DIANA® Defence Innovation Accelerator *for the* North Atlantic

2024 DIANA CHALLENGE PROGRAMME CALL FOR PROPOSALS

BACKGROUND

The Defence Innovation Accelerator for the North Atlantic (DIANA) works to accelerate the development of emerging and disruptive technologies across the NATO Alliance. Through a cross-alliance pool of technology innovators, DIANA aims to establish a ground-breaking talent supply base and dual-use technology pipeline to meet NATO's diverse and increasingly complex defence needs.

NATO operates in a world marked by systemic, global risks and challenges, including pandemics, climate change, resource scarcity, cyber security, nuclear threats, and the potential misuse of emerging technologies like artificial intelligence (AI) and quantum technology. Such risks threaten NATO's core objectives of collective defence for the preservation of peace and security. Together with its partner organisation, the NATO Innovation Fund (NIF), DIANA is creating and strengthening effective and responsive pan-NATO ecosystem from which advanced solutions will emerge. As global security challenges are rapidly evolving, complex, interconnected and increasingly interdependent, this ecosystem must be flexible, resilient, scalable and sustainable, adopting a risk-based approach to support the development of technology solutions across a broad set of problems. Throughout the fulfillment of its objectives, DIANA will be guided by principles of responsible technology development and innovation, striving for solutions that are effective, ethical and accountable.

Adopting the approach and principles above, DIANA has developed a set of **Focus Areas** derived from its 2024-2025 Strategic Direction. These dual-use priorities combine the potential to address NATO's security and defence needs, scientific and technical feasibility, and market potential, providing a structural framework developed with guidance from the Allies. The focus areas in turn form the basis for **Challenge Statements**, developed to be as technically agnostic as possible, allowing innovators the greatest flexibility for creativity in proposing novel technology solutions free from preconceived constraints or methods.

For its 2024 call, DIANA will seek solutions in a Challenge Programme comprising five Challenge Statements that address key focus areas from the Strategic Direction; these challenge statements are further refined by three cross-cutting themes (depicted in Figure 1, below).

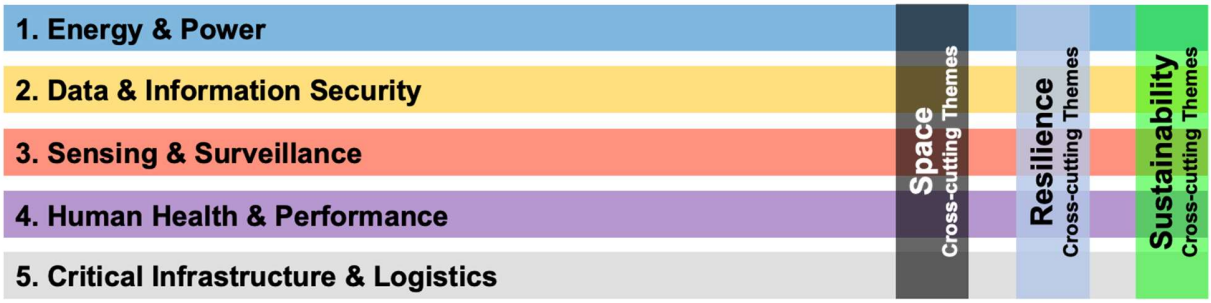

Figure 1: The Challenge Statements with cross-cutting themes.

The five Challenge Statements are listed below with detailed challenge descriptions in the subsequent sections:

- **Energy & Power**
- **Data & Information Security**
- **Sensing & Surveillance**
- **Human Health & Performance**
- **Critical Infrastructure & Logistics**

Three **cross-cutting themes** are designed to encourage innovators to consider the interconnection of applications and technologies across different domains. These themes are drawn from DIANA's Strategic Direction:

- **Space:** The environment of **space** represents a vast and largely unexplored frontier with immense potential for scientific discovery and technological innovation. It encompasses a wide range of technical challenges, from space exploration and astronomy to satellite technology and space-based communication systems and sensing. Cutting across the challenges, space-based technologies involve, or are implicated in, topics that span climate change, cybersecurity, artificial intelligence, and advanced manufacturing.

