EUROPEAN
COMMISSION

Strasbourg, 15.2.2022
COM(2022) 60 final

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

Commission contribution to European defence

1. Introduction

In today's world, the European Union faces increased global instability and geopolitical friction, as acknowledged by the first-ever comprehensive EU Threat Analysis, conducted in November 2020 in preparation of the upcoming EU Strategic Compass. Conflicts and crises in our neighbourhood and beyond have a direct impact on our own security, while our societies and economies are targeted by sophisticated hybrid threats, including cyber-attacks and disinformation campaigns which originate abroad. Meanwhile the climate crisis and biodiversity loss are creating challenges for global security in general and for civil-military operations in particular.

What is and has been occurring on and around our borders on land, air and at sea, as well in cyber space, along important maritime routes and in outer space, all underline the need for us to become better prepared, more capable and more resilient. Against the backdrop of an accelerated technological race between the United States and China, the European Union must further build and secure its technological edge. As geopolitical relations evolve and our environment is changing, the Union must evolve similarly, and intensify and accelerate its collective capacities to defend and secure its fundamental values and its citizens. **A quantum leap in European defence is an integral and indispensable part of securing the Union and its citizens in the years and decades to come.**

Current and past events serve as wake-up calls that Europeans need to work more closely together on defence to ensure their own security and become a stronger security provider for others, using the Union's uniquely broad toolbox. The EU is already engaged to address the multiple open and frozen conflicts in our Eastern and Southern neighbourhoods, as well as in different regions across Africa as our neighbouring continent. The recent **Russian military build-up along the eastern border of Ukraine, in Belarus, and in the Black Sea region,** together with Moscow's attempts to disrupt, divide, and redefine the security architecture in Europe, challenge the international rules-based order. It also reminds us that we need to deliver on a stronger European defence, in close partnership with the North Atlantic Treaty Organization (NATO). The abrupt end of the international military mission in **Afghanistan** in August 2021 taught us that Europe needs to be better prepared to deal with complex stabilisation tasks and sudden emergencies by itself. We have seen how instability can become a breeding ground for terrorism and uproot people, and how global and regional powers can use such situations to gain influence and access to resources. Adding to the complexity is the multiplier effect of climate change on the potential for conflicts within and between states.

At the same time, the EU needs to step up its own preparedness, capability and resilience to better protect its citizens. **Threats to the EU's security are increasingly not only of a military nature.** We are facing more damaging cyber-attacks targeting our critical entities, paralysing industrial plants, energy supply facilities, city administrations, and hospitals, while foreign information manipulation and interference also goes to the heart of our democracies. The state-sponsored hybrid attack by the Lukashenko regime, instrumentalising migrants for political purposes, is a clear example of the evolving nature of hybrid campaigns that aim to subvert, coerce and manipulate us below the threshold of armed aggression. The EU has responded to this

situation with humanitarian support, diplomatic outreach to third countries, support to our Member States and sanctions against those responsible. The COVID-19 pandemic meanwhile underlined the need for enhanced resilience as well, with the armed forces providing logistical, security and medical assistance to civilian authorities in the early stages in 2020. In this rapidly changing environment**, the European Union needs to further strengthen its preparedness, capabilities and resilience, notably by enhancing shock absorption mechanisms and building its toolbox across all relevant sectors**.

Member States are working to tackle all threats and challenges more robustly through the new EU **Strategic Compass for security and defence** ('Strategic Compass'), to be adopted by Member States in March 2022. It 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. With this communication, the European Commission is further contributing to this work.

The European Union needs to act now to advance its defence capabilities in the present context and also equip the EU to face the future battlefields, encompassing a new generation of state-of-the-art technologies capable of addressing threats deriving from cyber, hybrid, space collaborative and autonomous systems based on connectivity and Artificial Intelligence (AI). At the same time, the industrial ecosystem that defence forms together with the aerospace and the security sector constitutes a **high-tech industrial ecosystem** that is not only an essential driver for Europe's open strategic autonomy and technological sovereignty, but also a major contributor to growth and innovation. On top of contributing to the security of the European Union's citizen, the European defence sector can contribute to the sustainable **economic recovery** following the pandemic and the overall innovative nature of an ecosystem that has the potential of greatly contributing to the green transition and resulting in positive spill-overs for civilian use.

Achieving our goals is only possible by **developing, procuring, and operating military equipment together.** The EU has put in place new tools and instruments[1] to reverse the long standing fragmentations that hamper the efficiency of Europe's defence sector and diminish the ability of the EU and its Member States to build the next generation of defence capabilities that will be critical for Europe's future security and its ability to provide security in its neighbourhood and beyond.

In particular, the European Defence Fund (EDF)[2], with a budget close to EUR 8 billion for 2021-27, is already a game-changer for establishing a European defence ecosystem capable of delivering state of the art interoperable defence technologies and equipment that will enhance the Union's freedom of action and its technological sovereignty and competitiveness.

Against this challenging background, the European Commission will keep working closely with the High Representative and the Member States to:

[1] Including the European Defence Fund, the Permanent Structured Cooperation (PESCO) and the Coordinated Annual Review on Defence (CARD).
[2] PE/11/2021/INIT

- Ensure **effective and focused implementation** of the innovative instruments and initiatives that we have put in place, such as the EDF and the Action plan on Military Mobility, including through a number of additional measures put forward in this Communication;
- Support **closer defence cooperation between Member States and between industries**, underpinned by the necessary financial resources and enhanced collaborative spending in line with existing commitments, to enhance cost-effectiveness, strengthen interoperability, foster innovation and improve industrial competitiveness and resilience;
- Strengthen our ability **to respond in the face of acute crises**, including cyber-attacks and hybrid campaigns, **as well as longer-term challenges and geopolitical contestations in strategic domains**, based on a whole-of-government approach and reinforcing dual-use and civil - military synergies across a wide variety of Commission-led policies, tools and instruments;
- Maintain and enhance **close interaction with NATO**, in line with the commitments undertaken and the agreed principles guiding EU-NATO cooperation under the Joint Declarations, as well as with other key international partners such as the United Nations (UN) and like-minded bilateral partners including the United States of America, Norway[3] and Canada.

