Destination - Resilient Infrastructure

Proposals for topics under this Destination should set out a credible pathway to contributing to the following expected impact of the Horizon Europe Strategic Plan 2021-2024: *"[...] resilience and autonomy of physical and digital infrastructures are enhanced and vital societal functions are ensured, thanks to more powerful prevention, preparedness and response, a better understanding of related human, societal and technological aspects, and the development of cutting-edge capabilities for [...] infrastructure operators [...]"*

More specifically, proposals should contribute to the achievement of one or more of the following impacts:

- Ensured resilience of large-scale interconnected systems infrastructures and the entities that operate them in in case of complex attacks, pandemics, natural and human-made disasters, or the impacts of climate change;
- Upgraded systems for resilience of the operators and the protection of critical infrastructure to enable rapid, effective, safe and secure response and without substantial human intervention to complex threats and challenges, and better assess risks ensuring resilience and open strategic autonomy of European infrastructures;
- Resilient and secure smart cities are protected using the knowledge derived from the protection of critical infrastructures and systems that are characterised by growing complexity.

The capabilities built by research and innovation in this Destination would clearly be relevant to be better prepared for potential future challenges to European internal security and crises as the ones in Ukraine in 2022.

Where possible and relevant, synergy-building and clustering initiatives with successful proposals in the same area should be considered, including the organisation of international conferences in close coordination with the Community for European Research and Innovation for Security (CERIS) activities and/or other international events.

The following call(s) in this work programme contribute to this destination:

Call	Budgets (EUR million)		Deadline(s)
	2023	2024	
HORIZON-CL3-2023-INFRA-01	14.50		23 Nov 2023
HORIZON-CL3-2024-INFRA-01		16.00	20 Nov 2024
Overall indicative budget	14.50	16.00	

Call - Resilient Infrastructure 2023

HORIZON-CL3-2023-INFRA-01

Conditions for the Call

Indicative budget(s)[68]

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per project (EUR million)[69]	Indicative number of projects expected to be funded
		2023		
Opening: 29 Jun 2023 Deadline(s): 23 Nov 2023				
HORIZON-CL3-2023-INFRA-01-01	IA	5.00	Around 5.00	1
HORIZON-CL3-2023-INFRA-01-02	IA	9.50	Around 4.75	2
Overall indicative budget		14.50		

General conditions relating to this call	
Admissibility conditions	The conditions are described in General Annex A.
Eligibility conditions	The conditions are described in General Annex B.
Financial and operational capacity and exclusion	The criteria are described in General Annex C.
Award criteria	The criteria are described in General Annex D.

[68] The Director-General responsible for the call may decide to open the call up to one month prior to or after the envisaged date(s) of opening.
The Director-General responsible may delay the deadline(s) by up to two months.
All deadlines are at 17.00.00 Brussels local time.
The budget amounts are subject to the availability of the appropriations provided for in the general budget of the Union for years 2023 and 2024.

[69] Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.

Documents	The documents are described in General Annex E.
Procedure	The procedure is described in General Annex F.
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G.

INFRA01 – Improved preparedness and response for large-scale disruptions of European infrastructures

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-INFRA-01-01: Facilitating strategic cooperation to ensure the provision of essential services

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 5.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 5.00 million.
Type of Action	Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 3 government authorities responsible for resilience on national level and / or for overseeing operators, from at least 3 different EU Member States. For these participants, applicants must fill in the table “Information about security practitioners” in the application form with all the requested information, following the template provided in the submission IT tool. If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). In order to achieve the expected outcomes, and safeguard the Union’s strategic assets, interests, autonomy, or security, namely to protect and

	to preserve the confidentiality of risk assessments and of the vulnerabilities of critical entities of Member States, participation is limited to legal entities established in Member States only. Proposals including entities established in countries other than EU Member States will be ineligible.
Technology Readiness Level	Activities are expected to achieve TRL 6-8 by the end of the project – see General Annex B.
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G. The following exceptions apply: Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025). [70].
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Outcome: Projects' results are expected to contribute to all of the following outcomes:

- Tools for EU Member State authorities and operators for the assessment and anticipation of relevant risks to the provisions of essential services are identified;
- The cooperation between authorities of EU Member States is facilitated by providing solutions for data exchange and joint cross-border risk assessments;
- Simulation tools are developed for large-scale exercises to test the resilience of operators and of specific sectors, and related training courses are designed;
- Measures by Member State authorities to facilitate risk assessments by operators are identified, including the assessment of dependencies on different sectors and cross-border interdependencies;
- Provide common European guidance and support for the drafting of their resilience plans in order to meet all the provisions of the proposed CER-Directive: risk analysis, domino

[70] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

effects, cross-sector and cross-border analysis, standardised plans, educational and training tools;

- An all-hazards framework is created to support Member States in ensuring improved concepts and instruments for the anticipation of risks to entities that provide essential services, resulting in an improved preparedness and response against disruptions of key sectors in the EU and enhanced resilience of the EU internal market.

