EN

ANNEX 9

Of the Commission Implementing Decision on the 2020 Annual Action programme for the Partnership Instrument

Action Document for EU Cyber Diplomacy Support Initiative

1 KEY IDENTIFICATION DATA

Title of the Action	EU Cyber Diplomacy Support Initiative			
Country/region/global	Global			
Sector of intervention	Peace, security and defence in cyberspace			
Indicative budget	Total: 3 500 000 EUR EC contribution: 3 500 000 EUR Other contributions: N/A			
Duration and target start date of implementation	Duration: 36 months Target start date: March 2021			
Method of implementation	Direct management - Grants: call for proposals			
Legal basis	Regulation (EU) No 234/2014 of the European Parliament and of the Council of 11 March 2014 establishing a Partnership Instrument for cooperation with third countries			
Programming document	European Commission Implementing Decision C(2018)4001 on the second Multiannual Indicative Programme for the Partnership Instrument for the period 2018-2020			
DAC code(s)	99810			
Markers	**General policy objective**	**Not targeted**	**Significant objective**	**Principal objective**
	Participation development/good governance	☐	☐	☑
	Aid to environment	☑	☐	☐
	Gender equality	☑	☐	☐
	Trade Development	☑	☐	☐
		☑		
	RIO Convention markers	☑		
	Biological diversity	☑	☐	☐
	Combat desertification	☑	☐	☐
	Climate change mitigation	☑	☐	☐
	Climate change adaptation	☑	☐	☐

2 RATIONALE AND CONTEXT

2.1 Action summary

This Action aims to promote principles of the EU approach to cyberspace as defined in the 2015 Council Conclusions on Cyber Diplomacy, 2017 Joint Communication on Resilience, Deterrence and Defence and 2018 Council Conclusions on EU External Cyber Capacity Building Guidelines with a specific focus on promoting and protecting a global, open, free, stable and secure cyberspace where human rights and fundamental freedoms and the rule of law fully apply for the social well-being, economic growth, prosperity and integrity of our free and democratic societies. The project focuses on enhancing cyber security cooperation globally and strengthening the EU's role as a global security stakeholder, as foreseen in the EU's Global Strategy on Foreign and Security Policy. Strengthened international cyber policy cooperation is high on the political agenda and directly contributes to international peace and security. This action is thus fully in line with Commission priority 2019-2024: A stronger Europe in the world.

The EU has a core interest in actively contributing to discussions on the future governance of cyberspace. Therefore, in order to better promote its position and disseminate its core values, the EU should engage via various outreach and capacity building activities with wide range of stakeholders, both with internal and external, governmental and non-governmental. The new project will facilitate taking forward agreed positions and share best practices in bilateral, multilateral and regional fora (e.g. Organisation for Security and Cooperation Europe (OSCE), ASEAN Regional Forum (ARF), Organisation of American States (OAS), African Union (AU), G7, within UN bodies as appropriate), as well as in the bilateral cyber dialogues and consultations that the EEAS holds inter alia with the U.S., China, Japan, the Republic of Korea, India and Brazil.

The project will support EU priorities to establish a strategic framework for conflict prevention and stability in cyberspace, which is based on the application of existing international law, the development and implementation of voluntary non-binding norms, and promotion of regional cyber confidence building measures, supported by capacity building efforts and complemented by the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (9916/17). With two important UN processes, UN Group of Governmental Experts (UNGGE) and Open-ended Working Group (OEWG) in the Field of Information and Telecommunications in the Context of International Security, started in 2019 and taking up further discussions on these matters, the EU plays a very significant role as a model for developing countries how to advance an global, open, free, stable and secure cyberspace. To support this work, the EEAS has developed an Outreach plan and foresees the project to significantly contribute to and support the operationalisation of this plan by providing policy support, technical assistance and logistical support for planned activities.

This Action aims to deepen the EU's engagement globally with stakeholders of strategic interest in cybersecurity field. It will seek to advance dialogues and cooperation where there is a high potential to advance, focusing on regional organisations and countries who are willing and able to go further to promote common goals. The action will support cyber dialogues and cooperation at the bi-regional, sub-regional and country levels, as foreseen in the agreements, action-plans and declarations concluded with various sub regional groups and countries. It is intended also to contribute to further the dialogue beyond governments, with civil society and the business community.

The proposed set of activities will contribute ultimately to bring concrete returns for the EU's foreign policy goals in promoting and protecting a global, open, free, stable and secure cyberspace, further progress towards policy and regulatory convergence and alignment of positions and policy objectives in cyber sphere in the global arena.