In this ever-evolving geopolitical and technological context, and in view of the upcoming informal Summit in Paris on 10 and 11 March 2022, this Communication outlines **concrete, new measures and initiatives in a number of critical areas** and identifies key success factors towards a more competitive and harmonised European defence market, including by:

- **Stepping up investments for defence research and capabilities developed in EU cooperative frameworks;**
- **Facilitating synergies between civilian and defence research and innovation and reducing strategic dependencies;**
- **Incentivising the joint procurement of defence capabilities developed in a collaborative way within the EU;**
- **Calling upon Member States to continue moving towards streamlined and more convergent export control practices, in particular for defence capabilities developed in an EU framework;**
- **Strengthening the security and defence dimension of space at EU level;**
- **Enhancing European resilience inter alia by stepping up cybersecurity and countering cyber and any other hybrid threats, enhancing military mobility and addressing climate change challenges for defence.**

Through these building blocks, and drawing on the synergies between internal and external policies including those fostered under the 2020 Security Union Strategy, the Commission will continue to actively contribute in the years to come to the process of building a **European**

[3] As a member of the European Economic Area.

Defence Union with targeted initiatives and projects, using the full spectrum of tools at its disposal to further counter the fast-changing multi-layered threats we face.

2. Stepping up investments for defence research and capabilities developed in EU cooperative frameworks

The EDF is an **ambitious, balanced and inclusive programme** that ensures Member States' strong involvement so that funded projects meet armed forces' operational needs, paving the way to production and procurement. Its **eligibility criteria** keep the market open while strengthening the competitiveness of the European defence industry and protecting the EU's security and strategic interests.

By the end of 2022, the European Commission will have invested EUR 1.9 billion in defence research and capability development projects answering Member States' capability needs. It will thus **kick-start key large-scale collaborative capability development projects** addressing critical shortfalls while also **stimulating defence innovation**, including in particular niche areas**.** It includes smaller projects and open calls that widen the cross-border participation of start-ups and Small and Medium-sized Enterprises (SMEs), with up to 8% of its 2021 budget devoted to funding disruptive technologies for defence and around 6% dedicated to open calls for SMEs. They represent 48% of the 1100 entities that have submitted proposals and 20% of the total funding demand[4] for EDF 2021 calls[5]. The Commission will continue to promote the participation of SMEs across the EU, including by encouraging the integration of the most innovative and competitive ones within supply chains.

The first calls for proposals published in **2021 already plan to allocate around EUR 700 million to projects addressing large-scale and complex defence platforms and systems** such as next generation fighter systems, ground vehicles fleet, multirole and modular offshore patrol vessels, and ballistic missile defence.

Also through its development precursor programme[6], **two major capability development projects of high strategic importance received a total grant of around EUR 140 million**. MALE RPAS supports the development of a medium-altitude and long-endurance drone. It contributes to building technological sovereignty in drones, a critical asset for Member States' armed forces. The European Secure Software-defined Radio (ESSOR) will boost interoperability by creating a European standardisation for defence secure communication technologies. Other meaningful funded projects focus, inter alia, on command and control, AI enabled decision-making, collaborative combat, cyber defence or space-based observation.

Developing defence capabilities is a long-term process, which requires coordinated and upfront planning. **Strategic orientation for the EDF is provided through the defence capability**

[4] Subcontractors included.
[5] Under the precursor programme, the European Defence Industrial Development Programme (EDIDP), in 2020, for which outcomes are available, SMEs represented 35% of the entities and benefited from 30% of the total funding of the 26 projects, before taking into account the participation of sub-contractors that are often SMEs.
[6] The European Defence Industrial Development Programme (EDIDP)

priorities commonly agreed by Member States within the framework of the Common Security and Defence Policy (CSDP), and in particular in the context of the Capability Development Plan (CDP) and in coherence with other EU defence related initiatives such as the Coordinated Annual Review on Defence (CARD) and the Permanent Structured Cooperation (PESCO).

In addition, to provide transparency and predictability especially in view of the planning of national defence budgets, the Commission has prepared **an indicative and flexible multiannual perspective** for the four years ahead, to be reviewed each year in light of developments. It ensures consistency of collaborative defence capability projects and coherence of work programmes along the duration of the EDF while also providing both transparency and predictability. In this context, the Commission and Member States will keep strengthening the multiannual annual perspective **taking into account key capabilities and strategic enablers identified as priorities by Member States following the adoption of the Strategic Compass**.

Thanks to its catalyst effect, the EDF will thus continue to pave the way for targeted defence investments in support of the European Defence Technological and Industrial Base (EDTIB) and matching priorities commonly agreed by Member states within the EU. To better support the development of large-scale defence capability projects, the possibility for multi-annual work programmes should be assessed in the context of the EDF's mid-term review. It is equally important to **ensure that other horizontal policies,** such as initiatives on sustainable finance, **remain consistent with the European Union efforts to facilitate the European defence industry's sufficient access to finance and investment**.

In order to further enhance both cooperation in the framework of the EDF and the integration of the internal defence market, the Commission will also continue to work with Member States to exploit the possibilities offered by the Directive 2009/43/EC[7] on the intra-EU transfer of defence related products with a view to facilitate transfers related to EU-funded collaborative projects. By advising on the rules and procedures under Directive 2009/43/EC, and working to build consensus amongst Member States, the Commission will aim at simplifying the transfer of defence-related products within the internal market, and notably in the framework of EU-funded collaborative projects, and facilitating exchanges of best practices.

Enhancing the coordination, focus and level of collaborative defence investments is critical to improve the overall efficiency of defence expenditures within the EU, while taking into account as well existing commitments such as those undertaken in the PESCO context to regularly increase defence budgets. The collective delivery of strategic defence capabilities can only be achieved through coordinated planning as well as EU and national public investments targeting common defence research and development priorities.