Scope: The EU Security Union Strategy for 2020-2025[71], Counter-Terrorism Agenda[72]. for the EU and the Cyber Security Strategy stress the importance of ensuring resilience in the face of various risks. The livelihoods of European citizens and the good functioning of the internal market depend on the reliable provision of services fundamental for societal or economic activities in many different sectors. Those services often are reliant upon one another, thus disruptions in one sector can generate severe and long-lasting effects on the provision of services in others.

Member States hold the primary responsibility in ensuring that operators who use critical infrastructures to deliver such services (hereafter: 'operators') comply with applicable rules and have the necessary support to ensure their own resilience and as part of a complex system of interdependencies. On EU-level, there has been a revision of certain legislation aiming at the minimum harmonisation of such rules, such as the directive on the resilience of critical entities (CER[73]) and the directive on measures for high common level of cybersecurity across the Union (NIS-2[74]). In combination with sectoral EU-legislation and policies on resilience (e.g. for a Network Code on sector-specific rules for cybersecurity aspects of cross-border electricity flows[75]), this provides a comprehensive framework that needs to be put in practice.

"Facilitating strategic cooperation" refers to the necessity for public authorities of the Member States to be able to exchange information, in a secure way, on the risk assessments of their critical entities as well as their resilience. "Critical entities" is the specific term used in the CER directive to designate those entities that will be identified by the Member States under the directive. Pursuant to the directive, in particular of its articles 1 and 5, the identity of the critical entities will be classified. In the performance of the project, project participants will interact directly with Member States authorities responsible for risk assessment and analysis of the vulnerabilities of their critical entities. Pursuant to the proposed directive, the confidentiality of the critical entities (and of their vulnerabilities) shall be ensured and protected.

---

71 COM(2020) 605 final.

72 COM(2020) 795 final

73 Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

74 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

75 Revised Network Code on Cybersecurity (NCCS)_1.pdf.

Proposals under this topic should support the competent authorities of Member States to identify and develop the most suitable tools, solutions and strategies to ensure the resilience of key sectors and thus facilitate the implementation of [related/ future] EU legislation.

Applicants should focus on delivering solutions that can be used by the competent authorities of EU Member States, to support their task in overseeing the resilience of key sectors in line with relevant EU rules. Such solutions should enhance their ability for cooperation and communication, conducting large-scale risk assessments (including the cross-border dimension), developing best practices for exercises and dedicated complex training modules. The proposals should address the development of improved concepts and instruments for the anticipation and management of strategic risks, strengthening governance framework and enhancing coordination between different authorities.

It is recommended that proposals develop concrete tools to support all-hazard analysis by integrating domain specific risk assessment and allowing to manage interdependencies phenomena among different sectors and Member States. Possible examples are virtual reality tools, dashboards, complex training and serious gaming modules or other instruments to be used and that currently may not exist on such scale.

Proposals should aim to cover the largest possible number of sectors described in the respective Annexes of the directive on the resilience of critical entities (CER) and the directive on measures for high common level of cybersecurity across the Union (NIS-2). The inclusion of associations representing private or public operators in specific sectors, or across sectors on EU- or national level, is encouraged.

In this topic the integration of the gender dimension (sex and gender analysis) in research and innovation content should be addressed only if relevant in relation to the objectives of the research effort.

Projects are expected to outline how results are fed into the work of relevant Commission expert groups – [for example the Critical Entities Resilience Group (CERG) and the NIS-2 Cooperation Group] – and to explore synergies with the actions undertaken by relevant EU agencies.

HORIZON-CL3-2023-INFRA-01-02: Supporting operators against cyber and non-cyber threats to reinforce the resilience of critical infrastructures

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 4.75 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 9.50 million.
Type of Action	Innovation Actions

Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used). The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 3 infrastructure operators, which could include civil protection authorities, at national level from at least 3 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool.
Technology Readiness Level	Activities are expected to achieve TRL 6-8 by the end of the project – see General Annex B.
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G. The following exceptions apply: Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025). [76].
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Support is provided to the resilience of operators against cyber and non-cyber threats in specific sectors;

[76] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

- A reliable state-of-the-art analysis of physical/cyber detection technologies and risk scenarios is created, in the context of an operator in a specific sector in sectors that have not yet been covered by previous research projects;

- Strengthened cooperation against natural or human-made threats and subsequent disruptions of infrastructures in Europe, allowing for operational testing in real scenarios or realistic simulations of scenarios with specific regard to disruptions in a specific sector of critical entities;

- Improved situational awareness, preparedness and governance by the implementation of effective solutions that enhance detection and anticipated projection of a determined threating situation, as well as implementation of prevention, preparedness/mitigation, response, and recovery types of intervention;

- Significant reduction of risks and exposures to anomalies or deliberate events on cyber-physical systems, or on complex and critical infrastructures/systems;

- Enhanced preparedness and response by definition of operational procedures of operators as well as public authorities considering citizen's behaviour/reaction and societal impact in case of disruption in a specific sector.