Through a mix of organisation of events, specialised assistance, awareness raising, communication, expert exchanges, internships, study visits, summer schools, workshops, thematic events, sponsoring programme and provision of technical assistance and technical exchanges, the Programme will act as the EU’s project facility globally by translating policy commitments agreed at the political level into follow-up actions and results. The Action will complement ongoing EU interventions in cybersecurity globally.

2.2 Background/Context/Rationale for PI funding

EU Cyber Diplomacy Support Initiative: EU policy and key issues

Cyberspace, and in particular the global, open Internet has become one of the backbones of our societies. As global Internet usage continues to expand with almost three billion people using online platforms in all spheres of life, the 2030 Agenda for Sustainable Development recognises the importance of ICT and digitalisation as a cross-cutting issue, offering a platform that drives connectivity and economic growth. It also contributes to the sustainable development in the context of innovation, especially in least developed countries, with positive impact on education and gender equality. The spread of information and communications technology, use of the new and emerging technologies and global interconnectedness has great potential to accelerate human progress, to bridge the digital divide and to develop knowledge-based societies.

However, the borderless nature of cyberspace and the rapid digital evolution has been accompanied by increased number of threats posed by malicious cyber activities. It also refers to vulnerabilities in new and emerging technologies. The use of cyberspace as a domain of conflict, either solely or as part of a hybrid approach, is now widely acknowledged. Cyber threats can disrupt the supply of essential services. Moreover, cyber-attacks and disinformation campaigns constitute a substantial threat to democratic processes and risk to erode public trust in institutions and information. Cybercrime is one of the fastest growing forms of crime and the risks are increasing exponentially.

To respond to these challenges, the EU adopted in February 2013 its Cybersecurity Strategy. The Strategy states that the EU will seek to promote openness and freedom of the Internet, encourage efforts to develop and implement norms of behaviour and apply existing international law in cyberspace in its international cyberspace policy. The EU will also work towards closing the digital divide, and will actively participate in international efforts to build cybersecurity capacity. The strategy also outlines that the EU will seek close cooperation with the international organisations that are active in this field such as the Council of Europe, OECD, UN, OSCE, NATO, AU, ASEAN and OAS.

To further enhance international cooperation on cyber security, the Joint Communication from September 2017 Resilience, Deterrence and Defence: Building strong cybersecurity for the EU underlines that the EU will strengthen its response to cyber-attacks, including via new cyber capacity building efforts to assist third countries to address cyber threats, as well as through the use of the framework for a joint EU diplomatic response to malicious cyber activities (the "cyber diplomacy toolbox"). As stated in this Joint Communication, the EU's international cybersecurity policy is designed to address the continuously evolving challenge of promoting global cyber stability, as well as contributing to Europe’s strategic autonomy in cyberspace, and is guided by the EU core values and fundamental rights such as freedom of expression and the right to privacy and protection of personal data, and the promotion of the open, free and secure cyberspace. The EU promotes a strategic framework for conflict prevention, cooperation and stability in cyberspace in its bilateral, regional, multi-stakeholder and multilateral engagements. This ambitious framework is based on (i) the application of international law, and in particular the UN Charter in its entirety and the Universal Declaration of Human Rights, in cyberspace; (ii) the development and implementation of universal non-binding norms, rules and principles of responsible State behaviour; and (iii) regional confidence-building measures (under the OSCE, the ARF and the OAS level).

Stability in cyberspace is of strategic interest to the EU, as well as to international peace and security. However, the responsibility for a more open, stable and secure cyberspace lies with all stakeholders involved, from citizens to governments, often operating in different value systems. Consequently, the question of international cyber stability and preventing conflicts through the application of existing international law and the adherence to and use of norms of responsible state behaviour and confidence building measures in cyberspace, as well as the promotion of human rights and fundamental freedoms online and the security threats accompanying emerging technologies have become mainstream foreign policy topics and at the centre of numerous discussions.

