BIOTECHNOLOGY IN SECURITY AND DEFENCE

Contents

Introduction

AseBio has prepared this document with the aim of **assessing the role of biotechnology in the field of security and defence**, providing information **on funding opportunities** that have so far been largely unknown to companies in the sector, and analysing how biotechnology is defined as a dual-use technology.

Over the past year, AseBio has received invitations from various organisations to participate in events exploring the role of innovative sectors in the fields of security and defence. We have also received information from members interested in submitting proposals under NATO's Defence Innovation Accelerator for the North Atlantic (DIANA) initiative. In addition, biotech companies have expressed concerns regarding the complex process involved in exporting biotechnology products and determining whether they should be classified as dual-use items.

By way of context, the European Commission (EC) presented the **European Economic Security Strategy**[1], including proposals on the **screening of inbound and outbound investment in the EU, the coordination of export controls, the promotion of R&D in dual-use technologies, and the strengthening of research security**. Furthermore, in a Recommendation, the European Commission identified biotechnology as a critical strategic technology for Europe's economic security.

International context and the Industrial and Technological Plan for Security and Defence

Recent developments, such as the **war between Russia and Ukraine, hybrid threats, and the significant shift in United States foreign policy**, have led Europe to take a more active role in its own defence and security, as well as in developing certain technological, industrial and military capabilities on which it had previously relied less heavily.

Against this backdrop, the **Spanish Government launched the Industrial and Technological Plan for Security and Defence (PITSD)**[2], aimed at ensuring the security of the population and promoting a **new phase of industrial and technological development across Spain's productive sector**.

The Plan provides for an investment of EUR 10.471 billion in 2025, of which EUR 3.26276 billion will be allocated to **new telecommunications and cybersecurity technologies**. This includes:

- **Enhancing healthcare capabilities through the application of biotechnology, robotics and data technologies:** Within the framework of the NATO Defence Planning Process, which identifies the capabilities required by NATO, strategic investments are needed to **strengthen operational healthcare capabilities. These include critical burn care, CBRN decontamination, experimental surgery, 3D technologies and robotics, medical information systems, advanced telemedicine, and bio- and neurotechnologies for the biomedical monitoring of deployed personnel**. EUR 72.26 million.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023JC0020&qid=1687525961309

[2] https://www.lamoncloa.gob.es/consejodeministros/resumenes/Documents/2025/230425-plan-industrial-y-tecnologico-para-la-seguridad-y-la-defensa.pdf

Within the framework of the Industrial and Technological Plan for Security and Defence, the Spanish **Centre for Technological Development and Innovation (CDTI)** will channel **EUR 500 million towards R&D** through the following instruments:

- **CDTI: Grant schemes for business consortia and research centres.** Grant schemes aimed at business consortia and research centres. **EUR 100 million.**
- **CDTI: Pre-commercial public procurement of prototypes and demonstrators.** Funding for the pre-commercial public procurement of prototypes and demonstrators. **EUR 150 million.**
- **CDTI: Investment in venture capital funds specialising in defence.** Investment in venture capital funds specialising in the defence sector. **EUR 200 million.**
- **CDTI: Strengthening and enhancing the capabilities of technology centres and centres of excellence.** Support to strengthen and enhance the capabilities of technology centres and centres of excellence, including test facilities and laboratories. **EUR 50 million.**

The R&D areas to be funded by CDTI are defined in the **Spanish Ministry of Defence's Technology Roadmap and are based on the priorities established by NATO.**

Biotechnology as a disruptive technology for NATO

NATO regularly publishes reports on science and technology trends. Its report "Science & Technology Trends 2023–2043" identifies science and technology trends relevant to the defence sector that may affect capability development and pose operational challenges for NATO. The report includes a section analysing biotechnology alongside human enhancement.

More recently, the updated report "Science & Technology Trends 2025–2045"[3] devotes a specific section to the **Biotechnology Revolution**, identifying synthetic biology as a key driver of the next technological revolution in areas such as healthcare (personalised medicine, gene therapies and rapid responses to epidemics), agriculture (climate-resilient food production), energy (bioenergy), and the environment (waste and emissions management). The report also identifies a number of risks and challenges, including the potential use of CRISPR and artificial intelligence for bioterrorism, concerns regarding the privacy of biological data, and weak governance in relation to biological weapons, for which no clearly defined international framework exists.

