1. Goal of the call

Development and validation of innovative dual-use defence solutions potentially benefiting the national defence forces, international defence organisations (EDA, NATO), the defence forces of allied nations, as well as civilian research and local industry.

2. Objectives

Incentivise individual and collaborative R&D projects leading to advances in joint areas of defence, civilian research, and industry.

- smart mobility
- resilient infrastructures
- strategic foresight and climate change adaptation

The joint call intends to provide a financial incentive to applicants who have an identified research or material/technology/product/solution and have to demonstrate its relevance and potential benefit for defence applications (the "project"). Technology transfer from civilian applications is acceptable, insofar as military applications still require a significant RDI effort with significant technical risks.

Using a flexible approach, applicants may apply for funding at any steps below, which can be considered as key R&D milestones (TRL 2-6) towards market access for defence applications.

- Research activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies, which can achieve significant effects in the area of defence (**generating knowledge**)
- Activities that aim to increase interoperability and resilience, including secured production and exchange of data, to master critical defence technologies, to strengthen the security of supply or to enable the effective exploitation of results for defence products and technologies (**integrating knowledge**)
- The design of a defence product, tangible or intangible component or technology as well as the definition of the technical specifications on which such a design has been developed, including any partial tests for risk reduction in an industrial or representative environment (**design**)
- The system prototyping of a defence product, tangible or intangible component or technology enabling the identification of prime contractors (**system prototyping**)

Projects shall comprise clear R&D milestones towards dual-use applications. Due to the specificities of the Defence Sector and Luxembourg's current positioning within the EU defence industry landscape, commercialising the product immediately after the call is not a requirement, however, identifying the adequate defence value chain and the potential prime contractor while aiming at becoming an acknowledged technology supplier in the EU/NATO defence value chain, will be essential.
The challenges addressed in this joint call are based on the Luxembourg Defence Guidelines for 2025 and beyond, the Space defence strategy of the Directorate of Defence, the European Defence Agency (EDA)'s overarching strategic research agenda (OSRA) as well as the EU capability development plan (CDP) and the EDA 2023 EU capability Development Priorities.

3. Call topic

While the European Commission (EC) - under Horizon Europe - and the European Space Agency (ESA) R&D activities are related to pure civilian applications, the European Defence Agency (EDA) and NATO (North Atlantic Treaty Organisation), as well as EC's European Defence Fund (EDF), are focussing on

dual-use and defence applications. With the EU striving for more autonomy, cooperation in defence R&D within EDA, NATO and the EDF is key. To prepare the Luxembourgish industry for future international R&D collaborations that contribute to the EU Capability Development Plan and the Strategic Compass, the technologies to be developed through this Call must be innovative dual-use solutions addressing both defence and civil community needs.

In line with Luxembourg's vision for a digital and sustainable economy by 2025 as well as national (Luxembourg Defence Guidelines 2035) and EU (the 2023 EU Capability Development Plan, A Strategic Compass for Security and Defence) priorities in Defence as well as the EU-NATO Joint Declarations on Cooperation (2023), focussing on military mobility, resilience and protection of critical infrastructures, emerging disruptive technologies, security implications of climate change, Space and Foreign information manipulation and interference, consortia will focus on the following topics:

- Call topic 1: SMART MOBILITY
- Call topic 2: RESILIENT INFRASTRUCTURES
- Call topic 3: STRATEGIC FORESIGHT AND CLIMATE CHANGE ADAPTATION

3.1 Call topic 1: SMART MOBILITY

Relevance for Defence

Taking into consideration the European Commission Action Plan on Synergies between Civil, Defence and Space Industries, the EU Action Plan on Military Mobility 2.0 (following the Strategic Compass call to enhance the military mobility and the support of military operations of armed forces within and beyond the Union) as well the European Defence Agency's Action Plan on Autonomous Systems (APAS), the SMART MOBILITY topic is relevant for the military operational domains LAND, AIR, CYBER and SPACE as well as for strategic research domains related to ENERGY & ENVIRONMENT and MATERIALS.

The following priority domains shall be addressed by consortia:

- SMART MOBILITY 1: Autonomous Systems
- SMART MOBILITY 2: Alternative powertrain systems and fuels
- SMART MOBILITY 3: Lightweight Materials

Detailed description

3.1.1 SMART MOBILITY 1: Autonomous Systems (LAND, AIR, SPACE, CYBER)

Autonomous systems have the potential to provide operational benefits across a broad range of missions, from intelligence, surveillance, target acquisition, and reconnaissance (ISTAR), through widely distributed vehicles and sensors, to logistics and resupply – with autonomous platforms increasingly capable of delivering supplies to soldiers, provide in-theatre transport and support MEDEVAC operations.

Stakeholders proposing RDI projects will consider including the development and/or usage of digital technologies (e.g. simulation, virtual testing and/or validation, digital twins, real-time monitoring, IoT, sensors, AI/ML, virtual reality, data analytics, predictive analytics, rapid prototyping, etc.).

Proposals including system engineering or System of Systems (SoS) approaches are encouraged. Proposals should take on a security-by-design approach when applicable.

Application domains

- **Autonomous systems for sensing, analytics, decision-making and acting (LAND, AIR):** This category aims at R&D related to the development of enhanced sensing, thinking and decision capacity systems, the development of enhanced acting capacity and of enhanced mobility. Solutions range from object or target recognition and full spectrum sensing to integrated perception and scene understanding, as well as from self-localisation, mapping and routing navigation to agile obstacle avoidance and smart navigation in dense and dynamic environments, in all types of settings or weather conditions. The development of explainable mathematical models and accountable rule-based decisions to produce intelligence is also targeted. The use of high-performance computing (HPC) and big-data analytics (BDA) is encouraged.

Technological subcategories (non –exhaustive list):

- computer vision;
- robust and lightweight real-time simultaneous location and mapping;
- tracking of fast-moving assets;
- automated dispatching, trip coordination and control of multiple vehicles in formation;
- forecasting and prediction;
- automated failure detection;
- recommender systems;
- human-machine collaboration.