- **Resilience:** This theme emphasises the need for solutions and technologies that can withstand and quickly recover from disruptions or threats. With this theme, DIANA seeks resilient energy systems, secure and robust data infrastructures, rugged sensing and surveillance systems, adaptable human health and performance systems, and strong critical infrastructures that can withstand various operational environments and challenges.

- **Sustainability:** DIANA seeks to emphasise the importance of developing and implementing environmentally friendly, energy-efficient technologies and practices that ensure long-term viability. A key part of responsible innovation, this objective is designed to encourage solutions that meet current needs without compromising the ability of future generations to meet theirs.

CHALLENGE STATEMENTS

1. ENERGY & POWER CHALLENGE

Challenge Statement: The domain of energy generation and provision faces significant challenges, including increasing demand, aging infrastructure, environmental impact, systemic resilience issues, and cyber-physical security threats. Addressing these challenges requires an inherently dual-use approach to develop energy systems that can ensure a reliable power supply, withstand a variety of threats, and adapt to changing environmental conditions.

This challenge focuses on enhancing resilience in energy and power across various contexts, including generation, storage, distribution, recovery, harvesting, and access across land, sea, air, and space. Potential solutions may involve modular power generation and storage; low power chips for energy efficiency in digital transformation; advanced batteries and fuels; and interfaces to provide energy to mobile systems.

Example Scenarios: In a remote arctic research station, scientists rely on renewable energy technologies, such as wind and solar, to power their research equipment and maintain their living conditions in the harsh environment. Simultaneously, a nearby military outpost uses the same renewable energy systems to power their operations, reducing their reliance on fuel supplies that are difficult to deliver in the extreme conditions. During a severe winter storm, both the research station and the military outpost face the challenge of maintaining power supply as the storm impacts the efficiency of their wind and solar systems. However, their advanced energy storage technologies, including advanced batteries, ensure a steady supply of energy throughout the storm. Post-storm, the challenge lies in quickly recovering and restoring any damaged energy infrastructure. This scenario illustrates the dual-use of renewable energy technologies and the challenges they can face in extreme conditions for both civilian and military applications.

These scenarios are illustrative and not exhaustive. We encourage innovators to think creatively about the potential dual-use innovation solutions to energy and power statement.

Exemplar Descriptive Attributes: The aim of the Energy & Power Challenge is to develop innovative solutions that may:

- Enhance the resilience of power generation systems, enabling them to withstand various threats and adapt to changing conditions.
- Improve the efficiency and reliability of energy storage systems, ensuring a steady supply of energy even during peak demand periods or power outages.
- Decrease the mass and volume of energy storage systems for mobile applications.
- Optimise the energy distribution network, reducing energy losses and minimising the risk of single-point failures.
- Promote energy recovery, harnessing waste energy and converting it into usable power.
- Advance energy harvesting and conversion technologies, capturing energy from the environment and converting it into electrical power or (clean) fuel.
- Enhance energy replenishment for mobile applications, with robust reusable modular interfaces for fast recharging or refuelling that can be navigated both manually and autonomously.

Potential Enabling Technologies and Technical Approaches: May include, but are not limited to the following:

- Renewable Energy Technologies: harnessing power from renewable and ambient sources such as solar, wind, hydro, kinetic and geothermal.
- Synthetic Fuels and Biofuels: can be used as alternatives to traditional fossil fuels, providing potential practical solutions and reducing dependency on oil.
- Energy Storage Technologies: examples include advanced batteries, supercapacitors, flywheels thermal storage, etc.
- Smart Grid Technologies: optimising distribution and use of electricity, reduce energy losses and disruptions, and enable rapid response to changes in supply and demand.
- Nuclear Micro-Reactors, Small Modular Reactors and Novel Reactor Technologies: generate electricity and heat and be used in remote or mobile locations where it is difficult to establish a traditional power grid.
- Cyber-Physical Security: protecting from cyber threat of energy systems as they become more digital and interconnected.
- Data Analytics and Artificial Intelligence: can be used for predictive maintenance, real-time energy management, and anomaly detection.
- Vehicle Energy Infrastructure: modular interfaces allowing rapid, repeated, safe recharging or refuelling of autonomous vehicles in land, sea, air or space.
- Energy Efficiency Technologies: reducing power consumption (insulation, retrofitting, heat loss reduction technologies) on external energy supplies.
- Microgrid Technologies: providing independent operation of the main grid during power outages and disruptions.
- Energy Recovery Technologies: harnessing waste energy and convert it into usable power.
- Materials Science: advances in materials science (e.g., battery materials, superconductors, smart materials, etc.) can lead to more efficient energy generation, storage, and distribution technologies.
- Systems Engineering: designing and managing complex energy systems, ensuring their resilience under various operating conditions and threats.
- Blockchain Technology: enabling secure energy transactions and promote decentralised energy systems.