Scope: The operational environment in which operators operate has changed significantly in recent years. Security research and innovation related to infrastructure resilience has been following a sectorial approach in order to increase the resilience. This approach to critical infrastructure resilience is needed that as it reflects the current and anticipated future risk landscape, the increasingly tight interdependencies between different sectors, and also the increasingly interdependent relationships between physical and digital infrastructures.

A disruption affecting the service provision by one operator in one sector has the potential to generate cascading effects on service provision in other sectors, and also potentially in other Member States or across the entire EU.

With more and more infrastructure systems being interconnected, a stronger focus on the systemic dimension and complexity of attacks and disruptions by cyber or physical means needs to be applied. As such, not only interdependencies within one type of infrastructure (or closely related types) can be taken into account. The risk landscape is more complex in the recent years, involving natural hazards (in many cases exacerbated by climate change), state-sponsored hybrid actions, terrorism, insider threats, pandemics, and accidents (such as industrial accidents).

Physical disruptions of the activities of operators active in these sectors have possibly serious negative implications for citizens, business, governments, in the environment and endanger the smooth functioning of the internal market. Therefore, operators should be equipped with the best possible means to be able to prevent, resist, absorb and recover from disruptive incidents, no matter if they are caused by natural hazards, accidents, terrorism, insider threats, or public health emergencies.

Another important issue is to have in place efficient cybersecurity measures to block the access to critical infrastructures. A possible project focusing on the protection of critical infrastructures against such threat should consider gaps and vulnerabilities that need to be identified and overcome (e.g. protection of drinking water supply systems from high chemical levels, nuclear facilities, etc.).

Therefore, the successful proposal, following a sector-based approach and identifying a specific priority sector, should work on how to increase the combined cyber and non-cyber resilience operators. It should do so by orienting itself on sectors that have not been covered in previous research, out of the list of sectors described in the respective Annexes of the of the directive on the resilience of critical entities (CER[77]) and the directive on measures for high common level of cybersecurity across the Union (NIS-2[78]) and thus contribute to enhancing the overall resilience on EU-level, in line with the EU Security Union Strategy[79].

The proposal should orient itself on the policy shift from protection towards resilience and thus focus on operators acting in the internal market, rather than only on physical or digital assets. This includes concepts of wider business continuity, as well as logistics and supply-chains. Proposals should also focus on the development of a more effective resilience plan conception method, which shall support operators to draft their resilience plans according to the provisions of the CER and NIS-2 Directives. The resilience plan conception method should include risk analysis, domino effects analysis, cross-sector and cross-border analysis, standardised plans etc. In addition, this method could include measures on adequate protection, measures on prevention, response, mitigation, and recovery from the consequences of incidents, protection of classified (e.g. the proposal for a Network Code on sector-specific rules for cybersecurity aspects of cross-border electricity flows) or sensitive information and measures that ensure adequate employee security management.

The main practitioners in this topic should come from private or public operators, meaning organisations and enterprises that use critical infrastructure to deliver services, vital for the functioning of society and the internal market. Consortia that will include MS public entities would be considered as an asset. Competent authorities of MS in charge of resilience and/ or overseeing operators in one or more sectors are also encouraged to join the consortia of applicants.

If the infrastructure includes processing of personal data, the proposal should consider including a risk assessment or privacy impact of individuals and society.

This topic requires the effective contribution of SSH disciplines and the involvement of SSH experts, institutions as well as the inclusion of relevant SSH expertise, in order to produce

---

77 Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

78 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

79 COM(2020) 605 final.

meaningful and significant effects enhancing the societal impact of the related innovation activities.

Applicants are encouraged to explore and demonstrate synergies with the work conducted in the European Reference Network for Critical Infrastructure Protection (ERNCIP), as applicable.

Call - Resilient Infrastructure 2024

HORIZON-CL3-2024-INFRA-01

Conditions for the Call

Indicative budget(s)[80]

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per project (EUR million)[81]	Indicative number of projects expected to be funded
		2024		
Opening: 27 Jun 2024 Deadline(s): 20 Nov 2024				
HORIZON-CL3-2024-INFRA-01-01	IA	5.00	Around 5.00	1
HORIZON-CL3-2024-INFRA-01-02	IA	6.00	Around 6.00	1
HORIZON-CL3-2024-INFRA-01-03	RIA	5.00	Around 5.00	1
Overall indicative budget		16.00		

General conditions relating to this call	
Admissibility conditions	The conditions are described in General Annex A.
Eligibility conditions	The conditions are described in General

[80] The Director-General responsible for the call may decide to open the call up to one month prior to or after the envisaged date(s) of opening.
The Director-General responsible may delay the deadline(s) by up to two months.
All deadlines are at 17.00.00 Brussels local time.
The budget amounts are subject to the availability of the appropriations provided for in the general budget of the Union for years 2023 and 2024.

[81] Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.

	Annex B.
Financial and operational capacity and exclusion	The criteria are described in General Annex C.
Award criteria	The criteria are described in General Annex D.
Documents	The documents are described in General Annex E.
Procedure	The procedure is described in General Annex F.
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G.