- **Integrated Perception and Scene Understanding (SPACE):** Proposals in this category should focus on developing autonomous systems integrating data from high-resolution EO sources and using advanced Positioning, Navigation, and Timing (PNT) techniques for tasks like object recognition, scene understanding, and solution orientation. This includes employing data fusion techniques to enhance the system's ability to interpret complex on-field environments and integrating in-situ data. The goal is to develop agile systems effectively combining data sources for improved adaptability and precision in understanding real-world scenarios in support to ground troops.

- **Agile Obstacle-Avoidance and Smart Navigation Systems (SPACE):** Applicants are invited to submit proposals that address navigating dynamic terrestrial environments. The primary emphasis should be on developing sophisticated obstacle-avoidance techniques and intelligent navigation algorithms capable of processing environmental data. This includes information from the immediate surroundings, encompassing aspects such as topography, weather conditions, obstacles, human activities, and threat assessments. The goal is to create adaptive navigation systems that dynamically respond to real-time data, ensuring agility in complex terrestrial settings.

- **Testing, validation, verification of Autonomous Systems, including training (LAND, AIR):** This category aims at R&D to support the development of fault-tolerant Autonomous systems and to overcome Testing, Validation and Verification (V&V) gaps. Solutions range from learning by using training data to anomaly detection, value-based reasoning, abstraction and judgement. The use of virtual reality (VR), augmented reality (AR) and/or mixed reality (MR) solutions as a means of interaction are also targeted, including for man-in-the-loop training applications.

Technological subcategories (non –exhaustive list)

- context-aware applications;
- distributed virtual environments;
- multi-parameter testing scenarios;

- realistic/immersive scenarios; simulation tools;
- traceability of results and progress backup;
- ethical and/or legal framework.

- **Secured Connectivity for Enhanced Military Mobility (LAND, AIR, SPACE):** Current and future space-based navigation (Galileo/EGNOS), secured communication, and Earth Observation (Copernicus), have the potential to significantly benefit military mobility. This subcategory focuses on the development and integration of advanced communication technologies to ensure secure, reliable, and high-speed connectivity for high mobility network nodes with inconsistent connectivity. Proposals should leverage on technologies such as 5G networks, QKD, Software-Defined Networking, cloud-enabled solutions, for enhanced security and reliability of mobile military assets.

Technological subcategories (non –exhaustive list):

- 5G networks;
- QKD;
- Software-Defined Networking;
- Cloud-enabled solutions.

- **Tactical drones and UAV (LAND, AIR, SPACE, CYBER**): While drones and UAV are being used extensively for civil purposes (Rescue, Environmental Monitoring), the importance of drones for military logistics, demining, energy relay and ISR has also been increasing in recent years. In addition, cybersecure artificial intelligence and autonomy are critical to operating unmanned platforms.

Technological subcategories (non –exhaustive list):

- Developing advanced autonomous swarming capabilities for tactical drones and UAVs (related to SPACE): This involves creating intelligent algorithms and communication protocols to enable a coordinated and efficient swarm of drones for applications such as military logistics, demining, and ISR.
- Improvement of energy efficiency and endurance of tactical drones and UAVs (related to SPACE). This includes advancements in battery technologies, lightweight materials, and energy management and transfer systems to extend mission durations. New techniques for energy transfer (ground to air) should be explored.
- Adaptive Sensing and Perception Systems (related to SPACE): This involves enhancing onboard sensors, computer vision algorithms, space-based navigation systems for precise positioning and machine learning capabilities.
- AI decision engines capable of autonomously generating its goals based on continuous risk evaluation and models.
- Directed energy using optical solutions.

- **Autonomous systems with resilient cybersecurity (SPACE, CYBER):** Given that more and more defence products are developed, produced and commercialised from off-the-shelf solutions provided by civil companies, especially in the unmanned and autonomous realm, the need for a system engineering approach to adapt these assets to the demanding defence and cyber resilience requirements – addressing the complexity of the digital battlefield – is getting more pressing. Moreover, the usage of off-the-shelf components is creating system vulnerabilities and breach risks that need to be addressed with a security-centric mindset1. In order to limit the risks related to deception, denial of service / usage, misuse by unauthorized parties, or breach of confidentiality, which all may prevent legitimate users to fulfil their mission, or even to expose them to harmful situations, there is a need to cover three dimensions.

- First dimension: Intrinsic Security
  - Organisations engaged in operating Autonomous systems have to reach a good enough level of information security. In particular, they have to monitor their system to detect any malicious or accidental event that would harm the integrity and availability of their systems. They also need to perform effective threat hunting in order to prevent or limit the occurrence and impact of an incident.
- Second dimension: Product security, with a focus on supply chain.
  - Indeed, most of the time, Autonomous systems are actually systems of systems, embedding a significant number of digital capabilities. Product testing must happen on a recurrent, if not quasi real-time, basis, and be as automated as possible. Here too, threat-hunting is a mandatory capability.
- Third dimension: Providers' security
  - These systems of systems merge tools and products from various origins. Therefore, it's mandatory to be able to confirm and monitor the level of security of the external providers involved in the assembly of the product .

Technological subcategories (non –exhaustive list):

- Secure System Architecture Design (related to Space): Proposals should include advanced system engineering techniques to design architectures that can withstand cyber threats, enhance interoperability of systems, and ensure the integrity and availability of critical functions in autonomous systems. This implies handling cyber protection requirements and military engineering needs simultaneously and in a coordinated manner.
- Intrusion Detection and Response Systems for Autonomy (related to Space): Efforts should target the development of sophisticated intrusion detection and response systems tailored for autonomous systems. Applicants can explore innovative approaches in system engineering to create adaptive and real-time methods that detect and mitigate cyber threats and vulnerabilities stemming from the usage of off-the-shelf hardware, while preserving the autonomy and functionality of the system.
- End-to-End System Resilience Testing (related to Space): Proposals should target system engineering methodologies for end-to-end resilience testing of autonomous systems. This includes the development of testing ranges and frameworks, simulation environments, and methodologies to assess the cybersecurity resilience of the entire autonomous system (ground to space), from perception, and decision-making to action execution.
- Capacity to monitor the system in real-time (Cyber).
- Capacity to monitor information shared about the system's producer or user in order to detect signals about a possible incident that would not have been identified through the first capacity (Cyber)
- Capacity to detect, assess and monitor emerging threats targeting products or organisations (Cyber)
- Secure and efficient cloud-based capacity to share raw security data concerning the system or the supporting organisations, and to offer specific security services (Cyber)
- Definition of generic scenarios documenting threats and risks related to autonomous systems. And sharing through a standardized risk management platform (Cyber)
- Capacity to perform automated and remote security tests on autonomous systems (Cyber)