Against this background, the Commission will also **develop further incentives to stimulate Member States' collaborative investments in defence strategic capabilities, notably where they are developed and/or procured within European Union cooperative frameworks.** The

[7] Directive 2009/43/EC of the European Parliament and of the Council of 6 May 2009 simplifying terms and conditions of transfers of defence related products within the Community.

Commission will include a chapter with observations on developments, barriers and opportunities relative to **multinational defence capabilities projects in the Annual Single Market Report**, which is usually published in conjunction with the European Semester Autumn Package. In this context, the Commission could also consider how to scale up collective efforts to secure and coordinate the co-funding of Member States channeled through the EDF with a view to securing greater value for money.

Way forward

- With the EDF, the Commission will continue to actively encourage Member States to further define strategic defence capabilities priorities and enablers following the adoption of the Strategic Compass through the revised CDP and the CARD outcomes. It will contribute to align defence planning and collective spending to support their development.
- The Commission will develop further additional incentives to stimulate Member States' collaborative investments in strategic defence capabilities, notably those that are to be developed and/or jointly procured in European Union cooperative frameworks, and will report on the developments, barriers and opportunities related to multinational defence capability projects in the Annual Single Market report.
- In 2022, the Commission will continue to work with Member States to further facilitate the transfer of EU-funded defence products within the internal market, in particular by supporting the full exploitation of possibilities offered by the Directive 2009/43/EC.

3. Facilitating synergies between civilian and defence research and innovation and reducing strategic dependencies

The Commission outlines, in its Roadmap on critical technologies for security and defence that is adopted alongside the present Communication[8], a path for boosting research, technology development and innovation and reducing the EU's strategic dependencies in critical technologies and value chains for security and defence.

Building on the update of the '2020 New Industrial Strategy: Building a stronger Single Market for Europe's recovery'[9] and the Action Plan on synergies between civil, defence and space industries[10], it proposes a way forward for the EU and Member States to:

- identify technologies being critical for EU security and defence;
- promote from the outset an EU-wide strategic and coordinated approach for those critical technologies by leveraging research, technology development and innovation programmes;
- reduce strategic dependencies.

[8] COM (2022) 61 final
[9] COM (2021) 350 final
[10] COM (2021) 70 final

This requires greater awareness of the criticality of certain technologies, such as semiconductors, for the security and defence sectors, a better identification of related strategic dependencies, and possible mitigating measures, taking into account the diversity of sources and the prospect that operational use of the technology might be compromised or denied[11]. The Observatory of critical technologies[12] ('Observatory') will establish a dedicated mechanism to identify such assessments, based on inputs of Member States and the industry. The findings of the Observatory will be instrumental to boost EU research, technology development and innovation on those technologies, in an EU-wide coordinated approach. This work complements broader efforts to address security of supply of critical civilian goods, in fields such as health and energy[13].

The Commission will also prepare **an approach to encourage dual use for research and innovation at EU level,** and deploy a Defence Innovation Scheme to support innovation and entrepreneurship on critical technologies in close coordination with the Defence Innovation Hub to be established by the European Defence Agency (EDA).

Finally, in order to reduce strategic dependencies, the Commission will continue to systematically assess security and defence considerations when implementing and reviewing existing - or designing new - EU instruments.

4. Incentivising the joint procurement of capabilities developed in a collaborative way within the EU

Member States' **joint procurement of European defence capabilities** substantially **increases the inter-operability** of European national armed forces and **supports the competitiveness of the EDTIB**, notably through greater economies of scale.

However, Member States have yet to meet the long-standing European collaborative equipment procurement collective benchmark[14] – 35% of defence equipment spending, which they have confirmed within the PESCO framework[15]. According to the EDA, in 2020 Member States[16] have spent around EUR 37 billion in defence equipment procurement expenditure (i.e. procurement of new defence equipment). Of this amount about only 11% (around EUR 4.1 billion)[17], was spent on European Collaborative Defence Equipment Procurement Expenditure (i.e. procurement of new defence equipment in collaboration with other Member States). This means that the bulk of Member States' defence equipment procurement expenditure (around 89%) was made on a national basis and/or in cooperation with third countries.

---

[11] As regards semiconductors, see the accompanying Roadmap on critical technologies for security and defence, section 2.2, and the Commission Communication, A Chips Act for Europe, COM(2022) 45 final.
[12] In association with relevant Commission services and with the European Defence Agency.
[13] In line with Commission proposals COM (2021) 577 of 16.9.2021 on a framework of measures for ensuring the supply of crisis-relevant medical countermeasures in support of a public health emergency, COM(2021) 660 of 13.10.2021 on tacking rising energy prices, and COM (2021) 350 on updating the new industrial strategy.
[14] In November 2007, the EDA Ministerial Steering Board approved four collective benchmarks for investment including the 35 % of total equipment spending for European collaborative equipment procurement.
[15] EUR-Lex - 32021H1117(01) - EN - EUR-Lex (europa.eu)
[16] Except DK
[17] Based on data provided by eleven Member States

The year 2020 is not an exception and can even be considered as part of a trend that has worsened in recent years. Indeed, the percentage in European collaborative defence equipment procurement has been constantly decreasing since 2016, and the 2020 figure is the lowest since such data is being collected (2005).

Two EU instruments already pave the way to joint procurement. As a condition for financial support for development actions, **the EDF** Regulation requires that Member States intend to procure the final product or use the technology in a coordinated manner. **The Defence Public Procurement Directive** 2009/81/EC provides for a dedicated exclusion from the public procurement rules for cooperative projects based on Research and Development (R&D)[18]. This exclusion applies also to the phases of the life cycle after R&D if the procurement contracts are awarded in the framework of the same cooperative project. In 2019, the Commission published a Notice[19] providing guidance on various possibilities for cooperative procurement offered under the Directive. Further support to Member States will be available, in particular through the Expert Group on Defence and Security Procurement.

