the EU's resilience.

– *Data security* – The European strategy for data sets out measures to ensure that individuals and companies can stay in control of their data. This will be addressed in the Data Act that the Commission will adopt in early 2022.

  As part of the multi-country project on common data infrastructures and services (bringing together the European cloud federation and common European Data Spaces), the Commission is facilitating investments (e.g. DEP, CEF, Next Generation EU fund) in cloud-to-edge capacities that are secure, resilient, energy efficient and accessible in real time, and that provide quality of service throughout Europe. Ensuring technology transfer in cloud and edge technologies between the civil (notably security), defence and space industries would enhance technological sovereignty. The European Alliance for Industrial Data, Edge and Cloud provides a possible platform to foster such synergies.

– *Trade policy* –The complexity and vulnerability of global supply chains is an issue not just for the EU. Other countries depend on the EU ('reverse dependencies') and trade (or 'inter-dependence') may contribute to the stability of global value chains. The EU is also ready to act assertively and defend itself against unfair trading practices, such as the use of distortive foreign subsidies, while acting in accordance with its international commitments. The EU will continue to make the most of its toolbox of trade and competition instruments, while making sure that the EU tools are efficient and up to date. The Commission has therefore proposed new instruments, such as the Foreign Subsidies Regulation[16] that addresses distortions on the internal market caused by foreign subsidies.

Further relevant policy measures (e.g. introducing a potential value-added tax (VAT) waiver, facilitating the transfer of EU funded defence products) are listed in the defence communication.

Way forward:

- The Commission is exploring the possibility of adding defence work strands in initiatives such as the European Alliance for Industrial Data, Edge and Cloud and the Industrial Alliance on Processors and Semiconductor Technologies.
- The Commission together with Member States will identify and report in 2023 on the need for risk-assessing supply chains of critical infrastructure, in particular in the digital domain, to better protect the EU's security and defence interests.
- The Commission encourages all remaining Member States to set up a national FDI screening mechanism.

5. External dimension

Cooperating with like-minded partners around the world is essential for enhancing the EU's resilience and security of supply, while reducing strategic dependencies and increasing mutual benefits. The principle of reciprocity plays an important role in this context. The EU's traditional

[16] COM(2021) 223 final

partners in the areas of technology, security and defence include the member of the European Economic Area (in particular Norway), candidate countries, neighbourhood countries, and other third countries (e.g. United States, Canada, Japan, South Korea), as well as international organisations (e.g. NATO). Recent exchanges include in particular:

5.1. EU-U.S. Trade and Technology Council

The EU-U.S. Trade and Technology Council (TTC) had its first meeting on 29 September 2021. In the joint statement the EU and the US reaffirmed their commitment to 'focus on advancing respective supply chain resilience and security of supply in key sectors for the green and digital transition and for securing the protection of our citizens' and its aim to 'increase transparency of supply and demand; map respective existing sectoral capabilities; exchange information on policy measures and research and development priorities; and cooperate on strategies to promote supply chain resilience and diversification'. Ongoing work in working groups on secure supply chains (including on semiconductors under a specialised track), information communication technology security, export controls and investment screening are most relevant for the present roadmap. The recently launched EU-U.S dialogue on security and defence could also serve as a forum for discussions on these issues.

5.2. Partnership with NATO

At the 2021 Brussels Summit, NATO leaders set out an ambitious agenda on technologies, in particular Emerging and Disruptive Technology (EDTs).[17] This provided further guidance to the work carried out in accordance with NATO's implementation strategy on EDTs, endorsed by NATO defence ministers in February 2021.

The Commission and the High Representative will monitor the progress of relevant NATO initiatives in this area through regular contacts with NATO at working level with a view to possible mutually agreeable and beneficial interaction with relevant EU initiatives in full transparency towards Member States, while avoiding creating new or increasing existing technological or capability dependencies.

Way forward:

- The Commission and the High Representative will explore in the context of the EU-U.S. TTC and the recently launched EU-U.S. dialogue on security and defence how to advance supply chain resilience and secure the protection of our citizens.
- The Commission and the High Representative will explore with NATO, in the framework of the Joint Declarations on EU-NATO cooperation and in full transparency with Member States, how to promote a mutually agreeable and beneficial interactions between their respective relevant initiatives.

[17] This included the decision to launch the Defence Innovation Accelerator for the North Atlantic (DIANA) and a NATO Innovation Fund.

6. Conclusions

As the global geopolitical situation remains complex and the race for new technologies that are relevant for security and defence continues, the EU and its Member States must reinforce cooperation on technologies that are critical for Europe's long-term security and defence and efforts to reduce related strategic dependencies.

This roadmap proposes to work closely with Member States on identifying critical technologies and value chains for security and defence – as well as the root causes of associated strategic dependencies in the context of the Observatory of critical technologies – to underpin an EU-wide strategic coordinated approach for critical technologies relevant for security and defence that will make the most of EU and national RTD&I programmes and instruments.

To enhance the competitiveness and resilience of the security and defence sectors, the findings from the Observatory and related work under the updated industrial strategy will also contribute to ensuring that security and defence considerations are better taken into account within EU industrial and trade policies, as appropriate and in line with EU competition rules and the EU's international obligations.

The proposals contained in this roadmap aim to contribute to the RTD&I dimension of the upcoming EU Strategic Compass, through which Member States will set ambitious, long-term goals to substantially enhance Europe's security and defence.