3.1.2 SMART MOBILITY 2: Alternative powertrain systems and fuels:

Innovative solutions for hybrid, electric and alternative propulsion systems and fuels (in gaseous and liquified forms) are being already developed and deployed for civilian applications (references: the EU Green Deal, the EU 2030 climate and energy framework (Stepping up Europe's 2030 climate ambition) and the EC Sustainable and Smart Mobility Strategy). This includes systems for power supply, storage and management.

Military applications are broadly similar to those of civilian applications, although further defence-specific developments are required for military operating environments. Achieving higher levels of self-sufficiency is needed, so that equipment powered by alternative fuels and powertrain systems can perform under conditions of isolation from sources of supply, such as on a battlefield, exhibiting previously unattained levels of consumptions and reliability. In addition, the capacity to generate and distribute high-density energy to cope with unexpected energy demands needs to be considered as mission critical.

Stakeholders proposing RDI projects will consider including the development and/or usage of digital technologies to support their efforts (e.g. simulation, virtual testing and/or validation, digital twins, real-time monitoring, IoT, sensors, AI/ML, data analytics, predictive analytics, rapid prototyping, etc.).

Application domains

- **Zero and low-emission propulsion systems/ powertrains**: This category seeks to incorporate renewable and alternative energy/fuel systems into power source combinations, encompassing e-fuels, with the goal of diminishing energy consumption and reducing reliance on fossil fuels.
  Technological subcategories (non –exhaustive list):
  - electric,
  - renewable hydrogen;
  - hydrogen-fuelled internal combustion engines (H2 ICE);
  - hydrocarbon or synthetic fuels;
  - fuel cells (FCEV);
  - dual-fuel;
  - hybrid, plug-in hybrid and range-extended electrified propulsion technologies;
  - retrofitting of the above; gas control products and systems.

- **Electric high-voltage (HV) components**: this category targets power electronics and electrical high-voltage (HV) components (e.g. electric motors, inverters, etc.) and their efficiency improvements, including cost, weight and/or size reduction measures, as well as overall system optimization, robustness or hardening considerations.
  Technological subcategories (non –exhaustive list):
  - electric drive motors, inverters, converters;
  - Battery Management Systems (BMS),
  - Thermal Management Systems (TMS);
  - Transmission control units (TCU); integrated drive modules (iDM);
  - thermal management systems;
  - software development and system integration;
  - charging technologies...

- **Energy storage solutions for military systems**: This category aims at R&D related to energy storage (batteries; capacitors; thermal; kinetic; solid-state; efuels, including hydrogen, …) and energy converters for mobile platforms reducing the reliance on fossil fuels.
  Technological subcategories (non –exhaustive list):
  - high-performance battery cells for high energy / high power applications;

- military-grade battery module and pack solutions;
- cell and pack validation testing capability, recycling and remanufacturing of the above;
- light, durable and safe hydrogen storage tanks.

3.1.3 SMART MOBILITY 3 Lightweight Materials

Advanced Materials technologies can be used in a wide variety of defence applications such as more agile aircrafts and emerging hypersonic systems, autonomous terrestrial and air-borne systems (UAV) with extended autonomy or payload, robust terrestrial vehicles built with lightweight and durable (e.g. reparable) structures as well as improved lightweight protection equipment's for hostile / harsh operation conditions, and personal protective equipment based on lightweight ballistic materials.

Regarding military applications of advanced materials, lightweight structures have been identified as one of the main technology trends [4]. Lightweight materials and structures (i.e. through lightweight design) lead to reduced fuel/energy consumption, hence providing improved range, autonomy or payload capabilities to any vehicle or aircraft. Military applications also call for ballistic materials that exhibit high-strength and are very lightweight. These materials and structures could be well integrated in or associated to load-bearing structures and could provide ballistic protection to combat vehicles or militaries (in Personal Protective Equipment such as ballistic inserts, lightweight under suits, combat helmets, anti-mine boots and flame-resistant uniforms).

Based on EDA and NATO evaluations, specific defence priorities are: materials and design with improved protection of persons, vehicles and systems; new materials & coatings & sensors, their production and repair methods for joining of different materials, to be implemented in future platforms that are lighter and have improved & multifunctional & self-healing properties; nanotechnology, graphene-based technologies, hybrid composites and smart materials.

Application domains

- **Bio-sourced and/or recyclable lightweight materials & structures for mobile and static applications**: This category aims at reducing carbon footprint (in production and use) for mobile (rolling vehicles, ships, submarines, aircrafts, launchers, spacecrafts, and satellites) and static applications (energy & communication supply & operations command infrastructure).

Technological subcategories (non –exhaustive list)

- composites, ceramics, graphene and metals; nanoparticles for thermal management
- Support structures, satellite panels, body panels, high pressure hydrogen tanks, interior cabin components
- fiber winding technology
- additive manufacturing
- improved properties for impact, de-icing …

- **Bio-sourced and/or recyclable lightweight materials & structures for soldier & vehicles & critical infrastructure**: This category aims at R&D related to the development of protective systems (kinetic, HPEM, laser or C-IED activities, cyber-attacks, etc.) and add-on armoured solutions.