2. DATA AND INFORMATION SECURITY CHALLENGE

Challenge Statement: In our interconnected world, reliable data and information is society's backbone. The secure and trustworthy generation, exchange, computation, and verification of data and information are vital for both societal resilience as well as Allied defence and security. As interactions among computing systems, robots, and humans become more ubiquitous and complex, the attack surface expands dramatically, posing significant risks for commerce, social fabric, and democracy. To address these risks requires dual-use solutions that ensure the safe production, utilization, distribution, and protection of data and information. This need is particularly critical in multi-domain environments, which include diverse devices, transmission pathways, physical contexts, and operational concepts for both civilian and miliary applications.

Example Scenarios: In a civilian context, a social media platform could use advanced AI algorithms to detect and counter disinformation and misinformation threats, ensuring the integrity of information shared and protecting users from false narratives. This could be particularly crucial during election periods, when the spread of false information could have significant societal impacts. In a military scenario, the same technology could be used in an information warfare context, detecting and countering enemy disinformation campaigns aimed at disrupting operations or undermining morale. The system could also safeguard data used in AI systems, ensuring the integrity and accuracy of the data, and protecting it from unauthorized access, manipulation, and breaches. In both scenarios, the technology would provide a robust defense against the spread of false information, ensuring the integrity of data and information security.

This challenge invites innovators to propose a wide range of potential solutions, including hardware, software, or combinations of both, and spanning from components to complete systems. We encourage innovators to think creatively and innovatively about the potential applications of dual-use data and information security technologies.

Exemplar Descriptive Attributes: The Data & Information Security Challenge seeks to develop innovative solutions for secure generation, transmission, storage and exploitation of information as well as support for rapid integration of heterogenous systems that may:

- Enhance the security and trustworthiness of data generation, exchange, and computation across disparate devices and systems in multi-domain environments.
- Develop advanced low-power encryption methods, such as homomorphic systems, that ensure data security while maintaining computational efficiency.
- Create innovative security architectures (e.g., zero-trust models) that provide robust protection against a dynamic and escalating threat landscape.
- Design and structure networks (decentralised vs. centralised) to provide optimal capabilities in data production, utilisation, distribution, and protection.
- Develop non-traditional uses of quantum technology such as disruptive applications including quantum-assured positioning to support operations in GNSS denied environments, ultra-precise timekeeping for revolutionising global network synchronisation, and space-based applications.
- Provide resilience for high data rate communications, navigation, remote sensing, and beyond are of particular interest via space-based assets.
- Safeguard data used in artificial intelligence systems ensuring the integrity, accuracy, and privacy of the data, as well as protecting it from unauthorised access, manipulation, and breaches.
- Develop methods for detecting and countering disinformation and misinformation threats, especially those driven by generative methods.

Potential Enabling Technologies and Technical Approaches: May include, but are not limited to the following:

- Quantum and Post-Quantum Cryptography: secure data and prevent it from being intercepted or altered, and advance new algorithms against potential attacks from quantum computers.
- Artificial Intelligence (AI) and Machine Learning (ML): examples include predictive analytics, anomaly detection, privacy protection, intelligent authentication, AI-driven encryptions, etc.
- Data Assurance: ensure data integrity, privacy protection, compliance, trust, prevention of malicious activities for AI-enabled systems.
- Edge Computing: push data processing to the edge of the network, closer to the source of the data such as, IoT devices, autonomous vehicles, space-based systems and satellites and smart cities.
- Blockchain Technology: provide a decentralised and secure way for data sharing and data storage, supply chain management, smart contracts, voting systems, etc.
- Homomorphic Encryption: allow computations to be carried out on encrypted data, without requiring access to the decryption key.
- Biometrics: use unique physical or behavioral characteristics for secure access control, identity verification, authentication, etc.
- Zero-Knowledge Proofs: enable provability without conveying any information apart from the fact they know the value.
- Cyber Deception Technology: use of decoys or deception technology to detect, analyse, and defend against cyber-attacks.
- Deepfake Detection Technology: use advanced machine learning algorithms to analyze multi-modal data to identify if the content has been manipulated or artificially created.