INFRA01 – Improved preparedness and response for large-scale disruptions of European infrastructures

Proposals are invited against the following topic(s):

HORIZON-CL3-2024-INFRA-01-01: Open Topic

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 5.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 5.00 million.
Type of Action	Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 2 critical infrastructure operators and 2 civil protection authorities from at least 3 different EU Member States or Associated Countries. For these participants, applicants must fill in the table “Information about security practitioners” in the application form with all the requested information, following the template provided in the submission IT tool. If projects use satellite-based earth observation, positioning, navigation

	and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology Readiness Level	Activities are expected to achieve TRL 6-8 by the end of the project – see General Annex B.
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G. The following exceptions apply: Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025). [82].
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Outcome: Projects' results are expected to contribute to all of the following outcomes:

- Critical infrastructure operators are more resilient to threats and natural and human-made hazards;
- Improved monitoring, risk assessment, forecast, mitigation and modelling techniques aimed at increasing the resilience of critical infrastructures, validating multi-hazard scenarios, creating interactive hazard maps supported by Earth Observation and other data sources.

Scope: Under the Open Topic, proposals are welcome to address new, upcoming or unforeseen challenges and/or creative or disruptive solutions for increasing the resilience of critical infrastructure, that are not covered by the other topics of Horizon Europe Calls Resilient Infrastructure 2021-2022, Resilient Infrastructure 2023 and Resilient Infrastructure 2024.

Adapted to the nature, scope and type of proposed activities, proposals should convincingly explain how they will plan and/or carry out demonstration, testing or validation of developed tools and solutions. Proposals should also delineate the plans to develop possible future uptake and upscaling at local, national and EU level for possible next steps after the project.

[82] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

In this topic the integration of the gender dimension (sex and gender analysis) in research and innovation content should be addressed only if relevant in relation to the objectives of the research effort.

Proposals should consider, build on if appropriate and not duplicate previous research, including but not limited to research by other Framework Programmes' projects. When applicable, the successful proposal should build on the publicly available achievements and findings of related previous national or EU-funded projects.

INFRA02 – Resilient and secure urban areas and smart cities

Proposals are invited against the following topic(s):

HORIZON-CL3-2024-INFRA-01-02: Resilient and secure urban planning and new tools for EU territorial entities

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 6.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 6.00 million.
Type of Action	Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 2 local or regional government authorities from 2 at least different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool. If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology Readiness Level	Activities are expected to achieve TRL 6-8 by the end of the project – see General Annex B.
Legal and financial set-up of	The rules are described in General Annex G. The following exceptions apply:

the Grant Agreements	Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025). [83].
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Outcome: Projects' results are expected to contribute to all of the following outcomes:

- Evaluation of the resilience of an urban and peri-urban environment, identification of weaknesses and recommendations for changes to organizational processes;
- Creation of new tools and cost-efficient security upgrades of urban infrastructures with possibilities of pooling and sharing of complex security systems, taking into account limited budgets of local authorities;
- Improved efficiency of the security forces and emergency services (police, firefighters, paramedics ...) for the benefit of the European citizens and residents;
- Promotion of best practices, creation of EU sovereign trusted decision support tool/solution and spreading of effective tools and capabilities across entities in different EU territories despite their size and location.

Scope: European territories are developing into more connected and complex systems of different services and infrastructures empowered by technologies and growing digitisation. This change in urban areas in Europe, brings new opportunities but also new threats for the authorities and their relationship with the citizens and residents. It is therefore critical for the resilience of our urban areas and for their citizens' wellbeing that those services are trusted and secure.

The classical large-scale infrastructures have a long tradition of implementing the principles of Safety-by-design and Security-by-design when planning their assets. However, with more and more infrastructures on the local level becoming vulnerable, security research can support their protection with new approaches in 'Security-by-design'[84]. In view of limited budgets of

[83] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

[84] See for example the handbook "Security by Design, Protection of public spaces from terrorist attacks" published by the European Commission, 2022: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC131172/JRC131172_01.pdf

many local administrations, improved knowledge as well as innovative security upgrades and processes for existing urban infrastructures equipped with advanced connectivity technologies and cooperative systems could be explored.

EU territories, despite their size and location, suffer from a lack of dedicated EU sovereign and trusted tools in order to enhance the coordination of local first responders and to improve security coverage, such as the preparation of operational staff, field intervention and predictive tools. Even though some complicated tools already exist, it is clear that there is no generic, cost effective and easy to use solutions for local authorities. Therefore, there is a need for creation of new tools that are designed in a simple manner and deployed in an effective way.

Resilient and secure urban planning tools for the development of holistic approaches that network the different organizational levels, sensor and communication levels and data rooms are very pertinent. These tools should assess the resilience of urban and peri urban territories, identify weaknesses and recommend changes to organizational processes, sensors and communication infrastructure. The secure urban and rural living spaces, technical solutions, organizational levels, and data rooms must be more closely linked. There is a clear need for a development of tools for recovery strategies and proactive foresight for urban and peri urban environments. The tactical tools should include modelling of urban centres and rural areas, predictive tools, improved global situational awareness and day-to-day planning and crisis management (e.g., simulation, training).