Technological subcategories (non –exhaustive list)

- ballistic inserts, lightweight under suits, combat helmets, anti-mine boots and flame-resistant uniforms

- **New manufacturing, joining and repair processes in mobile applications**: With the introduction of new (ultra) lightweight materials with improved properties, as well as multi-materials structures, it is essential to develop other joining techniques than bolting/riveting/welding to reduce weight and to reduce possible damages, as well as reducing the time for maintenance. Moreover, new production techniques (such as additive manufacturing) can be developed to make new design and assembly of components possible Finally, advanced materials with self-healing, self-repairing or self-replicating properties permit to develop less time consuming and more cost effective repair processes

- **Computational Design and materials modelling applied to mobile applications**: This category aims at R&D related to the development and design of new structures, components and platforms/systems using computational methods, design tools and software tools (codes, algorithms) for prediction of the properties and behaviour of new/novel materials and structures; virtual manufacturing and simulation of manufacturing processes (deformations during AM processing, thermal processes during fiber placement etc.); improve damage tolerance: multi-scale methods to relate microstructure to processing and material and component or platform properties, including signature-related parameters. Initial testing is done on a computer before physical prototypes are built to save cost and time spent on the development. Moreover, new production techniques (such as additive manufacturing) make new design and assembly of components possible, even onsite production of repair and spare parts.

Technological subcategories (non –exhaustive list):

  - Numerical Simulation of composites materials and processes;
  - Data-driven computational modelling of materials and processes;
  - Virtual testing;
  - Calculation tools for hybrid materials.

3.2 Call topic 2: RESILIENT INFRASTRUCTURES

Relevance for Defence

Taking into consideration the European Commission Action Plan on Synergies between Civil, Defence and Space Industries, the EU Policy on Cyber Defence, the EU Space Strategy for Security and Defence, the Joint Communication on a "new outlook on the climate security nexus" the as well as EC JRC/EDA's report on the "Impact of Climate change on defence related critical energy infrastructures", as well as the final report of the EU-NATO Task Force for Resilient Critical Infrastructures, the RESILIENT INFRASTRUCTURES topic is relevant for the military operational domains CYBER (Digital) and SPACE, as well as for strategic research domains related to ENERGY (& ENVIRONMENT) and MATERIALS.

The following priority domains shall be addressed by consortia:

- RESILIENCE 1 Resilience of critical infrastructures and supply chains
- RESILIENCE 2 On-site Manufacturing and Clean Energy

Detailed description

3.2.1 RESILIENCE 1: Resilience of critical infrastructures and supply chains

NATO and the European Union released a Final Assessment Report produced by the NATO-EU Task Force on the Resilience of Critical Infrastructure on on the 29 June 2023). Launched at the beginning of

the year, the Task Force focused on mapping out current security challenges, and the particular importance of resilience in energy, transport, digital infrastructure, and space.

Application domains

- **Resilience and Protection of Space assets:** The EU Space Strategy for Security and Defence outlines the counterspace capabilities and main threats in space that put at risk space systems and their ground infrastructure. Increasing the resilience and protecting space systems and services against threats such as Cyberattack sabotage, electronic warfare, Radiation, Space Debris/Micro meteorites and non-kinetic laser or indirect energy weapons. The protection against cyberattacks requires the same types of security capabilities than for any system of systems. It means that the three dimensions described for autonomous systems are the same, with the need to adapt the specific detection, assessment and monitoring capabilities to the features and environment of a space asset. Key digital technologies in resilience and operations are Cloud Computing, Digital Twins, AI managed grids, AI managed Cyber offense/defence, Quantum Computing, Blockchain and zero-trust. Proposals including system engineering or System of Systems (SoS) approaches are encouraged. Proposals should take on a security-by-design approach when applicable.
-

Technological subcategories (non –exhaustive list):

- ***On-orbit Servicing of Space Systems (Space):*** *Proposals are encouraged to explore the feasibility and initial stages of development for robotic systems intended for servicing missions. Preliminary work should encompass activities related to rendezvous, proximity operations, and the development of system components such as robot tools, avionics, and sensors (among others). Special focus should be directed towards satellite refuelling concepts or early-stage developments. Technologies to be explored may include those pertaining to propellant transfer, fluid management, and interfacing and docking, catering to both prepared and unprepared satellites scheduled for refuelling. Proposals aimed at advancing the maturity of technologies, including testing, are also welcome.*
- ***Cyber Resilience for space infrastructures (Cyber****): Proposals should address the development of robust cybersecurity measures that adhere to defense-in-depth principles, precisely customized for both ground and space segments. This includes advanced threat and vulnerability detection, protection of ground-to-space command link, protection of the supply chain and the development environment, implementation of secured communication strategies, and so on. The utilisation of international standards, such as NIST, NIS, CCSDS, ECSS, etc., is strongly encouraged to ensure a comprehensive and standardized approach to cybersecurity.*
- ***Remote testing and monitoring of IoTs (Cyber in Space****) : space assets are for most of them unmanned and similar to industrial systems. The fundamentals of their protection are therefore similar, with specific requirements related to the physical environment (extreme condition, possible interferences) and the distance.*

- ***Space based defence / Protection against Non-kinetic or directed energy attacks (Space):*** *Research proposals are sought in the following key areas to enhance protection against non-kinetic or directed energy attacks in the space domain. Investigations into coatings, adaptive optics, and thermal management systems are sought, aiming to develop materials, components, or systems that are resilient to thermal and structural effects and damages. Encouragement is given for the integration of cybersecurity*

measures and the strengthening of space situational awareness for early threat identification.

- ***Satellite self-healing and damage prevention capabilities (Space**): Propose concepts that incorporate robust incident response, damage identification and prevention for space assets. This comprises protocols capable to re-install system software, shut down of critical systems in case of solar radiation storm and third-party threat identification to enhance mission lifetimes. This subcategory should also address self-healing material that can repair itself in case of minor damage caused by impacts from micrometeoroids or other debris.*
- ***Smart Radiation-Hardening (Space):** Propose cutting-edge concepts leveraging innovative hardware and/or software solutions to enhance the resilience of space systems against radiation-induced challenges. The objective is to prevent system failures, enhance the reliability of power management and ensure data and communication integrity in harsh space environments. Develop intelligent solutions enabling the use of Commercial Off-The-Shelf (COTS) components.*
- ***On-Orbit computing for increased spacecraft mobility (Space)** : This call invites innovative proposals targeting on-orbit computing solutions to elevate spacecraft mobility. Proposals should focus on developing technologies that enhance space situational awareness, facilitate threat identification, and enable a real-time decision-making process using on-board computing. The goal is to achieve increased reactivity and optimise manoeuvres.*

- **Innovation high throughput and secure earth to space connectivity (Space)**: Providing secure, rapid and reliable connectivity is crucial for government digital inclusion programmes, disaster relief management and critical services.