3. SENSING AND SURVEILLANCE

Challenge Statement: The Alliance operates in an environment in which sensing technologies are pervasive, ranging from Internet-of-Things (IoT) devices to space-based Earth observations and cellular biomarker detection. Sensing broadly involves the detection, measurement, monitoring, and analysis of physical or behavioural attributes across various domains. Surveillance refers to the systematic observation of physical domains, places, or things using a variety of sensors, including optical, radio, acoustic, and magnetic.

These sensor and surveillance technologies play a critical role in military operations, enabling forecasting, early warning, situational awareness, post-action assessment, decision-making, and population behaviour analysis. In complex defence and security missions, personnel often operate in challenging dynamic scenarios and adverse environmental conditions, such as bad weather or rugged landscapes. Military environments are often hostile and contested, with electromagnetic and cyber-attacks being common. To navigate these challenging scenarios, interconnected multimode sensors are typically deployed. These sensors improve situational awareness, identify potential threats, and monitor the position and status of platforms and personnel in the mission area.

Example Scenarios: In a military context, a network of interconnected IoT devices and sensors could be deployed across a battlefield to monitor enemy movements, detect potential threats, and provide real-time situational awareness, enhancing decision-making capabilities. These sensors could range from ground-based devices to aerial drones and space-based satellites, providing a comprehensive view of the operational environment. In a civilian context, a similar network could be used in a smart city setup, where sensors and IoT devices monitor traffic flow, air quality, energy usage, and other key metrics. This data could be used to optimize city services, improve sustainability, and enhance the quality of life for residents. In both scenarios, the integration of various sensing modalities and advanced data analysis algorithms would be crucial for extracting meaningful information from the vast amounts of data generated.

These examples illustrate the potential applications of sensing and surveillance technologies in various challenging environments, but they are not exhaustive. We encourage innovators to think creatively about the potential dual-use innovative solutions to sensing and surveillance across multiple domains.

Exemplar Descriptive Attributes: The aim of the Sensing and Surveillance Challenge is to develop innovative (hardware, software, algorithms) solutions that may:

- Enhance the capabilities of multi-modal sensing technologies, improving their accuracy, range, and reliability in various dynamic complex operating conditions.
- Improve the efficiency and effectiveness of interconnected interoperable multiple sensor systems, enabling them to monitor large complex areas with greater detail and accuracy.
- Develop advanced algorithms for signal/image processing, big data analysis and interpretation for improving the ability to extract meaningful information from large volumes of distributed sensing and surveillance data.
- Advance the integration of various disparate sensing modalities and surveillance technologies, creating comprehensive systems that can provide a complete and more accurate picture of the operating environment.
- Use autonomy to enable real-time data collection and analysis, optimise the use of multimode sensors, and enhance decision-making capabilities in various dynamic operational environments.
- Innovate and expand the use of wearable sensing technologies, enhancing the ability to monitor and track personnel in real-time, ensuring their safety and well-being in various operational environments.

- Enhance environmental sensing and surveillance capabilities, enabling continuous monitoring and data collection.
- Ensure the responsible use of sensing and surveillance technologies, balancing the need for security and efficiency with respect for privacy and human rights.