The proposals should include a high level of confidence in data management and sharing, provide solutions on cybersecurity issues and take on board new type of threats. The proposed solutions should suggest trusted shared architectures, trusted data collection, secure computation on the data and management processes, modelling capabilities, hypervisor supporting global situational awareness with open and trusted API’s, trusted data processing engines and, e.g., artificial intelligence tools. If the tools include processing of personal data, it should consider including a risk assessment or privacy impact of individuals and society.

The testing and/or piloting of the tools and solutions developed in a real setting and the participation of one or more relevant local authorities is an asset; regardless, actions should foresee how they will facilitate the uptake, replication across setting and up-scaling of the capabilities - i.e. solutions, tools, processes et al. – to be developed by the project.

This topic requires the effective contribution of SSH disciplines and the involvement of SSH experts, institutions as well as the inclusion of relevant SSH expertise, in order to produce meaningful and significant effects enhancing the societal impact of the related innovation activities.

HORIZON-CL3-2024-INFRA-01-03: Advanced real-time data analysis used for infrastructure resilience

Specific conditions

Expected EU contribution per project	The Commission estimates that an EU contribution of around EUR 5.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 5.00 million.
Type of Action	Research and Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: The following additional eligibility criteria apply: This topic requires the active involvement, as beneficiaries, of at least 3 infrastructure operators, which could include civil protection authorities, at national level from at least 3 different EU Member States or Associated Countries. For these participants, applicants must fill in the table "Information about security practitioners" in the application form with all the requested information, following the template provided in the submission IT tool. If projects use satellite-based earth observation, positioning, navigation and/or related timing data and services, beneficiaries must make use of Copernicus and/or Galileo/EGNOS (other data and services may additionally be used).
Technology Readiness Level	Activities are expected to achieve TRL 5-6 by the end of the project – see General Annex B.
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G. The following exceptions apply: Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025). [85].
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

[85] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Improved capabilities for risk and faulty events identification in infrastructure networks and smart cities through real-time analysis (including big data) by public and private actors via secured and trusted platforms and interconnected systems where the collaboration follows clear legal and political frameworks;
- Tools and processes for facilitating stakeholders efforts to identify, analyse, assess and continuously monitor risks and boost adaptive capacity to unexpected events risks in advance by allowing for the analysis of various data sources (e.g. audio, video, social media, web-content, spatial information, sensor or machine generated data);
- Fast and continuous real-time identification, classification and tracking of hazardous agents, contaminants or anomalies in infrastructure networks and supply-chains;
- Interoperable interfaces and improved collaboration between infrastructure operation detection and response systems, national/EU risk management/coordination centres and first responder equipment in order to allow for remote on-scene operations considering citizen knowledge;
- Increased cyber-resilience of industrial xG networks and cloud data covering specific infrastructure domains
- Improved ability to map in real-time the source(s) of risk factors that could endanger the networked infrastructure supported by Earth Observation and geolocation data. If the analysis includes processing of personal data, it should consider including a risk assessment or privacy impact of individuals and society.

Scope: Today's society is more interconnected than ever before. Telecommunication networks, transport networks, aviation, energy, water grids, finance are the backbone of today's society. Due to their exceptional complexity and size, infrastructure networks pose a specific challenge when it comes to identifying different risks, either cyber or physical. Especially in the cyber-domain, many intrusions or attacks remain unnoticed or are detected relatively late. Technological developments in areas like machine learning for analytics, user interfaces as well as storage applications have the potential to improve related capabilities.

Modern urban environments and interconnected infrastructures create constantly big amounts of data. In addition, other sources can be exploited to support the identification and analysis of risks to infrastructures. Therefore, research on enhanced risk anticipation through real-time data analysis has the potential to lead to useful tools to enhance preparedness (contingency plans, scenario-based exercises, allocation of resources, etc.).

Resilience of smart cities is marked by a set of specific requirements taking into account most notably aspects from the integration considering user centred approaches as well as social and ethical aspects of Industrial Internet of Things (IIoT), AI/ Machine Learning approaches for

real-time data analytics, ensuring transparency, sufficient knowledge and their operational challenges in this area.

While the availability of larger amounts of data from different sources offers potential to improve the identification of possible risks to infrastructures, it also increases the demand for fast and resilient analytical tools. There is a need to filter information to identify data that is relevant as an indicator for risks and - given the large number of different forms of cyber-attacks or intrusions - also a need to prioritise and decide according to the degree of danger they present. This implies the need for matching data in the appropriate context and verifying the source with a view of ensuring that only relevant data is analysed, thus avoiding false results. Faster identification and localisation of hazardous agents and contaminants inside the infrastructure networks is a key to allow for quick response, inform and involve citizens and residents as well as avoid large-scale damage of any incident. Such identification capabilities can be deployed as part of the infrastructure and integrate with the systems public authorities use to make sure information is available as soon as possible. Furthermore, it is crucial to develop methods for better cooperation between different actors to ensure a common understanding and interpretation of data and to provide interactive tools for exchange and visualisation for decision support. Cooperation between different public and private actors is essential in this regard.