International cyber policy is one of the fast growing global policy fields, where major international players have high interests and stakes. There are diverging views on cyber issues as some governments would like to gain stricter control over cyberspace and the Internet, aspiring to launch a UN treaty or/and bringing the Internet infrastructure under a UN body, while the EU and its Member States support an open and free Internet governed by a multi-stakeholder model (i.e. private sector, governments, civil society, academic and technical community). In addition, the EU, its Member States and like-minded countries maintain that States' conduct in cyberspace should adhere to existing international law and norms of responsible state behaviour. The efforts to regulate cyberspace via a UN treaty and bring the Internet under the UN auspices raises concern in relation to restrictions of the Internet as an open, secure and stable platform contributing to economic growth as well as human rights and fundamental freedoms. Furthermore raising unnecessary doubt whether already existing international law applies in cyberspace, may encourage miscalculation, erode accountability for actions and in result lead to increase instability in cyberspace.

In recent years States have negotiated normative behaviour and the application of existing international law in cyberspace in a UN Group of Governmental Experts (UNGGE) on Developments in the Field of Information and Telecommunications in the Context of International Security under the UN First Committee. In 2018 the UNGA First Committee adopted two resolutions. Russia and China had put forward a resolution for convening an open-ended working group to further develop norms and principles of responsible behaviour selectively chosen previous GGE reports. US had submitted a counter-proposal to establish a group of governmental experts with a view to work on possible cooperative measures to address existing and potential threats in the sphere or information security, from the assessment contained in previous GGE reports.

The EU has a vital interest in actively contributing to international cyber policy discussions as mitigation of cybersecurity threats, conflict prevention and greater stability in cyberspace through the use of all available instruments, including diplomatic and legal, is one of the EU’s priorities, as set out in the 2015 Council conclusions on Cyber Diplomacy.

In order to better promote EU position and core values, the EU needs to engage with wide range of stakeholders globally. Given the global nature of the threat, building and maintaining robust alliances and partnerships is fundamental to the prevention, mitigation, deterrence of and respond to malicious cyber activities and to advance international stability and security and build resilience of all stakeholders.

Effective engagement with states and other stakeholders participating in the process can be a challenge. Many external partners are still developing their policy, legal and institutional landscape to address cyber-related challenges, including in the context of international peace and security. As a result, the EU and the Member States need to be flexible and innovative to be successful in promoting their values and delivering messages, but also engaging in workshops and dialogues on cyber capacity building, sharing technical and institutional expertise and supporting legal and regulatory reforms. Given the growing importance of cyber in policy discussions, the EU should continue to support the development of cyber diplomacy capacities of diplomats and policy makers in partner countries.

The EU has achieved to build up specific cyber dialogues with the US, Japan, Brazil, India, South Korea and China. Close consultations with international organizations, such as NATO, the ASEAN Regional Forum, the OSCE, the Council of Europe, and the OECD are well in place, cooperation with AU and OAS is developing. To operationalise these dialogues and translate discussions into concrete partnerships and actions on the ground is necessary.

While cyber issues related to international security are mainly negotiated between states, the EU recognises the importance of involving multiple stakeholders into the discussions on cyber governance, frameworks and norms to support the multi-stakeholder approach. These meetings allow governmental and non-governmental actors to work together and thus encourage new thinking that can inform the formal processes.

Civil society organisations play an important role in cyber discussions. In parallel, the private sector has also an important role to play for at least two reasons. Firstly, the security of products put on the market by IT companies and internet service providers has a direct impact on the level of trust towards

ICTs in general. Secondly, private companies – either due to their innovative potential or critical infrastructure providers and therefore importance for national security – are one of the main targets of cyber-attacks. Consequently, the engagement of the private sector in discussions regarding common minimum standards for protecting critical infrastructure is important.

To ensure equal participation of all stakeholder groups in the discussion, it is important to ensure that gender issues are in line with the EU's commitment to further develop and implement a common and comprehensive EU approach for cyber diplomacy at global level that promotes a cyber policy informed by gender equality. In particular, participation of women in cybersecurity related discussions in different foras, promoting female diplomats' expertise on cyber issues, supporting development of necessary cyber capabilities and the participation of women in all aspects of peace processes within the scope of this project need support. The women, peace and security (WPS) agenda should be used as a common platform to further develop the EU's engagement with global partners.

Already through the EU Cyber Direct project, the EU supports the development of a global, open, free, stable and secure cyberspace, and rights-based international order online. Current action builds on the work of the existing project EU Cyber Direct, and seeks to provide complementarities and additional possibilities for a more targeted outreach activities and flexible engagements bilaterally, multilaterally and via regional/thematic international platforms to support the EU's cyber diplomacy efforts globally.