Defense Innovation Acelerator for the North Atlantic (DIANA)

At the 2021 NATO Summit in Brussels, Allied leaders agreed to launch the Defence Innovation Accelerator for the North Atlantic (DIANA)[4] programme to **foster transatlantic cooperation on critical technologies, promote interoperability among Allied forces, and harness civilian innovation** through collaboration with academia and the private sector. DIANA aims to accelerate defence innovation across the North Atlantic.

One of DIANA's initiatives is the establishment of **Test Centres**[5], consisting of a network of testing facilities located within innovation hubs across the Alliance. Test Centres are accredited facilities where innovative technologies with applications in

[3] https://www.nato.int/cps/en/natohq/news_236107.htm?selectedLocale=en
[4] https://www.diana.nato.int/
[5] https://www.diana.nato.int/test-centres.html

defence and security can be tested and validated, with the **aim of accelerating the development and maturation of disruptive technological solutions.**

- They provide access to infrastructure and specialised technical support.
- They facilitate the development of dual-use technologies with both civilian and military applications.
- They form part of a transatlantic network of testing facilities across NATO countries.

Success Case: DIANA Test Centre for Multi-Omics and Explainable AI

The Centre for Genomic Regulation (CRG) has recently submitted a proposal to establish a DIANA Test Centre specialising in multi-omics and explainable artificial intelligence, in response to DIANA's **Data-Assisted Decision Making** challenge.

The aim is to establish the CRG as Europe's first DIANA Test Centre specialising in multi-omics and explainable AI for data-assisted decision-making. The Test Centre would model complex biological systems and support applications in both military and civilian healthcare, including personalised medicine, pandemic preparedness and response, and exposome research. It would therefore constitute a dual-use technology initiative.

Biotechnology as a dual-use biotechnology

Dual-use items are defined as items, including software and technology, that can be used for both **civilian and military purposes**. These may include items that can be used for the design, development, production or use of nuclear, chemical or biological weapons or their means of delivery, including all items that can be used for both non-explosive purposes and for assisting in the manufacture of nuclear weapons or other nuclear explosive devices.

The definition of dual-use items also encompasses dual-use technology. The terms **dual-use technology** and **dual technology** are commonly used to refer specifically to this **technological component; that is, the specific information required for the development, production or use of an item that may have both civilian and military applications.**

Regulation (EU) 2021/821, which establishes a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items, includes a 400-page **Annex I setting out the items and technologies considered to be dual-use**. Several of these are related to biotechnology.

The Spanish Ministry of Defense Technology Roadmap

Despite the above, in the **recent presentation of its Technology Roadmap**, the Spanish Ministry of Defence outlined seven strategic pillars[6] aimed at transforming Spain's defence industry.

One of these pillars focuses on **strengthening sovereign technological capabilities** in order to reduce technological dependence on third countries through investment in artificial intelligence, advanced sensors, robotics, unmanned systems and cyber defence. **Biotechnology is not included among these strategic pillars.**

[6] https://www.infodefensa.com/texto-diario/mostrar/5309279/teniente-general-ivorra-anuncia-hoja-ruta-siete-ejes-transformar-industria-defensa-espanola

However, in its document "High-Impact Technologies for Defence in the 2035 Operational Environment", published in 2024, the Spanish Ministry of Defence identifies **biotechnology** as one of the **technological advances** increasingly featured in research, analyses and capability-development plans related to security and defence worldwide, in line with NATO priorities.

Conclusions

In Spain, biotechnology is not included in the Spanish Ministry of Defence's Technology Roadmap as a key technology for the defence sector.

However, institutions such as NATO, and initiatives such as DIANA, identify biotechnology as a relevant technology for defence and security.

From AseBio's perspective, and based on the main conclusions drawn from the session in which we participated during the **First NATO Biotechnology Conference — Panel 2: Fostering Biotechnology Ecosystems in Defence and Security**, we can conclude that:

- The biotechnology and defence sectors have limited knowledge of each other, and there are currently few connections between the two fields. The biotechnology sector has a strong capacity to respond to emerging challenges but requires a framework that can help align its capabilities with the needs and challenges of the defence and security sectors.
- Greater cooperation between the two sectors is possible. However, the biotechnology sector requires:
    - A better understanding of defence and security needs.
    - A flexible and agile framework, including adaptable regulation, mechanisms to anticipate demand, and measures to ensure security of supply.
    - Tailored instruments to support its development, including funding mechanisms for research and development. One potential example would be preferential public procurement for biotechnology products developed and manufactured in Europe.