This topic requires the effective contribution of SSH disciplines and the involvement of SSH experts, institutions as well as the inclusion of relevant SSH expertise, in order to produce meaningful and significant effects enhancing the societal impact of the related innovation activities.

Destination - Increased Cybersecurity

Proposals for topics under this Destination should set out a credible pathway contributing to the following impact of the Strategic Plan 2021-2024: "Increased cybersecurity and a more secure online environment by developing and using effectively EU and Member States' capabilities in digital technologies supporting protection of data and networks aspiring to technological sovereignty in this field, while respecting privacy and other fundamental rights; this should contribute to secure services, processes and products, as well as to robust digital infrastructures capable to resist and counter cyber-attacks and hybrid threats".

More specifically, proposals should contribute to the achievement of one or more of the following impacts:

- Strengthened EU cybersecurity capacities and European Union sovereignty in digital technologies
- More resilient digital infrastructures, systems and processes
- Increased software, hardware and supply chain security
- Secured disruptive technologies
- Smart and quantifiable security assurance and certification shared across the EU
- Reinforced awareness and a common cyber security management and culture.

All proposals of projects under this Destination should aim to be complementary and avoid overlaps with relevant actions funded by other EU instruments, including the European Defence Fund and its precursors (the European Defence Industrial Development Programme (EDIDP) and the Preparatory Action on Defence research (PADR)), based on the information publicly available[86] and while maintaining a focus on civilian applications only.

The following call(s) in this work programme contribute to this destination:

Call	Budgets (EUR million)	Deadline(s)

[86] *See for instance:*
- relevant work programmes of the EDF (https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf_en) and of the DEP (https://digital-strategy.ec.europa.eu/en/activities/work-programmes-digital)
And information on ongoing projects of:
- the EDF (https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/programmes/edf)
- the DEP (https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/programmes/digital);
Visit the following links for more information on past projects of the:
- EDF (https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-results;programCode=EDF)
- EDIDP (https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-industrial-development-programme-edidp_en)
- PADR (https://defence-industry-space.ec.europa.eu/eu-defence-industry/preparatory-action-defence-research-padr_en).

	2023	2024	
HORIZON-CL3-2023-CS-01	58.70		23 Nov 2023
HORIZON-CL3-2024-CS-01		60.40	20 Nov 2024
Overall indicative budget	58.70	60.40	

Call - Increased Cybersecurity 2023

HORIZON-CL3-2023-CS-01

Conditions for the Call

Indicative budget(s)[87]

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per project (EUR million)[88]	Indicative number of projects expected to be funded
		2023		
Opening: 29 Jun 2023 Deadline(s): 23 Nov 2023				
HORIZON-CL3-2023-CS-01-01	IA	28.00	4.00 to 6.00	4
HORIZON-CL3-2023-CS-01-02	IA	15.70	2.00 to 4.00	4
HORIZON-CL3-2023-CS-01-03	RIA	15.00	4.00 to 6.00	2
Overall indicative budget		58.70		

General conditions relating to this call	
Admissibility conditions	The conditions are described in General Annex A.
Eligibility conditions	The conditions are described in General Annex B.
Financial and operational capacity and exclusion	The criteria are described in General Annex C.
Award criteria	The criteria are described in General Annex

87 The Director-General responsible for the call may decide to open the call up to one month prior to or after the envisaged date(s) of opening.
The Director-General responsible may delay the deadline(s) by up to two months.
All deadlines are at 17.00.00 Brussels local time.
The budget amounts are subject to the availability of the appropriations provided for in the general budget of the Union for years 2023 and 2024.

88 Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.

	D.
Documents	The documents are described in General Annex E.
Procedure	The procedure is described in General Annex F.
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G.

CS01 - Systems Security and Security Lifetime Management, Secure Platforms, Digital Infrastructures

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-CS-01-01: Secure Computing Continuum (IoT, Edge, Cloud, Dataspaces)

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of between EUR 4.00 and 6.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 28.00 million.
Type of Action	Innovation Actions
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Tools to support cybersecurity resilience, preparedness, awareness, and detection within critical infrastructures and across supply chains;
- Cloud infrastructures vulnerabilities mitigation;
- Secure integration of untrusted IoT in trusted environments;
- Use of Zero-Trust architectures;
- Trust & Security for massive connected IoT ecosystems & lifecycle management;

- Secure interoperability and integration of systems;
- AI-based automation tools for cyber threat intelligence;
- Secure infrastructure, secure Identities and usability for a security chain covering communication, data collection, data transport, and data processing.