The Commission aims at further **incentivising Member States' joint procurement of European defence capabilities**, including in relation to operations and maintenance. However, there are a number of practical financial and fiscal hurdles that need to be tackled to this end.

The Commission will explore enabling a possible **Value Added Tax (VAT) waiver to support the joint procurement and joint ownership of defence capabilities that are developed in a collaborative way within the EU**. These capabilities will be available for use by Member States for missions and operations in the framework of CSDP[20] or within the context of UN, NATO and national activities. Such a measure could especially benefit capabilities developed within cooperative EU frameworks (EDF and/or PESCO and/or within the EDA). The establishment of a legal framework inspired by the European Research Infrastructure Consortium[21] that would benefit from a VAT waiver on equipment that Member States consortia would buy and own, could be considered in this context.

Similarly, based on the lessons learned from the interim evaluation of the EDF, the Commission will consider reinforcing the current **system of EDF bonuses, in order to provide a financial incentive** on the condition that **Member States commit to jointly acquire and/or own the defence capabilities under development[22]**. This would provide stronger incentives to ensure that the collaboration continues beyond the R&D phases, to acquisitions, as well as operations and maintenance.

Furthermore, building on the work of the Expert Group on the Financial Toolbox, **new financing solutions** could lead to greater use by Member States of already existing joint procurement

[18] Article 13 of Directive 2009/81/EC
[19] 2019/C 157/01
[20] In line with the multinational forces foreseen by Art 42.3 of the Treaty on European Union
[21] The European Research Infrastructure Consortium (ERIC) is a specific legal form that facilitates the establishment and operation of Research Infrastructures with European interest.
[22] Beyond the eligibility requirement specified under Article 21(3) (a) of EDF Regulation that requires an intention to procure the final product or use the technology in a coordinated manner.

entities such as the EDA or the Organisation for Joint Armament Cooperation (OCCAR - *Organisation Conjointe de Coopération en matière d'Armement*). In particular, the Commission will assess whether the EDF regulation provisions, such as those related to pre-commercial procurement[23] may provide for financial support to contracting authorities and joint procurement entities to further coordinate their procurement procedures, including by covering administrative/transaction costs related to joint procurement of defence research and development services.

Way forward

- By early 2023, the Commission will make a proposal that would enable a **VAT waiver** to support the joint procurement and ownership of defence capabilities developed in a collaborative way within the EU, while ensuring compliance with World Trade Organisation rules.
- By mid-2023, the Commission will build on the work of the Expert Group of the Financial Toolbox with a view to propose **new financing solutions** to facilitate Member States' joint procurement of EU strategic defence capabilities relying on already available expertise.
- Following the interim evaluation of the EDF[24], the Commission will explore a possible amendment to article 13 of Regulation 2021/697 establishing the European Defence Fund to reinforce **the EDF bonus system when Member States commit to jointly acquire and/or own the defence capabilities under development.**

5. Calling upon Member States to continue moving towards streamlined and more convergent export control practices

While Member States are in charge of issuing export licences for military equipment, they assess their decisions on the basis of the Council Common Position[25] that defines common criteria for controlling the export of military technology and equipment. It also sets up denial notification and consultation mechanisms with a view to increase convergence in the application of their export policies for defence-related products.

However, as joint defence capabilities development will progressively become the norm in the EU rather than the exception, **Member States will benefit from increased sharing of best practices and gradually leading to a more convergent approach to arms exports controls**. Building upon work that has already been achieved, and acknowledging that exports are a key success factor for the business model of the European defence industry, the Commission is supportive of Member States moving towards gradual enhanced streamlining and further

[23] Article 17 of the EDF regulation

[24] The interim evaluation is to be carried out no later than four years (2025) after the start of the implementation period of the Fund according to article 29 of the Regulation establishing the EDF.

[25] Common Position 2008/944/CFSP.

convergence of arms export control practices, especially for those defence capabilities that they develop together, in particular under the EDF.

In this context, **the Commission welcomes the reflection that has been initiated in the Council[26]** on exportation of capabilities that have been developed in an EU framework and encourages Member States to pursue these discussions to facilitate exports control procedures for such products. This process could also draw on the experience of bilateral and multilateral accords between Member States for jointly developed capabilities.

In order not to hamper cooperation, this work should facilitate the definition of clear and easy-to-implement procedures. Efficient export control measures should be defined to provide EDF-funded products with adequate and competitive access to international markets while preserving Member States' sovereign decisions, in full respect of their relevant legal obligations and taking into account their national security interests. To preserve the attractiveness of joint defence capability projects**, the Commission invites Member States to seek an approach according to which, in principle, they would respectively not restrain each other from exporting to a third country any military equipment and technology developed in cooperation**. This could apply to intended exports of equipment or technology incorporating components from another Member State exceeding a certain *de minimis* threshold.

Way forward

- The Commission invites Member States to explore ways towards the streamlining and gradual further convergence of their arms export control practices, especially for those defence capabilities that are jointly developed, in particular in an EU framework, thus ensuring EDF-funded products will profit from adequate and competitive access to international markets without prejudice to Member States' sovereign decisions.

6. Strengthening the defence dimension of space at EU level

Space is a strategic area for **EU's freedom of action and security**. At the same time, it is an increasingly congested and contested area, marked by a growing power competition.

There is an urgent need to tackle these challenges. A new EU space strategy for security and defence, currently under consideration by Member States in the context of the Strategic Compass, should help building a common understanding of space-related risks and threats, develop appropriate responses to react better and faster to crises, strengthen our resilience and make full use of the benefits and opportunities linked to the space domain. Without prejudice to the content of the future joint strategy, the following actions will be considered:

[26] Within the Conventional Arms exports subgroup (COARM) of the Non-Proliferation and Arms Exports Working Party

First, EU space assets[27] should be further protected to enhance resilience of the EU in and from space.