Potential Enabling Technologies and Technical Approaches: May include, but are not limited to the following:

- Advanced Sensing Technologies: examples include space-based sensors, biometric sensors, IoT devices, quantum sensors, CBRNE detectors, etc.
  - Space-Based Remote Sensing: monitor Earth's surface and atmosphere, providing valuable data for weather forecasting, climate research, disaster management, and military surveillance.
  - Biometric Sensing: use advanced biometrics to provide secure and reliable methods for identifying individuals based on unique physical or behavioural characteristics.
  - Wearable Devices: monitor human health/fitness/performance/recovery, smart clothing for monitoring biometric and environmental data, etc.
  - Internet of Things (IoT): connect multiple devices and sensors for management and logistics, smart homes, healthcare, agriculture and environment.
  - Data Analysis and Interpretation: involve the use AI/ML algorithms to analyse and interpret large volumes of data, especially multi-modal and multi-domain data.
  - CBRNE Detection Technology: use to identify and mitigate potential threats and monitor and respond to industrial accidents and natural disasters (e.g., toxic industrial chemicals and energetic materials).
- Quantum Materials: can be used to develop high sensitivity and precision sensors for detection, navigation, communications.
- Novel Materials for Sensing: examples include smart materials, nanomaterials, biodegradable materials, photonic crystals, graphene, etc.
- Drone Surveillance: autonomous platforms with multi-modal sensing capabilities for monitoring the environment and sensing dangerous or hard-to-reach areas.
- Augmented Reality (AR): can overlay digital information onto the real world and provide enhanced situational awareness, remote surveillance, navigation and mapping, disaster response, telemedicine, etc.
- Next-Generation Wireless Technologies: support high-speed transmission and security of data from a vast network of sensors and devices, applicable in smart city infrastructure and real-time military operations.
- Secure Sensor Data Transmission and Storage System: enhance the security of the sensing and surveillance operations but also ensure the integrity and confidentiality of the data, thereby enabling decision-making based on reliable and accurate data.
- Intelligent Resource Allocation and Planning System: use AI/ML algorithms to analyse the data from the sensors and make predictions in a timely manner about the future state of the operational and tactical environment then allocate resources and plan their usage in an optimal and environmentally efficient way.

4. HUMAN HEALTH & PERFORMANCE

Challenge Statement: Human health and performance is a multifaceted issue that intersects human health, wellbeing, performance, and recovery, covering both physical and psychological aspects. This challenge seeks to stimulate innovative dual-use solutions that enhance our understanding and monitoring of human health and performance in extreme and complex environments such as military operations, disaster relief, sports and athletics, and space exploration. Addressing this challenge necessitates the integration of advancements in neuroscience, material science, and artificial intelligence to facilitate real-time monitoring and predictive analysis of physical and psychological stress loads, prevent performance degradation and injury, and oversee recovery and recuperation. The health data can then be used to implement tailored health and wellbeing interventions for individuals or groups, such as through precision medicine or customised training.

Example Scenarios: In a high-stress combat situation, a soldier might suffer a severe injury leading to significant blood loss. Wearable technology could monitor the loss of blood in real-time and alert the medical team for immediate intervention. It could also predict the rate of blood loss based on the severity of the injury and the soldier's vital signs, enabling the medical team to prepare for a potential blood transfusion. In the context of space exploration, astronauts are exposed to extreme conditions that can have significant impacts on their physical and psychological health. An AI-enabled wearable device could continuously monitor and collect data on the astronaut's vital signs, physical exertion, cognitive load, and psychological stress levels. Based on their current health status and recovery progress, it could suggest adjustments to diet, exercise routine, or work schedule. It could also provide psychological support by recommending stress management techniques or facilitating communication with a mental health professional.

These scenarios are illustrative examples and not exhaustive of possible applications. We encourage innovators to think creatively about the potential dual-use innovative solutions to human health, wellbeing, performance, and recovery.

Exemplar Descriptive Attributes: The aim of the Human Health & Performance Challenge is to develop innovative solutions that may:

- Integrate of advancements in neuroscience, material science, AI, autonomy and other relevant fields.
- Provide real-time monitoring and prediction of physical and psychological stress load (i.e., stress load analysis).
- Incorporate data-driven decisions and prediction that can lead to more effective and personalized heath management (e.g., bioinformatics).
- Utilise advanced software and hardware systems, including low-power consuming wearable technologies and next-generation algorithmic systems.
- Can operate under extreme conditions (e.g., high-stress, high-demand) and complex environments (e.g., severe weather, space).
- Can be used with minimal obtrusiveness, training and set-up required for operation and have compact and portable form factor for ease of deployment and use.