Furthermore, biotechnology is recognised as a dual-use technology, meaning that it can have both civilian and military applications. In light of the above, **there may be opportunities for biotechnology stakeholders to participate in initiatives such as DIANA, as already proposed by organisations such as the Centre for Genomic Regulation (CRG). There may also be funding opportunities for biotechnology under various CDTI programmes and through joint initiatives involving CDTI and the Spanish Ministry of Defence.**

For these reasons, AseBio believes that the following **actions should be undertaken**:

- **Information and exploratory activities among AseBio members** to raise awareness of the current context and the positioning of biotechnology within the defence sector at both national and international levels.
- **Information-sharing and engagement activities with the Spanish Ministry of Defence** to increase awareness of the capabilities, technologies and solutions developed by the biotechnology sector that may have potential applications in defence and security.

- As outlined in **Annex 2 on EU Funding for Defence and Security**, the European Commission is adapting and updating existing EU funding programmes, including the Strategic Technologies for Europe Platform (STEP) and the Framework Programme, in response to the ReArm Europe Plan and with the aim of strengthening defence preparedness and investment. Therefore, another area of action for AseBio would be to **monitor developments and policy changes introduced by the European Commission in the field of defence, particularly those affecting EU funding programmes.**

Annex 1 CDTI Iniciatives

Dual-use technologies – Colaboration with MINISDEF

CDTI collaborates with the Spanish Ministry of Defence through a cooperation protocol aimed at building a strong national industrial base in **dual-use technologies**.

CDTI serves as one of the main gateways for companies seeking to enter the security and defence sector, as it is, among other roles, an implementing agency for the Industrial and Technological Plan for Security and Defence (PITSD).

Areas of cooperation:

- **Coordination of funding at national level:** exchange of information and coordination in the use of R&D funding.
- **Mutual support within international programmes:** European Defence Fund (EDF), Horizon Europe (HE), Defence Innovation Accelerator for the North Atlantic (DIANA), and NATO Innovation Fund (NIF).
- **Multilateral programmes:** potential CDTI contributions to major strategic defence programmes are assessed on a case-by-case basis.

Science and Innovation Missions 2025

MISSION 6. Training for the strategic autonomy in security and defence.

- **Information security and protection:** aimed at preventing the unauthorised interception or decryption of data that could affect key decision-making centres and critical infrastructure or lead to technology leakage, among other risks. The development of advanced, higher-performance communication systems and solutions for cybersecurity, cyber surveillance and digital forensics based on quantum cryptography, post-quantum algorithms and new encryption techniques, among other technologies, is proposed as a priority area for action. Furthermore, to ensure strategic autonomy, the implementation of advanced hardware solutions is also envisaged.
- **Development of more efficient and cost-effective automated and remotely managed systems for security and defence applications:** aimed at enabling tasks to be carried out more safely, resiliently, efficiently and cost-effectively. These precision-based and autonomous systems, designed for aerial, land, surface or underwater operations, represent an innovative pillar of twenty-first-century defence and are therefore considered a priority area for action.
- **Higher-performing, more sustainable, efficient and secure products and systems for aerial, land and naval platforms:** incorporating new or enhanced features compared with conventional products and systems, using advanced materials and/or enabling more effective and efficient human–machine collaboration within a digital ecosystem. This area also seeks to enhance the survivability of platforms and the personnel they carry.
- **Enhancing the protection and security of critical infrastructure:** in the current context, it is essential to ensure that telecommunications networks and systems, strategic storage facilities and other critical infrastructure that are vital to the functioning of society and the economy receive a high level of protection. Accordingly, a priority area under this mission is the development of initiatives to strengthen capabilities for detecting, monitoring and responding to threats affecting these facilities, including cyberattacks, sabotage and natural disasters. This also includes critical subsea infrastructure that is essential for global connectivity, energy supply and

maritime surveillance, such as telecommunications cables, energy transport pipelines, offshore platforms and ocean-monitoring sensors, among others.

- **Protection against CBRN risks (chemical, biological, radiological and nuclear):** including advanced detection, monitoring and response systems, as well as solutions for the remote detection of storage and/or production sites and for detecting the use of weapons involving CBRN agents.