Technological subcategories (non –exhaustive list):

- ***Optical communication for High Data Rate Space Connectivity**: Proposals are sought for the development of critical technologies or concepts to demonstrate high-data-rate optical links (up to terabit/sec) and/or harness quantum entanglement for near-instantaneous communication. The envisioned technologies should ensure seamless interoperability among nodes and networks, connecting assets and users located in both space and on the ground.*
- ***Optical Space Communication Terminals for on-field Deployment:** This call invites proposals to advance optical communication terminals tailored for on-field deployment, emphasizing reliability across diverse operational settings, including combat environments. It is encouraged to explore innovative concepts for miniaturization and portability, develop robust optical components capable of withstanding harsh conditions, and design systems for rapid satellite link acquisition, ensuring timely and efficient performance.*
- ***Secure optical communication in MWIR**: Traditional radio technology has been the primary means of military communication for decades, but it is well-documented that radio is susceptible to interception and jamming, compromising the security and reliability of critical communications. There is a need for more secure and resilient communication solutions. Optical communication in a new band such as MidWave InfraRed (MWIR) would allow not only better covert operations and detection avoidance, but also higher robustness to weather conditions compared to current optical communication. One of the most promising light sources for MWIR are femtosecond fiber lasers which also have the potential to be miniaturized and ruggedized.*

- ***Quantum Key Distribution for Secure Earth-to-Space Connectivity****: Explore proposals leveraging QKD within satellite communication technologies to enhance the security of earth-to-space connectivity. This subcategory aims to develop innovative solutions that provide an ultra-secure communication channel, ensuring the confidentiality of sensitive data for government digital inclusion programs, disaster relief management, and critical services.*
- ***Secure Software-Defined Radio (SDR) Payloads for High Throughput Satellite (HTS) Communications:*** *Proposals are encouraged to advance the development of secure SDR-based satellite communication payloads. Integrating cutting-edge encryption and authentication protocols will ensure a high level of security, contributing to the provision of secure, rapid, and reliable earth-to-space connectivity. This is particularly crucial for governmental programs, disaster relief management, and critical services.*

- **Critical Energy Infrastructures with resilient Cybersecurity (CYBER)**: The European Union Agency for Cybersecurity (ENISA) has identified in 2022 8 primes threats to the European Cybersecurity landscape: Ransomware, Malware, Social Engineering Threats , Threats against data, Treats against availability as Denial of Service, Threats against availability as internet threats, Disinformation – misinformation and Supply-Chain attacks. This category aims at R&D for resilient cybersecurity for critical energy infrastructure, which are intrinsically linked to electrification, digitalisation, connectivity and automation.

Technological subcategories (non –exhaustive list):

- *Real time monitoring of complex industrial systems;*
- *Digital twins with predictive capabilities.*

- **Cyberdefence for supply chain product and system security (CYBER):** This category targets methodologies, processes and tools to make the supply chain resilient against a wide array of known and possible attacks.

Technological subcategories (non –exhaustive list):

- *Software supply chain assessment, monitoring and maintenance*
- *Product (Hardware or software) and systems' security through continuous testing*
- *Predictive simulation of products' models*
- *Automated attack surface mapping*
- *Automated threat hunting through online / cloud-based security information sharing*

3.2.2 RESILIENCE 2: On-site manufacturing and clean energy

In June 2023, the European Commission and the High Representative adopted a Joint Communication on the Climate-Security Nexus laying out how the EU will address the **growing impact of climate change and environmental degradation in the fields of peace, security, and defence, with a particular focus on military infrastructures**. A coherent and smart approach to the climate adaptation and mitigation efforts of the military must preserve, and where possible enhance, operational effectiveness. Improved energy efficiency and sustainability not only reduces the carbon footprint, it reduces costs49, decreases the logistical burden and advances self-sustainability in the operational context – thus adding to the safety and freedom of movement of the armed forces. It must also take into account that the armed forces operate specialised equipment that usually has a very long life-cycle, whereas developing next generation capabilities can take years if not decades.

Application domains

- **Smart Self-sustaining Camps**: Enhancing the resilience and viability of fossil free and low carbon military camps is a priority within initiatives such as the Consultation Forum for Sustainable Energies and the Incubation Forum for Circular Economy in European Defence. European Projects such as EDF-2021-INDY and EDF-2021 NOMAD target combining renewable energy sources, energy management and energy efficiency tools and methods to obtain energy self-sufficiency in small to medium sized military camps. Soil revitalisation and on-site additive manufacturing can moreover increase resilience within military camps.

Technological subcategories (non –exhaustive list):

- ***Smart camp design*** *(construction and net zero emission building such as AI-based data analytics and virtual reality technologies for camp design and spatial placement, BIM, modular construction units, self-sufficient or at least nearly zero energy building (at a standalone level), smart coatings, energy self-adaptable walls and windows ; materials for insulation)*
- ***Smart camp energy systems and energy efficiency*** *(energy technologies including energy storage, energy resilience, renewables, hydrogen; modular infrastructure units for energy production, storage, distribution; portable energy harvesting, storing and management; DC power systems with smart building and energy management; EMS ; micro-grids ; mobile heating and cooling, ….)*
- ***Technologies for self-sustaining camps*** *using energy recuperation and harvesting techniques, soil revitalization and on-site manufacturing (AM)*
- ***Security by design*** *for both components and integration / architecture as well as Security on edge for sensors and actuators*

3.3 Call topic 3: STRATEGIC FORESIGHT AND CLIMATE CHANGE ADAPTATION

Relevance for Defence

Taking into consideration the European Commission Action Plan on Synergies between Civil, Defence and Space Industries, the EU Climate change and defence Roadmap as well as the EU Space Strategy for Security and Defence as well as the report "Resilient and Robust: Climate-Proofing the Military for Increased Military Effectiveness", the STRATEGIC FORESIGHT AND CLIMATE CHANGE ADAPTATION topic is relevant for the military operational domains LAND and SPACE, as well as for Capability Technologies related to ENERGY & ENVIRONMENT.