Potential Enabling Technologies and Technical Approaches: May include, but are not limited to the following:

- Next-Gen Wearable Technologies: examples include lightweight, non-intrusive, ultra-low power, high accuracy physiological detectors and sensors; flexible materials with embedded electronic;

wearable biosensors, self-powered or body-power generated devices; and wearables that synchronise across users in complex environments.

- Personalised Healthcare: examples include additively manufactured prosthetics and other equipment, pharmaceutical or vaccine modelling, digital twins, regulated health applications, and tele-medicine.
- Bio-Inspired Technologies: examples include biomaterials for tissue engineering and drug delivery, bio-manufacturing, wearable biosensor, and food storage and transport.
- Advanced Exoskeletons and Prosthetics: can enhance physical performance and aid in recovery and recuperation.
- AI and Autonomy Enabled Technologies:
    - Digital Healthcare: examples include tele-medicine, digital twins, VR training systems, AR training systems, image analysis software, predictive and regulated health applications.
    - Multimodal Biomedical AI: combine multiple types of biomedical data using AI, such as medical imaging, electronic health records, genomics, and other biological data, to improve the diagnosis, prognosis, and treatment of diseases.
    - Human Agent Teaming Technology: enhance healthcare delivery and patient outcomes via collaboration between humans and AI systems or robots with tasks ranging from patient monitoring, data analysis, precise surgical procedures and rehabilitation support.
    - Human-Computer Interaction (HCI) Technology: can be used to develop advanced health monitoring system (e.g., real-time tracking of vital signs and early detection of potential health issues) and to create virtual or augmented reality-based therapies and exercises, improving physical and cognitive performance through personalised, interactive experiences.
    - Predictive Modelling: can analyse vast amounts of health data to predict disease patterns, enabling early interventions and personalised treatment plans and can also be used to predict athletic performance based on training data, helping athletes optimise their routines and prevent injuries.
    - Autonomous Systems: examples include remote robotic surgery, medical drones to deliver blood and other needed medicine, robots and drones to support search and rescue operations in disaster-stricken areas.
- Chemical, Biological, Radiological and Nuclear (CBRN) Detection and Defence: examples include use of personal protective equipment (PPE), decontamination methods, and medical treatments.
- Materials Science and Engineering: examples include smart fabric technology and material reducing heat-induced stress and failure risk while increasing performance, functionality, and safety.

5. CRITICAL INFRASTRUCTURE & LOGISTICS

Challenge Statement: The interconnection between critical infrastructure and supply chains presents a complex challenge due to their mutual vulnerabilities and risks. Vulnerability in a power grid or water supply system, critical infrastructures required for supply chain operations, could open the door to a successful cyber-attack that disrupts manufacturing processes, transportation systems, and last-mile supply. Natural disaster or geopolitical tensions can disrupt regional or global supply and value chains, and render a power grid vulnerable to failures. The interconnected nature of infrastructure and supply chains requires a systems approach when addressing potential risks from cyberattacks and terrorism, aging and brittle infrastructure, and natural disaster and climate change impacts. This includes measures like infrastructure and supply chain hardening and resilience, climate change monitoring, natural disaster prediction, protection of critical remote (e.g. underwater) national infrastructure, early warning systems, and real-time transportation infrastructure monitoring. Responses to this challenge should address the particular complexity of the risks, and consider the potential impacts on economic security, public health and safety, and national defence.

Example Scenarios: In a defense and security context, the interconnectedness of critical infrastructure and supply chains could be exploited by adversaries to disrupt military operations. For instance, a cyber-attack on a power grid could halt the production and transportation of essential military supplies. To counter this, advanced cyber-physical security measures and resilient infrastructure could be implemented, ensuring the continuity of supply chain operations even under threat. In a civilian context, a natural disaster could disrupt critical infrastructure such as power grids and transportation systems, affecting supply chains and causing shortages of essential goods. To mitigate this, predictive capabilities and real-time monitoring systems could be used to anticipate natural disasters and implement contingency plans, ensuring the resilience of supply chains. In both scenarios, the interconnected nature of infrastructure and supply chains requires a systems approach to risk management, emphasizing infrastructure hardening, resilience, and rapid response to incidents.