Cervera Programme

Thematic areas:

- **Advanced Communications — Mobile Networks:** The development of advanced mobile networks is an essential pillar in the digital transformation of defence capabilities. The evolution from 4G to 5G and, in the future, to 6G provides significant improvements in speed, latency, reliability and connection density, enabling secure, real-time communications even in complex operational environments. These networks support the effective deployment of autonomous systems, distributed operations, advanced command and control, and the rapid exchange of critical information in tactical and strategic scenarios. Their development is essential to ensuring the robust and resilient connectivity required by modern security and defence forces.
- **Defence against Asymmetric Threats:** Asymmetric threats, such as terrorism, cyber warfare and the use of drones, pose unique challenges to traditional security and defence forces. These threats often involve non-state actors using unconventional tactics to exploit vulnerabilities in critical infrastructure and target civilian populations.
- **Artificial Intelligence:** Technologies based on deep learning and generative artificial intelligence are revolutionising the way data are processed, decisions are made and complex operations are carried out. In the defence sector, these capabilities enable the development of systems capable of analysing large volumes of information in real time, identifying patterns, anticipating threats and supporting decision-making in dynamic and demanding environments. These developments must be implemented in accordance with the principles of human oversight, explainability, and ethical and responsible use, which are essential to ensuring operational trust. The integration of AI into defence systems represents a strategic advancement that can enhance effectiveness, response speed and information superiority in operational environments.
- **Advanced Materials:** Advanced materials drive innovation across multiple industries by improving the performance, sustainability and efficiency of products and systems. These materials possess enhanced or entirely new properties compared with conventional materials, enabling their application in strategic sectors.
- **Autonomous Systems — Advanced Mobility:** The traditional concept of transport is evolving towards the broader and more innovative concept of mobility. Priority is given to the development of autonomous or remotely operated systems capable of integrating sensors, real-time data processing and artificial intelligence, with the aim of improving route planning, movement efficiency and the responsiveness of land, aerial and naval vehicles. These technologies can enhance logistical efficiency, increase operational autonomy in hostile environments and reduce personnel exposure during high-risk missions.

CDTI Partially Repayable Support for Dual-Use Technologies

Complementary assessment of the dual-use nature of technologies — Consultation with the Spanish Ministry of Defence

Neotec 2025

The NEOTEC 2025 call included a budget allocation of EUR 20 million, entirely earmarked for financing dual-use technology areas linked to the Defence Technology and Innovation Strategy (ETID).

Public Procurement of Innovation (PCP)

PCP: procurement of R&D services up to Technology Readiness Level 7 (TRL 7) for validation by the public authority in a real-world environment, followed by the transfer or reallocation of the resulting assets to the relevant public administration. This instrument involves competitive procurement procedures for the development of prototypes.

PITSD allocates **EUR 150 million** to this line of action.

Innvierte

Investment in venture capital funds specialising in the defence sector.

PITSD allocates **EUR 200 million** to this line of action.

Annex 2 EU Funding for Defense [7]

The EU finances defence through various instruments included in its budget to support research, development, production, procurement and infrastructure projects.

The main EU defence funding instrument is the **European Defence Fund (EDF)**, launched in 2021 to support defence research and development, alongside other initiatives such as **military mobility projects.**

Since the beginning of Russia's war of aggression against Ukraine in 2022, the EU has increased defence expenditure under the Union budget. In 2023, it also adopted two temporary instruments to support **ammunition production** and strengthen the European defence industry through **common procurement**.

The EU is currently working on a new programme for the defence industry and simplifying existing rules and procedures in order to reduce regulatory bottlenecks in the Union's defence sector and accelerate access to European funding.