The following priority domains shall be addressed by consortia:

- STRATEGIC FORESIGHT: Open-Source Intelligence (OSINT)
- CLIMATE 1: Earth Observation and Intelligence, Surveillance and Reconnaissance
- CLIMATE 2: Clean Technologies

Detailed description

3.3.1 STRATEGIC FORESIGHT: Open-Source Intelligence (Space, Cyber)

Open-Source Intelligence (OSINT) has emerged as an indispensable asset capable of providing both tactical awareness and strategic foresight. OSINT can be utilised to understand an enemy's capabilities, intentions, and vulnerabilities - which can aid in pre-emptive actions – as much as it can serve to validate intelligence from diversified sources.

Application domains:

- **Visual Intelligence for Enhanced OSINT (Space):** Proposals should harness advanced visual intelligence technologies (GEOINT) to enhance Open-Source Intelligence (OSINT) capabilities. Proposals in this subcategory should focus on the development of innovative tools specifically designed for the analysis and interpretation of visual data, providing insights to support both tactical awareness and strategic foresight. Use and combination of publicly available space-borne imagery is strongly encouraged in the frame of this topic.

- **Media Analytics: real-time situational awareness (Cyber)**

- **Predictive analytics (Cyber, Space):** Proposals should develop tools that leverage on data extracted from historical earth observation imagery (both air and space) to identify patterns in order to predict potential future developments, understand adversary intentions and formulate pre-emptive strategies.

- **Anomaly detection/ verification of disinformation (Cyber, Space):** Proposals in this subcategory should aim to develop robust systems capable of leveraging data (including space-data) to identify irregularities, false narratives, and deceptive information.

Technological Subcategories (non-exhaustive list):

  - *AI "poisoning" detection and remediation*

3.3.2 CLIMATE 1: Earth Observation and Intelligence, Surveillance and Reconnaissance

With the European External Action Service (EEAS)'s Climate Change and Defence Roadmap, the EU intends to boost its strategic foresight, early-warning, situational awareness and conflict-analysis capacities using qualitative and quantitative data and innovative methods from various sources. This knowledge shall be used to design future missions, operations and actions properly, taking into account parameters ranging from changing weather conditions to the local political context. Earth Observation and ISR capabilities are crucial to understand climate change and its impact on security and defence in view conflict prevention and climate change mitigation and strategic foresight. (Flagship Reference projects to be mentioned from Copernicus, SatCen, EUSPA, ESA, etc...exemple. Digital Twin Earth, etc..)

Application domains:

- **Advanced Analysis for Climate Security Impact (Space) :** Proposals in this subcategory should concentrate on advancing algorithms and methodologies to effectively utilise EO data, in conjunction with ISR capabilities. The primary objective is to gain a comprehensive understanding of the impacts of climate change, particularly in conflict regions or areas prone to natural disasters or long-term effects of climate change. The analysis outputs should establish clear connections between environmental degradation and its implications for security. Additionally, proposals should identify indicators leading to sustainable and environmentally responsible Defence practices.

Technological subcategory (non-exhaustive list):

  - *AI powered EO data processing and exploitation of ISR for green defence*

- **Near-real-time space-borne Data processing and HPC for on-field risk assessment (Space):** Proposals are invited to develop tools that facilitate near-real-time decision-making by leveraging space-borne data, encompassing high spatial and/or temporal resolution data, and a variety of data sources beyond space. The generated information should directly

contribute to on-field risk assessments. The incorporation of high-performance computing is strongly encouraged to ensure timely output generation.

Technological subcategory(non-exhaustive list):

- *Real time monitoring for protecting sensors and communication integrity*

3.3.3 CLIMATE 2: Clean Technologies

Taking into account the changing security and operating environment (as set out in the EU Global Strategy, the EU's climate change and defence roadmap and the EU strategic Compass), the defence sector is likely to be deployed to increasingly harsh environments with possible energy and water shortages.

Application domains:

- **Environmental Technologies water & wastewater:** Water is a scarce natural resource and is as critical an enabler as energy for successful military operations. This subcategory looks at technological solution to ensure safe reuse of water for military and peace keeping missions, portable water treatment and generation, water saving applications and water management applications.

Technological subcategories (non –exhaustive list):

- *mobile water treatment, small greywater treatment units, desalination system powered by renewable energy, purification systems, personal water filters, water treatment, optimisation, management and monitoring of water consumption and quality, consumption reduction devices, IoT use for monitoring of water quality.*

- **Future green, efficient, safe and multi-sources energy solutions**: This category aims at R&D solution for energy generation and energy harvesting to respond to the challenges of eliminating or reducing the power source requirements and lowering the logistic burden from supplying power (including batteries) to remote or on the move equipment and devices.

Technological subcategories (non –exhaustive list):

- *Solar energy (Capturation of solar energy, solar energy from building surface;*
- *Lightweight / high efficiency panels;*
- *Building integrated photovoltaics (BIPV) and building applied photovoltaics (BAPV);*
- *Solar energy storage solutions and wind energy (horizontal & vertical axis);*
- *Hydro-energy and energy from waste technologies;*
- *Innovative approaches to Energy Harvesting based on the Complementary Combination of Technologies, nano-generators;*
- *IOT applications and AI systems for energy capability.*

- **Green innovative solutions for recycling soldier equipment**: This category targets R&D solutions for mechanical and/or chemical recycling and reuse of equipment. The Material dismantling, reuse and recycling, separation processes enabled by advanced technology.

Technological subcategories (non –exhaustive list)

- *Material dismantling;*
- *Reuse and recycling;*
- *Separation processes enabled by advanced technology.*

- **Land remediation solutions** : Land used for military purposes can be threatening to the environment. This subcategory aims developing R&D solution for depollution and remediation of such land. The call seeks proposals for projects dedicated to sustainable soil management in arid and semi-arid areas, mitigate water and wind erosion, facilitate plant growth, and establish a carbon dioxide sink.