In the Joint Communication on **Space Traffic Management (STM)**[28], the Commission and the High Representative provide concrete orientations on how to increase the protection of EU space assets and promote a more sustainable use of space. In particular, the Commission will reinforce its **space surveillance assets** through enhanced services in **Space Surveillance and Tracking (SST)** and the development of related technologies, such as automatic collision avoidance or artificial intelligence.

The Commission will also further support the development of projects related to **Space Situational Awareness (SSA) and early warning capabilities for defence**. Such projects will contribute to advanced space command and control (SC2) capabilities, enhanced SSA sensors, and early warning system against ballistic missile threats and novel hypersonic threats[29].

Second, the Commission will enhance the security and defence dimension in existing and upcoming EU space infrastructures, in cooperation with the High Representative**.**

The **Galileo public regulated service (PRS)**[30] offers a navigation service restricted to government-authorised users for sensitive applications. These requires a high level of service continuity, using strong, encrypted signals notably in the area of security and defence. The PRS is designed to offer unlimited and uninterrupted service worldwide. It is a clear demonstration that a common infrastructure under civilian control can meet defence and security needs.

The proposal for a regulation establishing the **Union Secure Connectivity Programme** for 2022-2027[31], which is being adopted alongside the present Communication as part of the space package, will enhance the resilience of the EU in connectivity through secure governmental communication. It will include defence requirements in terms of resilience from the outset and the Low Earth Orbit (LEO) constellation will provide an opportunity to take on-board pay-loads contributing to other EU space programme components. The system will build upon GOVSATCOM and synergies with the European Defence Fund.

The evolution of Copernicus should also take into account defence requirements to the extent possible, with a special attention given to the required levels of security and performance, and underpinned by the right governance based on trust.

To support the development of the defence dimension of existing and upcoming EU space infrastructures, the Commission will support the development of **space defence capabilities**

---

[27] The EU Space Programme has four components: Galileo/EGNOS for positioning, navigation and timing, Copernicus for Earth observation, GOVSATCOM for secure governmental satellite communications, and SSA for space situational awareness.

[28] JOIN (2022) 4 final

[29] Those projects are supported by the EDF and its precursor programmes.

[30] Decision No 1104/2011/EU of the European Parliament and of the Council of 25 October 2011 on the rules for access to the public regulated service provided by the global navigation satellite system established under the Galileo programme, OJ L 287, 4.11.2011.

[31] COM (2022) 57 final

through EDF. To date, about EUR 130 million have been allocated to fund space-related actions under the EDF and its precursor programmes.

As the Commission supports the development of collaborative platforms for future defence challenges, it also seeks to improve their performance by making the best use of existing and future European space assets. For example, the **Galileo for EU Defence** (GEODE) project is co-funded with EUR 44 million[32] and aims at developing European standardised military navigation receivers that are compatible with the Galileo PRS. More than EUR 22 million will also be invested to enhance sensors and Command and Control (C2) for an EU military space surveillance awareness and develop a space-based early warning capability.

Under the 2021 EDF work programme, the EDF will be dedicating EUR 50 million to both **space and ground-based navigation warfare (NAVWAR)** surveillance and European **technologies for resilient satellite communications against jamming**.

Third, the Commission will work to reduce related EU strategic dependencies on critical technologies, e.g. in the field of chips, quantum and AI. To achieve this, the Commission will maximise synergies with space-related initiatives implemented under existing Commission-led instruments (including EDF, Horizon Europe[33], Space Programme, European Innovation Council, and InvestEU) and will take advantage of the Observatory of critical technologies. The Commission will also strengthen the **resilience of related European supply chains** to ensure the integrity, the security and the operations of space infrastructures.

Fourth, the Commission, in cooperation with the High Representative, in line with their respective mandates, will implement the enlargement of the current Galileo threat response mechanism[34] to the systems and services under the other components of the EU Space Programme. This will further enhance the security governance of EU space infrastructures to better reply to threats and will promote adequate governance to be put in place by relevant actors**.** They will also improve situational awareness at EU level through better use of space data, in close cooperation with Member States and systematic cooperation between relevant agencies/bodies operating EU infrastructures.

The Commission and the High Representative will also contribute to Member States' efforts to further increase mutual assistance and crisis response mechanisms, including through exercises and by boosting readiness against threats, fostering interoperability and supporting a common strategic culture.

[32] Under the European Defence Industrial Development Programme (EDIDP)

[33] 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 them have an exclusive focus on civil applications.

[34] As provided in the EU Space Programme Regulation 2021/696 and by Council Decision (CFSP) 2021/698 of 30 April 2021 on the security of systems and services deployed, operated and used under the Union Space Programme which may affect the security of the Union.

Way forward

- Following the adoption of the Strategic Compass, the Commission and the High Representative will propose a Joint EU Space strategy for security and defence.
- By the end of 2022, the Commission will explore how to further enhance the **protection of EU space assets**, notably through additional SST services, improved performance of EU SST and by making full use of the potential of the EU industry.
- As of 2022, the Commission will promote a **'dual use by design'** approach for EU space infrastructures, with a view to offering new resilient services that address governmental needs. In this context, the Commission encourages the co legislators to swiftly adopt the proposal for a regulation establishing the Union Secure Connectivity Programme for 2022-2027.
- The Commission will intensify work towards reducing strategic technological dependencies and enhancing the resilience of space infrastructure related supply chains, notably through EU funding instruments as well as the Observatory of critical technologies.
- The Commission will set-up adequate governance for EU space infrastructures, in close cooperation with Member States, building on the model of the Galileo PRS. It will assess the feasibility to develop and deploy a more resilient and secured Copernicus service for governmental purposes,[35] taking into account defence requirements to the extent possible.
- By the end of 2022, the Commission and the High Representative will explore the possibility of activation of solidarity, mutual assistance and crisis response mechanisms in case of attacks originating from space or threats to space-based assets.