1. **European Defence Fund (EDF):** The Fund entered into force on 29 April 2021. It has a budget of **EUR 8.8 billion** to support defence research and development during the 2021–2027 period. The Fund promotes cooperation among EU companies and research organisations of all sizes and from across the Union in the fields of research and development and interoperable defence technologies and equipment. Of the total EUR 8.8 billion budget, **EUR 1.5 billion** would be allocated to projects under the Strategic Technologies for Europe Platform (STEP).
2. **European Defence Industry Programme (EDIP):** Agreed on 16 October 2025, the programme provides **EUR 1.5 billion in grants** to strengthen the European defence industry.
3. **Military Mobility:** A budget of **EUR 1.76 billion** is allocated to enabling armed forces to move more rapidly.
4. **Ammunition Production:** A budget of **EUR 500 million** is allocated to strengthening ammunition production capacity.
5. **Common Procurement in the Defence Sector:** This is a temporary instrument with a budget of **EUR 310 million**, which entered into force on 18 October 2023. It is aimed at encouraging Member States to jointly procure defence products, thereby generating greater economies of scale.
6. **Simplification of Rules and Procedures in the Defence Sector:** This consists of a Defence Readiness Omnibus package aimed at simplifying the legal and administrative framework governing the defence sector.
7. **Amendments to Existing EU Funding Programmes:** More recently, on 5 November 2025, the Council and the European Parliament reached an agreement to incentivise defence-related investment through the EU budget. These measures respond to the **ReArm Europe Plan / Readiness 2030**, an initiative proposed by the European Commission during the first half of 2025 with the aim of strengthening European defence preparedness and investment. They are intended to facilitate faster, more flexible and better-coordinated investment in the European defence technological and industrial base.
   Under the new rules, five existing EU funding programmes will be amended:

   - **Digital Europe Programme**
   - **Horizon Europe Programme**
   - **European Defence Fund (EDF)**

[7] https://www.consilium.europa.eu/es/policies/defence-funding/

- Connecting Europe Facility (CEF)
- Strategic Technologies for Europe Platform (STEP)

Results of the EU Framework Programme for Security (2007–2023)

Between 2007 and 2023, the EU Framework Programme for Security funded a total of **762 projects**, involving more than **5,000 organisations**. This represented an investment of over **EUR 3.5 billion**, accounting for approximately **50% of the total EU budget dedicated to security research and innovation (R&I).**

The projects focused on the following thematic areas:

- Disaster Risk Reduction
- Border Security
- Critical Infrastructure Protection
- Fighting Crime and Terrorism
- Cybersecurity

The overall objective of these projects was to strengthen research and innovation in the field of security.

Annex 3 Biotechnology trends in the Defense Sector – NATO

The research areas in this field that are of potential interest to NATO are outlined below:

1. **Biological warfare and health**

Specific areas of interest:

1. New technologies for the detection and identification of pathogens and CBRN threats.
2. Disruption of the pathophysiological processes caused by biological agents.
3. New classes of medicines, including performance-enhancing drugs and antibiotics.
4. Disease prevention.
5. Biometrics.
6. Wound healing and regeneration.

The development of medical countermeasures may combine advances in bioinformatics, biosensors, human enhancement and synthetic biology. Examples include:

- Prediction and detection of biological and disease-related risks.
- Rapid development of CBRN countermeasures.
- Improved rehabilitation through neural interfaces.
- Robotic prostheses.
- Diagnosis and treatment of traumatic brain injury and post-traumatic stress disorder.

Combat casualties are specifically addressed, with examples including biosensors, bioinformatics, remote monitoring, molecular and cellular biology, artificial intelligence for rapid diagnosis, surgical techniques and tools, and novel tissues for identifying and treating injuries and infections.

2. **Genetics and microbiology**

Genetic engineering and synthetic biology are identified as technologies that may provide new capabilities and influence the defence sector.

3. **Bioengineering and biomanufacturing**

Biomanufacturing of chemicals and novel materials for military applications.

Potential areas of application include:

- Biomaterials for the construction of facilities, reducing the need to transport materials and deploy heavy equipment.
- The use of biotechnology for the maintenance of facilities, platforms and equipment, including the management of biofouling and biofilms on maritime vessels.
- Xenobots for nanoscale manufacturing.
- Living biosensors, including persistent aquatic or land-based sensors and CBRN monitoring systems.

4. Systems Biology and bioinformatics

Areas of particular interest include:

- CBRN biological sensors.
- Computational biology.

Examples of biosensors include:

- Nanosensors embedded in clothing to detect CBRN agents.
- Treatment monitoring, for example in diabetes management.
- Photonic biosensors.
- Smart tattoos for monitoring physiological or cognitive stress.
- Sensors for detecting explosives and chemical warfare agents.

The combination of biosensors and bioinformatics may support:

- Predictive casualty care and diagnosis.
- Operational readiness assessment, including the monitoring of overtraining, nutritional deficiencies, immunocompetence, cardiovascular health and musculoskeletal injuries.
- Assessment of exposure to CBRN agents.