4. General eligibility criteria and instruments of the joint call

4.1 Consortia are expected to include at least one eligible participating company and one FNR-eligible participating public research organization. In the consortium, the contribution of the private and public parties should be as close to equal as possible, whereas no party shall bear more than 70% of the total project cost. Companies must fulfil the general eligibility criteria of article 2 of the RDI law[1] and the respective criteria of the specific State aid scheme they apply for as set out in the R&D schemes[2]. Research organizations must be eligible under article 3-(2) of the FNR statute (*Loi modifiée du 31 mai 1999 portant création d'un fonds national de la recherche dans le secteur public*) and be registered at the FNR.

4.2 The project must be in the field of industrial research[3] and/or experimental development[4] as defined in article 1 of the RDI law, and in line with the call topic.

4.3 For research and development activities under the joint call for projects, public institutions should comply with the general principles set forth in the FNR Guidelines, such as the formal requirements to qualify as PI (Principal Investigator) of an FNR-funded project and/or as supervisor of an FNR-funded Ph.D. student, the FNR Research Integrity Guidelines, and the FNR data management plan, as well as those included in the FNR BRIDGES Programme description.

The FNR will fund the costs of the eligible public research organizations in Luxembourg, up to 500.000 € per project, covering project-specific costs (see FNR Financial Guidelines for details).

The Ministry of the Economy will co-finance costs borne by Luxembourg-eligible companies up to 500.000 € per project, using the R&D aid scheme[2].

The maximum co-financing rates for companies through collaboration are as follows:

Maximum aid intensities	Large company	Medium company	Small company
Experimental development	40%	50%	60%
Industrial research	65%	75%	80%

[1] Modified law of 17 May 2017 on the promotion of research, development and innovation

[2] *https://guichet.public.lu/en/entreprises/financement-aides/aides-recherche-developpement/rdi/aides-rdi.html*

[3] 'Industrial research' means the planned research or critical investigation aimed at the acquisition of new knowledge and skills for developing new products, processes or services or for bringing about a significant improvement in existing products, processes or services. It comprises the creation of components parts of complex systems, and may include the construction of prototypes in a laboratory environment or in an environment with simulated interfaces to existing systems as well as of pilot lines, when necessary for the industrial research and notably for generic technology validation.

[4] 'Experimental development' means the acquisition, combination, shaping, and use of existing scientific, technological, business, and other relevant knowledge and skills with the aim of developing new or improved products, processes, or services. This may also include, for example, activities aiming at the conceptual definition, planning, and documentation of new products, processes, or services.

The costs related to patents and certifications are not eligible in this call. However, for SMEs (large companies excluded) these costs can be co-funded up to 50% under the Innovation Aid for SMEs aid scheme[5]. In this case, the SME has to file a separate State aid request to the Ministry of the Economy.

The project duration is a maximum of 36 months continuous period.

Upon justification regarding their liquidity needs, the Ministry of the Economy may give a 30% upfront payment to SMEs leading a project selected in this joint call. For public research organizations, the FNR financial regulations apply.

The consortium must be composed of national applicants only. Under justified conditions sub-contractors from NATO Members, EU EEA/EFTA States[6], as well as the following NATO Indo-Pacific Partners, Australia, Japan, Republic of South Korea and New Zealand, could contribute to the project. Self-funded partners are permitted to participate in the consortium.

Employees from companies and research organizations taking part in the project need to have nationalities of a NATO Member Country, from an EU EEA/EFTA Country or from one of the following NATO Indo-Pacific Partners, Australia, Japan, Republic of South Korea and New Zealand. Applicants will be required to:

- Provide a narrative CV for the Principal Investigator (PI) (for RPOs only)
- Provide a list of personnel that is going to work on the project (including their nationalities and work experience; full CV – Europass format) (for companies and RPOs)
- Sign a declaration of honour as part of the Project outline (PO) Phase-1 submission process, ensuring that in case of the presence of non-NATO or EU EEA/EFTA nationalities, appropriate measures are put in place for safeguarding project related information.

5. Evaluation criteria and scoring system

The project proposals will be evaluated in a balanced manner based on the following criteria and considering the general considerations formulated under the call topic and objectives:

5.1 Relevance (33,33%)

This criterion aims to evaluate the quality and the innovative character of the project through the following aspects:

- project idea; clarity and pertinence of the objectives;
- level of innovation, including advancements on the state of the art;
- soundness of the research approach and methodology or technology assessment study;
- due consideration of ethical and regulatory aspects;
- scientific and technical maturity of the project;

[5] https://guichet.public.lu/en/entreprises/financement-aides/aides-recherche-developpement/rdi/aide-innovation-pme.html
[6] NATO Member States: https://www.nato.int/cps/en/natohq/nato_countries.htm ; EU EEA/EFTA Countries: https://www.efta.int/EEA/EEA-EFTA-States#:~:text=Information%20about%20the%20three%20EEA,(the%2030%20EEA%20States)

- clarity, coherence, and adequacy of the application regarding the theoretical framework, objectives, methodology, work plan, and expected results and impacts;
- relevance for dual use and defence applications.

5.2 Implementation: quality and efficiency of the project plan (33.33%)

This criterion is intended to assess the quality and feasibility of the project work plan to ensure its success. The following aspects are taken into consideration:

- coherence and effectiveness of the work plan, including appropriateness of the allocation of tasks and resources;
- competencies, experience and complementarity of the individual participants, as well as, of the consortium and collaboration as a whole;
- the level of ambition of the collaboration and commitment of the participants in the proposed project;
- appropriateness of the management structures and procedures, quality of the risk management plan and soundness of the risk mitigation plan;
- development processes shall be based on "security by design" when applicable.