7. Enhancing European resilience

Europe needs to enhance its resilience to prevent, protect and withstand future shocks. Due to intrinsic links with national security and defence policies, responsibility for addressing these threats lies primarily with Member States. In the meantime, some vulnerabilities are common to all Member States, and some threats extend across borders, such as the targeting of cross-border networks or infrastructures as well as climate change.

The EU approach aims at integrating the external and internal dimension in a seamless flow. It brings national and EU-wide civilian and military considerations together to promote concrete solutions, while facilitating increased resilience and continued operational efficiency.

7.1. Countering hybrid threats

[35] Copernicus PRS-like service

In 2020, the **EU Security Union Strategy**[36] outlined hybrid threats as one of the priority areas to be addressed in order to enhance EU´s security. The Strategy sets out the basis for a renewed approach to these ever-evolving threats covering the full spectrum of action – from early detection, analysis, awareness, building resilience and prevention to crisis response and consequence management.

The **mapping of measures**[37] **related to enhancing resilience and countering hybrid threats includes more than two hundred tools and measures at EU level,** of which the vast majority of them are led or supported by the Commission. The Commission proposals in different areas, including the Digital Services Act[38], the proposal for a Critical Entities resilience directive[39] and the revised Union Civil Protection Mechanism[40], will further contribute to this increasing number of available EU tools to counter hybrid threats.

Resilience is one of the main pillars for countering hybrid threats. A joint staff working document of January 2022[41] identified 53 **resilience baselines**[42] elements at EU level. This identification, announced in the Security Union Strategy, has been a crucial first step to track and objectively measure progress in this area.

In this context, Commission services, the European External Action Service (EEAS) and the General Secretariat of the Council, will conduct the EU Integrated Resolve PACE exercise in November 2022, inter alia, to address hybrid threats, including their cyber dimension. This exercise will be conducted under the overall responsibility of the High Representative, with the participation of Member States and EU Agencies, and in a parallel and coordinated (PACE) format with NATO.

The Commission has also **adapted to the rapidly changing nature of threats**. Following the crisis at the EU border with Belarus, it proposed measures to tackle the **instrumentalisation of migration**, including blacklisting transport operators involved in smuggling or trafficking of people into the EU[43].

The COVID-19 pandemic has revealed the need to enhance coordinated EU-level action to respond to health emergencies. At a time, where Chemical, Biological, Radiological and Nuclear threats could put at risk public health, the European Health Emergency Preparedness and Response Authority (HERA) is a central element for strengthening EU preparedness and response to serious cross-border health threats, by enabling rapid availability, access and distribution of needed countermeasures. Drawing on the lessons from the early stages of the pandemic, work will continue to enhance military assistance to civilian authorities in this regard.

---

[36] COM (2020) 605
[37] SWD (2020) 152 final
[38] COM (2020) 825 final
[39] COM (2020) 829 final
[40] Regulation (EU) 2021/836 of the European Parliament and of the Council of 20 May 2021
[41] SWD (2022) 21 final
[42] Benchmarks, covering situations where this is a point of departure as well as an envisaged target or advice on minimum level requirements
[43] COM (2021) 753 final

Way forward

- By 2023, the Commission, in cooperation with the High Representative and the Member States, will assess the sectoral resilience baselines to identify **gaps and needs** as well as steps to address them.
- Following the adoption of the Strategic Compass, the Commission will contribute to the future EU hybrid toolbox by ensuring that the Member States have a full overview of existing internal instruments and measures to counter hybrid threats affecting the EU and its Member States. This will take into account the measures included in the 2020 mapping on countering hybrid threats and recent Commission's and High Representative's proposals in areas such as critical infrastructure and disinformation.
- Following the adoption of the Strategic Compass, the Commission will consider identifying experts in relevant policy areas, who could be deployed as part of Hybrid Rapid Response Team upon request, in synergy with the proposed JCU rapid response teams.
- In parallel Commission services and the EEAS will jointly review the EU Playbook on countering hybrid threats.
- By the end of 2022, the Commission, in cooperation with the High Representative, will define a comprehensive vision regarding its rapid alert mechanisms and in particular the possibility to create a better situational awareness picture, in coordination and complementarity with other EU existing mechanisms. This will strengthen the Union's capability for monitoring and early detection, prevention and preparedness, including resilience, and response to hybrid threats.
- Drawing on its expertise and instruments, the Commission will contribute to the EU effort to build resilience in partner countries.

7.2. Enhancing cybersecurity and cyber-defence

Countering cybersecurity threats is one of the most complex security and defence challenges today, especially considering their growing number and impact, and while state actors have developed specific sophisticated capabilities.

The EU needs to protect critical network and information systems and to play a leading role in guaranteeing the security, stability and resilience as well as freedom of the global internet. We need to boost cybersecurity and cyber defence in Europe by strengthening our cooperation, by investing more effectively into advanced capabilities, and by setting appropriate rules that will allow for a better linkage of all the dimensions of cyber. These efforts should focus on **protecting** citizens, businesses and EU interests, **detecting and deterring** malicious cyber activities and **defending** ourselves against cyber-attacks, thereby contributing to international security and stability and consolidating the EU's cyber deterrence potential.

The Commission and the High Representative have already set out ambitious actions contributing to these goals in the EU Cybersecurity Strategy of December 2020[44]. A number of important instruments are in place to increase EU resilience, notably the **Directive on measures for a high common level of security of network and information systems across the Union** (NIS)[45], the **Cybersecurity Act**[46], the **Directive on attacks against information systems**[47]**,** and the implementation of the **EU toolbox on 5G Cybersecurity**[48]**, Recommendation on a 'Blueprint' for a coordinated response to large-scale cybersecurity incidents and crises**[49] **and the EU cyber defence policy framework [2018 updates]**[50]. The Commission has also adopted a delegated act[51] under the Radio Equipment Directive[52] laying down legal requirements for cybersecurity safeguards, which manufacturers will have to take into account in the design and production of radio equipment. Finally, it released a recommendation for a **Joint Cyber Unit (JCU)**[53] and presented a proposal to **revise the NIS Directive** in December 2020[54], which is now under consideration by the co-legislators. In line with this level of ambition, the Commission will shortly present proposals to enhance the cybersecurity and information security of the EU institutions, bodies and agencies.