5. Human enhancement

Human enhancement may be addressed across several dimensions:

- **Cognitive enhancement:** including physiological or pharmacological approaches to improving cognitive performance.
- **Social enhancement.**
- **Physical performance enhancement:** including pharmaceuticals and exoskeletons.
- **Human–machine symbiosis.**

The overall objective is to enhance human capabilities and significantly extend the boundaries of human performance.

This section provides a summary of the report *Science & Technology Trends 2023–2043: Across the Physical, Biological, and Information Domains*, NATO Science & Technology Organization, **Volume 2: Analysis**, available at the following link.

Annex 4 Products and Technologies Considered Dual-Use under Regulation (EU) 2021/821

- 1C351: **Human and animal pathogens and "toxins",** as follows:
    - **1C351.a:** Viruses, whether natural, enhanced or modified, either in the form of "isolated live cultures" or as material including living material that has been deliberately inoculated or contaminated with such cultures, from a list of 59 viruses.
    - **1C351.c:** Bacteria, whether natural, enhanced or modified, either in the form of "isolated live cultures" or as material including living material that has been deliberately inoculated or contaminated with such cultures, from a list of 22 bacteria.
    - **1C351.d:** Toxins and toxin subunits thereof, from a list of 19 toxins. This category includes an exclusion for botulinum toxins and conotoxins formulated for medical use.
    - **Fungi:** Fungi, whether natural, enhanced or modified, either in the form of "isolated live cultures" or as material including living material that has been deliberately inoculated or contaminated with such cultures, comprising two specific species.

- 1C353: **"Genetic elements" and "genetically modified organisms"** containing genetic elements that encode:
    - Any gene or genes specific to any of the viruses specified in sub-items 1C351.a or 1C354.a.
    - Any gene or genes specific to any bacterium specified in sub-items 1C351.c or 1C354.b, or to any fungus specified in sub-items 1C351.e or 1C354.c, and which meet either of the following criteria:
        - They constitute, in themselves or through their transcribed or translated products, a significant hazard to human, animal or plant health; or
        - They could "confer or enhance pathogenicity".
    - Any of the "toxins" specified in sub-item 1C351.d or any "toxin subunits" thereof.

- 1C354: **Plant pathogens**, as follows:
    - **1C354.a:** Viruses, whether natural, enhanced or modified, either in the form of "isolated live cultures" or as material including living material that has been deliberately inoculated or contaminated with such cultures, comprising two potato viruses.
    - **1C354.b:** Bacteria, whether natural, enhanced or modified, either in the form of "isolated live cultures" or as material that has been deliberately inoculated or contaminated with such cultures, comprising five plant pathogens.
    - **1C354.c:** Fungi, whether natural, enhanced or modified, either in the form of "isolated live cultures" or as material that has been deliberately inoculated or contaminated with such cultures, comprising eleven plant pathogens.

- 2B352: **Equipment capable of use in handling biological materials, as follows:**
    - **B352.b: Fermenters capable of cultivating "microorganisms" or living cells for the production of viruses or toxins,** with a total internal volume

of 20 litres or more, as well as components designed for such fermenters, including cultivation chambers, cultivation chamber holding devices and process-control units.