These scenarios are illustrative examples and not exhaustive of possible applications. We encourage innovators to think creatively about the potential dual-use innovative solutions to critical infrastructure and supply chains

Exemplar Description Attributes: The aim of the Critical Infrastructure & Logistics Challenge is to develop innovative solutions that may:

- Advance infrastructure hardening and resilience. This can be achieved through:
  - Enhancing the capabilities of cyber-physical security
  - Rapidly assessing and repairing infrastructure
  - Discovering vulnerabilities and risks, and more generally support risk assessment/management.
  - Monitoring climate change effects and predict natural disaster
  - Providing real-time threat/incident detection and response
  - Providing early warning systems and communications
  - Advancing capabilities for modelling vulnerabilities, risks and solutions
- Operate in various environments, including remote or disaster-hit regions, maritime, underwater, land, and space.
- Prioritise technologies that can integrate rapidly into existing systems (e.g., IT system) for ease of adoption.

- Redesign critical infrastructure and logistics for resilience leveraging predictive capabilities and edge computing for faster and timely decision making in critical situations.
- Counter disinformation and prevent the spread of false information that could lead to panic or damage.
- Manage the complexity of an interconnected critical local, national and/or global infrastructures.
- Have the right health supplies and countermeasures available when needed to combat pandemics and CBRN emergencies.
- Mange supply chain risks that involve identifying, assessing, and mitigating potential vulnerabilities or disruptions to ensure business continuity and maintain the integrity of products and services.

Potential Enabling Technologies and Technical Approaches: May include, but are not limited to the following:

- IoT Technologies: connecting multiple devices and sensors to provide real-time monitoring and control and to aid predictive maintenance, automating re-supply, enable interoperability and communication between different organisations, and applications to provide early warnings to the emergency services or other relevant stakeholders.
- Component Integration: examples include effective integration of sensors into existing infrastructure and cyber-physical components and components for complex infrastructure inspection.
- Advanced Decentralised Data-Driven Logistics: examples include blockchain and distributed ledger technologies.
- Autonomy: examples include automated cyber security, drone surveillance, intelligent sensors, self-driving vehicles, automated unmanned vehicle (e.g. aircraft system) traffic management, increased degrees of freedom robotic arms and improved precision robotic systems.
- Underwater Cables Protection Technology: examples include vehicles that can carry out surveillance and/or detection under water, incident reporting software, on-chip cold-atom gravimeters, digital terrain correlation, acoustic and optical imagery, magnetic and electrical resistivity contrasts detecting methods, ultra-low frequency detection methods, components and systems that can survive at 6000 m depths.
- Climate Change Monitoring Technology: examples including using AI and machine learning to analyse data on spacecraft, spacecraft instrument / component miniaturisation, software to collate, visualise and store climate change data and surveillance drones with advanced sensors and geo-positioning systems.
- Data Analysis and Interpretation: examples involving the use of AI/ML algorithms to analyse and interpret large volumes of data, to enable natural disaster prediction, understand climate change effects, maintenance prediction, re-supply prediction, counter disinformation, mine data to replace proxies in life-cycle assessment, map complex and dynamic supply-chain pathways and discover vulnerabilities and risks.
- Material and Manufacturing Development: examples include radiation hardened materials for both nuclear and space-based critical infrastructure, corrosion resistant materials, materials and packaging methods for air-portable surveillance systems, low-carbon materials, and reliable joining processes.
- In-Situ Repair Technologies: examples include self-healing meta materials, self-healing networks that automatically detect and fix faults and direct energy deposition (DED) additive manufacturing.
- Alternate Power Supplies: examples include wireless power transmission, battery storage, modular generators or microgrids.
- Effective Communication: examples include 6G, data visualisation tools, secure mesh communication networks that can connect with multiple organisations, adaptive data compression, optical communication, hybrid spread spectrum systems, reconfigurable antennas, reconfigurable

intelligent surfaces / intelligent reflective services, digital twins, concurrent design facilities, interactive training software, and relay communications using drones or buoys.

- Modelling Capabilities: examples include improving the efficiency, computational effort, accuracy and other factors of models for areas such as transport, acoustic propagation, advanced manufacturing, additive manufacturing qualification, drug discovery, pandemics and energy demand through quantum computing, machine learning and other disruptive technologies.