Scope: The evolution of our interconnected society brings multiple layers of cloud, edge computing, and IoT platforms that continuously interact with each other. Yet this always-connected ecosystem populated with potentially vulnerable entities requires advanced, smart and agile protection mechanisms to manage the security and privacy of individual components throughout their lifecycle and of overall systems. The complexity of such interconnected environments underlines the need for the proactive and automated detection, analysis, and mitigation of cybersecurity attacks in cloud, at the edge, for OT, IoT deployments, and in application domains such as, for example, smart cities. Integrating end-to-end security and user-centric privacy in complex distributed platforms requires work to address security threats and vulnerabilities over the entire platform ecosystem.

The identification and analysis of potential regulatory aspects and barriers for the developed technologies/solutions is encouraged, where relevant.

CS02 –Privacy-preserving and identity technologies

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-CS-01-02: Privacy-preserving and identity management technologies

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of between EUR 2.00 and 4.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 15.70 million.
Type of Action	Innovation Actions
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G. The following exceptions apply: Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the

	Research and Training Programme of the European Atomic Energy Community (2021-2025). [89].

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Improved scalable and reliable privacy-preserving and identity management technologies for federated and secure sharing and for processing of personal and industrial data and their integration in real-world systems;
- Improving privacy-preserving technologies for cyber threat intelligence and data sharing solutions;
- Privacy by design;
- Contribution to promotion of GDPR compliant European data spaces for digital services and research (in synergy with DATA Topics of Horizon Europe Cluster 4). Also, contribution to the promotion of eID Regulation compliant European solutions;
- Research and development of self-sovereign identity management technologies and solutions;
- Provide resource efficient and secure digital identity solutions for Small and medium sized enterprises (SME);
- Strengthened European ecosystem of open-source developers and researchers of privacy-preserving solutions;
- Usability of privacy-preserving and identity management technologies.

Scope: Using big data for digital services and scientific research brings about new opportunities and challenges. For example, machine-learning methods process medical and behavioural data in order to find causes and explanations for diseases or health risks. However, a large amount of this data is personal data. Leakage or abuse of this kind of data, potential privacy risks (e.g. attribute disclosure or membership inference) and identity compromises pose threats to individuals, society and economy, which hamper further developing data spaces involving personal data. Likewise, there are similar challenges for the exploitation of non-personal/industrial data assets that may compromise the opportunities offered by the data economy. Advanced privacy-preserving technologies such as, for example, cryptographic anonymous credentials, homomorphic encryption, secure multiparty computation, and differential privacy have the potential to address these challenges. However, further work is required to ensure and test their applicability in real-world use case scenarios.

[89] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

The security of any digital service or the access to data is based on secure digital identities. The eID Regulation provides the legal framework on which to build technological solutions that address the user needs concerning their digital identity. With regards to personal data, it is also important to develop self-sovereign identity solutions that give users complete control on their personal data and use.

Proposals should address usability, scalability and reliability of secure and privacy-preserving technologies in supply chain and take integration with existing infrastructures and traditional security measures into account. They should further take into account, whenever needed, the legacy variation in data types and models across different organizations. The proposed solutions should be validated and piloted in realistic, federated data infrastructures such as, for example, European data spaces. They should ensure compliance with data regulations and be GDPR compliant by-design. Open-source solutions are encouraged.

Consortia should bring together interdisciplinary expertise and capacity covering the supply and the demand side, i.e. industry, service providers and, where relevant, end-users. The use of authentication and authorisation infrastructure framework tools developed for data spaces, and notably with the European Open Science Cloud, could be considered. Participation of SMEs is strongly encouraged. Legal expertise should also be added to ensure compliance of the project results with data regulations and the GDPR.

The identification and analysis of potential regulatory aspects and barriers for the developed technologies/solutions is encouraged, where relevant.

CS03 - Secured disruptive technologies

Proposals are invited against the following topic(s):

HORIZON-CL3-2023-CS-01-03: Security of robust AI systems

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of between EUR 4.00 and 6.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 15.00 million.
Type of Action	Research and Innovation Actions

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Security-by-design concept and resilience to adversarial attacks;
- Inclusion of context awareness in machine learning in order to boost resiliency.

Scope: Proposals received under this topic will address the security of AI systems, in the line with the following considerations. The availability of very large amounts of data, together with advances in computing capacity, has allowed the development of powerful Artificial Intelligence applications (in particular Machine Learning and Deep Learning). At the same time, concerns have been raised over the security, robustness of the AI algorithms (including AI at the edge), including the risks of adversarial machine learning and data poisoning. Thus, it is important to promote security-compliant AI algorithms, leading to possible certification schemes in the future.

Proposals should demonstrate awareness of the EU approach on Artificial Intelligence[90], such as the proposed Artificial Intelligence Act.

The identification and analysis of potential regulatory aspects and barriers for the developed technologies/solutions is encouraged, where relevant.