The 2021-25 multiannual work programme of the Digital Europe and of the Connecting Europe Facility (CEF - Digital sector) will support the deployment of a secure quantum communication infrastructure (Euro QCI). The CEF will also support other critical communication infrastructure, including certain backbones between Member States and with third countries, with the highest security standards.

To complement those instruments and further reduce the attack surface and exposure to risk, the security and standardisation of products and services related to information and communication technology (ICT) should be strengthened. This applies in particular to the security of critical hardware and software components. The Commission is therefore preparing new proposals laying down horizontal security requirements, that will form the centrepiece of the **Cyber Resilience Act** announced in the State of the Union address[55]. A defence dimension could be considered in this context, in particular as regards the potential development of common or hybrid cybersecurity standards.

---

[44] JOIN (2020) 18 final
[45] Directive (EU) 2016/1148 on security of Network and Information Systems (NIS)
[46] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013
[47] Directive 2013/40/EU (12/08/2013)
[48] COM (2020) 50 final
[49] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises, C/2017/6100
[50] 14413/18 (19/11/2018)
[51] C (2021) 7672
[52] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment
[53] C (2021) 4520 final
[54] COM(2020) 823 final
[55] State of the Union address 2021 - Strengthening the soul of our Union – 15 September 2021

To further enhance the technological capabilities of the EU and its cyber defence actors (mainly Member States' defence forces), more cooperation between relevant actors will be sought in the planning of civilian and defence investments for the development of relevant technologies as well as their use. The **Cybersecurity Industrial, Technology and Research Competence Centre and Network of Coordination Centres** (CCCN)[56] will adopt in 2022 its Strategic agenda on cyber investments. The agenda could cover possible synergies between civil and defence technologies and potential dual-use applications, thus seeking synergies with other EU programmes, including Horizon Europe, the Digital Europe programme, and the EDF, in a coordinated manner and while respecting relevant governance rules.

The Commission has already dedicated EUR 38.6 million[57] to six cyber defence projects. Among others, this budget is supporting the development of a European cyber situational awareness platform and a project on technologies for secure and resilient communication. The EDF will continue to support the development of cyber capabilities for defence. In 2021, two specific calls were launched under the EDF for a EUR 33.5 million financial envelope. While all defence capability projects entail a cyber-dimension, cyber defence will remain a priority for the EDF in the upcoming years.

To better prepare for potential large-scale incidents and crises in the Union, enhanced coordination is essential to ensure situational awareness, rapidly identify potential response needs and resources and to align effective communication amongst relevant actors at Member States' and EU level, in order to mitigate potential impacts in the Union.

To step up the **detection of malicious cyber activities and enhance situational awareness**, the Commission is working with Member States towards the establishment of **cross-border platforms to share cybersecurity threat intelligence (EU SOCs)** while also reinforcing capacities of Security Operation Centres (SOCs) at national level across the EU.The objective of those cross-border platforms ('EU SOCs') is to enable the exchange of data on cybersecurity threats from various sources, as well as tools and capabilities, on a large-scale basis, in a trusted environment. They will be equipped with next-generation, ultra-secure tools and infrastructures. This should allow to improve collective detection capacities and timely warnings to authorities and relevant entities. These actions will benefit from financial support from DEP, notably through a joint procurement to develop and operate EU SOCs, including advanced tools and infrastructures, as well as a call for grants to support SOCs capacities in the Member States.As a next step, promoting civil - military cooperation at national level in this area could be also considered, together with Member States.

The degree of cybersecurity cooperation between Member States when it comes to incident response should be increased including through possible cooperation among **civilian and defence response teams**. The Joint Cyber Unit aims at bringing together all relevant cybersecurity communities (i.e. diplomatic, civilian, law enforcement and defence) to ensure an EU coordinated response to large-scale cyber incidents and crises, as well as to

[56] PE/28/2021/INIT
[57] Under the EDIDP

offer assistance in recovering from these attacks. Therefore, the military could structurally cooperate and coordinate with other cybersecurity communities through the JCU.

Developing cyber skills through joint training and exercise is also key for effective resilience to cyberattacks, improving cyber capabilities, developing a shared understanding, and building a common response capacity. If Member States so decide, they could consider enhanced civilian military cooperation in cyber training and joint exercises, building on the European Security and Defence College and EDA's cyber education, training and exercises programmes.

Way forward

- By the third quarter of 2022, the Commission will propose the **Cyber Resilience Act** which will aim to increase the cybersecurity of products and associated services in the internal market.
- To set up the new 'EU SOCs' platforms for sharing of cyber threat intelligence and tools, by the second quarter of 2022, the Commission will publish a Call for expression of interest to select hosting entities for EU SOCs accompanied by dedicated Roadmap. This should pave the way for building an EU strategic capability for detecting and sharing information about cyber threats.
- The Commission will work with Member States on stepping up preparedness for large scale cyber-incidents through enhanced coordination, including identifying potential needs and resources to manage response.
- In 2022, a Strategic agenda for the Cybersecurity Competence Centre will be proposed, including on dual use technology and civil-military synergies to be enshrined in a coordinated manner with relevant actors.
- The Commission, together with the High Representative, will continue supporting Member States in setting up the JCU, in particular its mutual assistance mechanism, and will encourage civilian military cooperation to facilitate information exchanges and coordination between defence experts and other communities (i.e. civilian, law enforcement and diplomacy).
- The Commission will request the European Standardisation Organisations to develop harmonised standards in support of the recently adopted delegated act of the Radio Equipment Directive as regards cybersecurity and privacy.
- The Commission will work together with the High Representative to further develop the EU cyber defence policy to be presented to Member States by the end of 2022.
- The Commission invites Member States to consider joint cyber defence trainings and exercises, in cooperation with existing civilian and defence training and exercises frameworks.