5.3 Impact (33.33%)

This criterion is intended to assess the potential impacts and contributions of the project. The following aspects are taken into consideration:

- economic and societal added value of the proposed research and development project in line with national priorities;
- added value of the proposed research/technology/product/solution for dual use and defence purposes;
- strengthening the competitiveness and growth of involved companies by developing innovations addressing market opportunities in the defence sector;
- where applicable, soundness of the business plan outlining a clear path towards an economic exploitation of the project results, and to what extent the project can carry on beyond the co-funding period;
- effectiveness of the proposed measures to exploit and disseminate the project results;
- where applicable, demonstrate ambition of being recognised as Luxembourgish Tech Provider within EU defence supply chain.

6. Call process

The Submission and evaluation process will be composed of 2 phases.

6.1 Submission process

Phase-1: (*15 April 2024 9am – 14 June 2024 2pm*)

Project outline (PO) to be submitted on the research-industry-collaboration platform of Luxinnovation. The PO shall provide information on:

- Project description;
- Project outcomes;
- Expected technical contributions of the different partners;
- Intellectual Property Rights for collaborative project proposals (in view of a draft collaboration agreement in phase 2);
- Preliminary project costs;
- Declaration of honour;
- CV (Europass format) of the principal investigator from each public and private partner respectively;
- For companies: Organizational chart of the group, 2022 and 2023 balance sheets and P&L accounts of the applicant and the group, cash-flow forecast.

Phase-2: (*22 July 2024 9am – 30 September 2024 2pm*)

Full project proposal (FPP) to be submitted by each project participant to the Ministry of the Economy (Myguichet platform) for companies and to FNR (FNR Grant Management System) for accredited research organizations. The models of FPP as well as the financial annexes to be appended by each partner to the aid application can be downloaded from the platform www.research-industry-collaboration.lu.

The FPP shall provide information on:

- Detailed description of the research project;
- Different activities of the project (work packages);
- Description of the technical challenges and implementation of the project;
- Description of the expected outcome and the economic impact;
- Milestones;
- Timeline;
- Resources;
- Description of costs;
- Collaboration agreement (draft ready for signature) including agreement on intellectual property[7];
- GDPR aspects: data flow and ownership, delegations to data processors.
- Narrative CV for the Principal Investigator (PI) (for RPOs only)
- List of personnel that is going to work on the project (including their nationalities and work experience; full CV – Europass format) (for companies and RPOs)

Each consortia submitting a phase 2 proposal should contact the Control office for exports, imports and transit (OCEIT) to get support if the technology developed falls under the dual-used importation and exportation rules.

6.2 Evaluation process

[7] Any intellectual property (IP) rights that result from the collaboration should be allocated to the different collaboration partners in a manner which adequately reflects their contributions and respective interests in the project. The main IP terms of the collaboration agreement between the company and the public research institute should thereby comply with the "Framework for State aid for research and development and innovation (2014/C 198/01)", paragraph 2.2.2. "Collaborations with undertakings".

Phase-1:

Based on the Project Outlines (PO) and the annexes submitted via the research-industry-collaboration platform, the granting authorities in collaboration with Luxinnovation will check:

- Eligibility of all parties and co-funding capacity of the company;
- If the project description is in line with the call topic;
- If the project objectives are in line with the objectives of the call.

Participants will obtain written feedback from the granting authorities on Luxinnovation's research-industry-collaboration platform. In case of a high number of POs, the granting authorities reserve the right to make a pre-selection based on the budget of the joint call, the level of innovation and quality of the application, as well as the economic and societal impact in line with national strategic priorities. In case of a positive pre-evaluation, applicants will be invited to proceed to Phase-2, possibly with some recommendations from the organizers of the call.

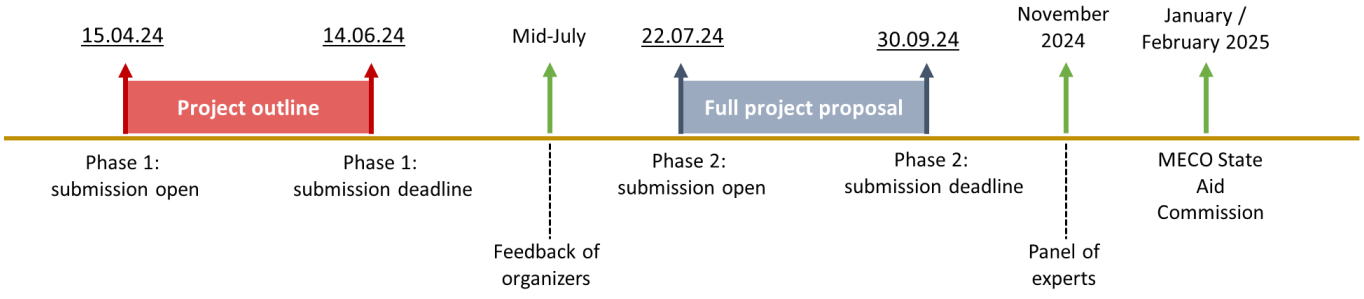
Phase-2:

Full project proposals (FPP) prepared in Phase-2 will be reviewed by an independent expert panel ("panel") that will assess FPPs from a scientific/technical and economic point of view. The panel will establish a ranking list based on the criteria set in the "Evaluation criteria and scoring system" section above. The highest ranked projects will be recommended for funding to FNR and the Ministry of the Economy. In the case of companies, all projects will need to undergo an additional consultation at the State Aid Commission. The decision on the company's grant is subject to a further positive recommendation by the State Aid Commission.

A project can only be funded by a concurring decision of FNR, the Ministry of the Economy, and the Directorate of Defence of the Ministry of Foreign and European Affairs.

The results of the evaluation will be communicated in February 2025. Projects are expected to start in March 2025.

The contracts will be established separately between FNR and the public partners on the one hand, and between the Ministry of the Economy and the private partners on the other hand. These contracts will include IP clauses, which restrict the sale or licensing of intellectual property resulting from the work to prior authorisation by the Directorate of Defence of the Ministry of Foreign and European Affairs, Defence, Development Cooperation and foreign Trade.



7. FAQ

Questions and answers related to the joint call can be found on the research-industry-collaboration platform (FAQ). Applicants are invited to consult the FAQ section regularly as there will be constant updates.