Call - Increased Cybersecurity 2024

HORIZON-CL3-2024-CS-01

Conditions for the Call

Indicative budget(s)[91]

Topics	Type of Action	Budgets (EUR million)	Expected EU contribution per project (EUR million)[92]	Indicative number of projects expected to be funded
		2024		
Opening: 27 Jun 2024 Deadline(s): 20 Nov 2024				
HORIZON-CL3-2024-CS-01-01	IA	37.00	4.00 to 6.00	6
HORIZON-CL3-2024-CS-01-02	RIA	23.40	4.00 to 6.00	4

90 A European approach to artificial intelligence: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

91 The Director-General responsible for the call may decide to open the call up to one month prior to or after the envisaged date(s) of opening.
The Director-General responsible may delay the deadline(s) by up to two months.
All deadlines are at 17.00.00 Brussels local time.
The budget amounts are subject to the availability of the appropriations provided for in the general budget of the Union for years 2023 and 2024.

92 Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.

Overall indicative budget		60.40		

General conditions relating to this call	
Admissibility conditions	The conditions are described in General Annex A.
Eligibility conditions	The conditions are described in General Annex B.
Financial and operational capacity and exclusion	The criteria are described in General Annex C.
Award criteria	The criteria are described in General Annex D.
Documents	The documents are described in General Annex E.
Procedure	The procedure is described in General Annex F.
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G.

CS01 - Systems Security and Security Lifetime Management, Secure Platforms, Digital Infrastructures

Proposals are invited against the following topic(s):

HORIZON-CL3-2024-CS-01-01: Approaches and tools for security in software and hardware development and assessment

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of between EUR 4.00 and 6.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 37.00 million.
Type of Action	Innovation Actions
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G. The following exceptions apply: Eligible costs will take the form of a lump sum as defined in the

	Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025). [93].

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Improved hardware and software security engineering; resilient systems design;
- Improved access to testing of hardware and software in virtual, closed and secure environments;
- Systematic and, where possible, automated study of vulnerabilities, software analysis, vulnerability discovery, and dynamic security assessment;
- Trustworthy certifiable hardware and software;
- AI-based security services e.g. predictive security, advanced anomaly and intrusion detection, system health checks.

Scope: Software is at the foundation of all digital technologies and, as such, at the core of IT infrastructures, services, and products. Current software development prioritises fast deployment over security, which results in vulnerabilities and unsecure applications. Security engineering, both at the software and hardware levels, must be integrated in their development. Whilst a great portion of the software and hardware used in the EU is developed outside the European Union, it should comply with the security requirements within the EU. The EU should be able to rely on software and hardware that can be verified and audited as to their security. In particular, the potential security implications of using open-source software and hardware, and security auditability in that context, should be further explored. Software is subject to continuous update, so the security posture cannot be assessed once and for all, hence methods and tooling to perform continuous assessments of security are needed. In addition, security and privacy regulations also evolve, having to be factored in compliance approaches.

The identification and analysis of potential regulatory aspects and barriers for the developed technologies/solutions is encouraged, where relevant.

CS02 - Cryptography

Proposals are invited against the following topic(s):

[93] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

HORIZON-CL3-2024-CS-01-02: Post-quantum cryptography transition

Specific conditions	
Expected EU contribution per project	The Commission estimates that an EU contribution of between EUR 4.00 and 6.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 23.40 million.
Type of Action	Research and Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: In order to achieve the expected outcomes, and safeguard the Union's strategic assets, interests, autonomy, and security, participation in this topic is limited to legal entities established in Member States, Associated Countries and OECD countries. Proposals including legal entities which are not established in these countries will be ineligible.

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Increasing the maturity of current post-quantum cryptographic algorithms and contribution to further standardisation;
- Easy-to-use tools for the large-scale implementation of post-quantum cryptographic algorithms, based on state-of-the-art standards;
- Secure and efficient transition from pre- to post-quantum encryption through tools implementing a hybrid approach combining recognised pre-quantum public key algorithms and additional post-quantum algorithms;
- Phase-in of post-quantum algorithms or protocols to new or existing applications;
- Demonstrators and good-practice implementations of post-quantum cryptographic algorithms on varied hardware and software platforms;
- Application-oriented recommendations for the widespread implementation of post-quantum cryptography across the EU.

Scope: The advent of large-scale quantum computers will compromise much of modern cryptography, which is instrumental in ensuring cybersecurity and privacy of the digital transition. Any cryptographic primitive based on the integer factorization and/or the discrete logarithm problems will be vulnerable to large-scale quantum-powered attacks. The digital

data/products/systems that derive their security ultimately from the abovementioned primitives will be compromised and must be upgraded - including their replacement when needed- to quantum-resistant cryptography. The massive scale of this foreseen upgrade shows that preparations are needed today in order to widely implement the relevant mitigations in the future. Many companies and governments cannot afford to have their protected communications/data decrypted in the future, even if that future still seems distant. There is a need to advance swiftly in the transition to quantum-resistant cryptography.

Post-quantum resistant cryptographic algorithms should be deployable in a dynamic manner in order to quickly react to new quantum computer developments. Recommendations for post-quantum cryptography have already been published, but have to be maintained up-to-date, Proposals received under this topic should contribute to developing coordinated European recommendations for the transition to post-quantum cryptography across the EU.

The identification and analysis of potential regulatory aspects and barriers for the developed technologies/solutions is encouraged, where relevant.