7.3. Enhancing military mobility

Through thet implementation of the Action Plan on Military Mobility, the EU is already taking significant steps to enhance the mobility of military personnel, materiel and equipment within and beyond the EU, thus enhancing our ability to respond swiftly to a crisis or in view of routine activities like exercises. Military mobility is also a flagship project within EU-NATO cooperation.

With a **2021- 2027 EU budget of EUR 1.69 billion** to support dual-use transport infrastructure, military mobility is a key component of the new Connecting Europe Facility (CEF)[58]. The 2021-2023 Work Programme entails a yearly dedicated budget of EUR 330 million, and the first calls for proposals were launched in September 2021.

Military mobility is also a topic of the 2021 EDF Work Programme. The development of a digital system for secure and quick exchange of information related to military mobility is one of the two topics under the call for proposals on soldier and logistic systems, with a EUR 50 million indicative budget for the whole call.

On 14 December 2021, the Commission proposed revising the trans-European transport network (TEN-T) Regulation. Among other measures, the proposal aims to strengthen standards for civilian and military mobility and to expand the TEN-T maps to include new routes important for military mobility.

The Commission will continue its efforts to contribute to military mobility within and beyond the EU, including by considering it in relevant legislative proposals and initiatives, in particular in the area of transport and cross-border procedures.

Way forward

- By the end of 2022, the Commission, together with the High Representative, will propose an update of the joint Action Plan on Military Mobility, which may cover identifiable needs in relation to digitalisation in transport, cyber resilience of transport infrastructure and artificial intelligence.

7.4. Addressing climate change challenges for defence

Climate change and biodiversity loss poses new threats to security. While maintaining operational effectiveness remains a priority, the defence sector needs to meet the challenge of adapting to the security effects of climate change including operation under more extreme climatic conditions, as well as contribute to mitigation under the EU's climate change policies, in particular the European Green deal. Improving energy efficiency, increasing the use of renewable energy where possible, and reducing emissions in this sector, should become an

[58] Regulation (EU) 2021/1153 of the European Parliament and of the Council of 7 July 2021 establishing the Connecting Europe Facility and repealing Regulations (EU) No 1316/2013 and (EU) No 283/2014

integral part of our collective efforts towards climate neutrality by 2050 as well as the protection of biodiversity and a strengthened circular economy.

Circular systems can have major benefits for defence industries and procurement, increasing resource efficiency, increasing open strategic autonomy for certain critical materials, and prolonging and optimising the utility of defence equipment[59]. Opportunities to improve design for disassembly, component harvesting, repair, refurbishment and remanufacturing of defence equipment will be identified and supported. This also goes for opportunities to upgrade defence equipment so that it can continue to operate under increasingly harsh environmental conditions in operational theatres.

In this context, the Commission is committed to the implementation of the 2020 Joint EU Climate Change and Defence Roadmap[60] on which Commission services will present a first annual progress report together with the EEAS and the EDA in the first half of 2022. The EDF[61] 2021 Work Programme already identifies topics related to energy management and energy efficiency. EUR 133 million have been dedicated to a specific call to support research and development of defence technologies and products addressing these topics. As similar work is being stepped up within NATO, the UN and by the United States and other partners, the EU will intensify its staff-to-staff dialogues on the climate-security-defence nexus.

Way forward

- In the first half of 2022, Commission services, EEAS and EDA will present the first progress report on the implementation of the Climate Change and Defence Roadmap.
- During 2022, the Commission will assess climate/defence related initiatives implemented under existing Commission-led instruments (including EDF, Horizon Europe, Horizon 2020, CEF, and LIFE) in order to enhance potential synergies.
- By the end of 2022, the Commission will establish a policy framework, drawing on climate/defence aspects of Commission-led instruments to contribute to reduced energy demand and increasing energy resilience of critical technologies used by civilian security actors and armed forces, and develop concrete climate resilient solutions in this context.
- During 2022, the Commission will explore the potential of enhancing the impact of energy-related directives on military infrastructure (such as offices, headquarters, barracks, hospitals, academies), including the Green Public Procurement options, as part of the European Green Deal (i.e. the new energy efficiency action "the Renovation Wave", the revision of the Energy Efficiency Directive and the Energy Performance of Buildings Directive.
- During 2022, the Commission and the High Representative will increase and intensify

[59] IF CEED (europa.eu)Circular defence - News & insight - Cambridge Judge Business School
[60] 12741/20
[61] The EDF regulation states that the "Fund contributes to the mainstreaming of climate actions in Union policies and to the achievement of an overall target of 30 % of the Union budget expenditure supporting climate objectives".

staff-to-staff work on the climate-security-defence nexus with NATO, the UN and relevant bilateral partners such as the US and Canada.

8. Conclusions

In a more complex, contested, competitive and connected world than ever before, the EU must further step up its efforts to defend its strategic interests and values. The upcoming EU Strategic Compass on Security and Defence will set out ambitious goals for Europe's long-term security and defence, to which this Communication is actively contributing.

To this end, the Commission has identified the following main new areas to further strengthen the competitiveness of the European defence market:

- **explore how to further stimulate Member States investments in key strategic capabilities and critical enablers** that are developed and/or procured in European Union cooperative frameworks;
- **further incentivise the joint procurement of defence capabilities developed in a collaborative way within the EU**, including through a VAT waiver and a possible reinforcement of EDF bonuses;
- **call upon Member States to continue moving towards streamlined and more convergent arms exports control practices**, in particular for defence capabilities developed in an EU cooperative framework.

The Commission will also implement the initiatives already launched that are key enablers for European defence, such as the **EDF and military mobility**, as well as those that are essential for strengthening European resilience, in particular in space, to counter hybrid threats, strengthen cybersecurity, and address climate change challenges related to defence.

The Commission remains ready to consider additional steps forward in the light of progress made and the evolution of the threats and challenges the Union faces in the future.