- **2B352.c: Centrifugal separators** capable of continuous separation and possessing all of the following characteristics:
  - A flow rate exceeding 100 litres per hour.
  - Components made of polished stainless steel or titanium.
  - One or more seals within the steam-containment area.
  - The capability for in situ steam sterilisation while closed.
- **2B352.d: Cross-flow (tangential) filtration equipment** capable of separating "microorganisms", viruses, toxins or cell cultures and possessing all of the following characteristics:
  - A total filtration area equal to or greater than 1 m².
  - Either of the following characteristics:
  - The capability for in situ sterilisation or disinfection; or
  - The use of disposable or single-use filtration components.
  - Components designed for this type of equipment.
- **2B352.e: Steam- or gas-sterilisable freeze-drying equipment** with a condenser capacity of 10 kg or more, but less than 1,000 kg, of ice within a 24-hour period.
- **2B352.f: Protective and containment equipment, as follows:**
  - Full or partial protective suits, or hoods, dependent upon an external air supply connected to the suit and operating under positive pressure.
  - Biological containment chambers, isolators or biological safety cabinets possessing all of the following characteristics during normal operation:
    - A fully enclosed workspace in which the operator is separated from the work by a physical barrier.
    - The capability to operate under negative pressure.
    - The ability to safely manipulate materials within the workspace.
    - Air entering and leaving the workspace is filtered through a high-efficiency particulate air (HEPA) filter.
- **2B352.f: Aerosol inhalation equipment** designed for aerosol challenge testing with "microorganisms", viruses or "toxins" and possessing any of the following characteristics:
  - Whole-body exposure chambers with a capacity of **1 m³ or greater**.
  - Nose-only exposure devices using directed aerosol flow and with an exposure capacity for **12 or more rodents**, or **two or more non-rodent animals**.
  - Closed animal restraint tubes designed for use with exposure devices such as those described above.
  - **2B352.h: Spray-drying equipment** capable of drying toxins or pathogenic "microorganisms" and possessing all of the following characteristics:
    - A water evaporation capacity of **0.4 kg/hour or greater and 400 kg/hour or less**.
    - The capability to generate product particles with an average size of **10 µm or less**, using existing equipment or with minimal modification of the spray dryer.
    - The capability for in situ sterilisation or disinfection.

- 2B352.i: **Nucleic acid assemblers and synthesisers**, whether partially or fully automated, designed to generate continuous nucleic acids longer than **1.5 kilobases**, with error rates below **5% in a single run.**

With regard to **Royal Decree 679/2014**, it establishes the control regime governing the foreign trade of dual-use items and technologies, defence-related products and other materials. Therefore, for the purposes of this analysis, the following defence-related and dual-use items associated with the biotechnology sector have been included:

- **Annex I.1: Defence-related products in general.** The following items are particularly relevant to biotechnology:
  - **ML7: Chemical agents, "biological agents", "riot control agents", radioactive materials, related equipment, components and materials, as follows:**
    - **ML7.a:** "Biological agents" or radioactive materials selected or modified to increase their effectiveness in causing casualties among humans or animals, degrading equipment, or damaging crops or the environment.
    - **ML7.b:** Chemical warfare agents.
    - **ML7.e:** Equipment specially designed or modified for military use and designed or modified for the dissemination of the materials specified in ML7.a, among others.
    - **ML7.f:** Protective and decontamination equipment specially designed or modified for military use, as well as components and chemical mixtures intended to provide protection against the materials specified in ML7.a, among others.
    - **ML7.g:** Equipment specially designed or modified for military use and designed or modified for the detection or identification of the materials specified in ML7.a, among others.
    - **ML7.h:** "Biopolymers" specially designed or processed for the detection or identification of chemical warfare agents specified in ML7.b, and cultures of specific cells used in their production.
    - **ML7.i:** "Biocatalysts" for the decontamination or degradation of chemical warfare agents and biological systems covered by ML7.a and ML7.b
      - **12. Biological systems** containing the specific genetic information required for the production of the "biocatalysts" specified above, including:
        - "Expression vectors".
        - Viruses.
        - Cell cultures.
  - **ML22 – Technology**
    - **5.5:** "Technology" exclusively "required" for the incorporation of the "biocatalysts" specified in ML7.i.1 into military carrier substances or military materials.

- ANNEX III.3 — Lists of Dual-Use Items and Technologies Subject to Import and/or Introduction Controls

    - List of dual-use items covered by the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) Weapons and on Their Destruction:

        a. Bacteria: *Bacillus anthracis*, *Brucella abortus*, *Brucella melitensis*, *Brucella suis*, *Burkholderia (Pseudomonas) mallei*, *Burkholderia (Pseudomonas) pseudomallei*, *Coxiella burnetii*, *Francisella tularensis*, *Vibrio cholerae* and *Yersinia pestis*.

        b. Viruses: Ebola virus, Venezuelan equine encephalitis virus, tick-borne encephalitis virus, haemorrhagic fever viruses, yellow fever virus, Guanarito virus, Hantaan virus, Junín virus, Lassa virus, Marburg virus, Machupo virus, Nipah virus, Sabiá virus and variola virus.

        c. Toxins: Botulinum toxins, *Clostridium perfringens* toxins, *Staphylococcus aureus* enterotoxin B, ricin, saxitoxin and T-2 mycotoxin.