This new phase of this Cyber diplomacy project will focus on specific countries where there is a strategic interest. The EEAS recently developed a targeted outreach and engagement plan and identified strategic priorities in which to focus our efforts and foresees enhanced cooperation with like-minded partners to create a multiplier effect. This project will be instrumental to implement this plan.

Reference to relevant PI objectives and priorities

The proposed action fully reflects the objectives set out in article 1 (2a) as well as article 1 (2d) of the PI regulation (EU) No 234/2014. The activity also reflects the objectives listed in article 1 (2b) and 1 (2c). Through a more coherent and better planned approach to promote and protect a global, open, free, stable and secure cyberspace, the proposed action is in line with article 3 of the PI regulation.

The action could also directly and indirectly help open up business opportunities for EU companies in the field of cybersecurity (Article 1 (2c)). Through accompanying information actions, the proposed action will also enhance the understanding and visibility of the Union as a global security actor (article 1 (2d)).

2.3 Lessons learnt

PI-supported stand-alone and Policy Dialogue Support Facility projects (or similar) are being implemented in a number of strategic partner countries of the EU, and regionally/globally. Despite similar objectives, stemming from the EU's intention to consolidate and enhance the existent strategic partnerships, there is no "one size fits all" model. Each partnership is unique in its structure, scope, policy priorities and level of advancement. However, key elements to all are flexibility, to adjust the working methods and tools (means and activities) to the actual needs stemming from the political situation and developments at international level during the implementation period, and horizontal nature of the action.

A key element for the success of the action is the active involvement and close technical steer from the different EU services at Headquarters and Delegations. The set up of a comprehensive and workable Steering Committee and the appropriate planning and monitoring mechanisms will be essential to this purpose.

Another important element is to set up adequate criteria to prioritise the activities to be supported. For this action, criteria will be set at the beginning of the action based on: alignment with foreign policy priorities related to cybersecurity, potential return for EU's interests, political interest and capacity of

partner, and degree of commitment of competent EU service to accompany the implementation of the activity and to ensure its follow up.

To be more focused in its efforts and taking account that the action will have a global scope, driven by the developments at the United Nations level and the EU's interest to promote its positions and participate in the discussions on the future governance of cyberspace, the efforts will be targeted at regional organisations and focuses on specific countries of interest.

2.4 Coherence and complementarity

Throughout the implementation of the Action, synergies will be sought with all ongoing PI-supported stand-alone, PSF, and TAIEX actions in cybersecurity field, both bilateral and multilateral (global) ones,
but not limited to. In this context, special attention will be given to the existing projects EU Cyber Direct and Security in and with Asia. Complementarities will be furthermore sought with the relevant programmes implemented in cybersecurity by other Directorate Generals, in particular DEVCO, such as Cyber4Dev, CyberNet, GLACY+, Cyber capacity building toolkit, and ongoing projects and digital dialogues and interactions of DG CNECT with partners, etc. Taking account the importance of coherence and complementarity with other ongoing EU-funded projects in this domain, work to ensure coordination and build synergies have started. The exchanges with FPI, DEVCO and other relevant DG Team leaders of ongoing projects will continue to build complementarities for stronger impact. In addition, regular meetings with project implementers of relevant projects are planned to update on developments in the domain and to inform EU priorities.

Outreach and coordination with the EU Member States and their projects implemented in cyber security domain will be ensured from the onset, including through regular reporting on ongoing and planned activities under this Action to the Horizontal Working Party on Cyber Issues (HWPCI) and the EU Delegations who will report to EU Heads of Missions globally. This will improve the impact of planned interventions, and ensure coherence in delivering the messages. In addition, regular capital retreats will be used to share information of ongoing and planned initiatives.

This Action aims to support and promote EU-run cyber dialogues, but also security/political dialogues, where relevant, with partner countries and regional subgroups, as well as individual countries, and is hence to be managed at the EU Headquarters level. This will allow for identification of synergies with the ongoing EU-supported projects in relevant fields in order to ensure that added value is produced through additional coordination with services of the Commission. In light of the global nature of this action, regular outreach and engagement with the EU Member States is planned for this action, as well as with their agencies and projects funded by them.

2.5 EU added value

In the fluid of the fast changing cyber domain, this action is needed to equip the EU with the capacity to act, supporting the EU's bilateral, regional and inter-regional cooperation partnership strategies by promoting policy dialogue and collective approaches and responses to challenges of global concern and enhancing understanding and visibility of the Union by means of public diplomacy, think tank cooperation and outreach activities.

EU interest in this action stems from the increasing importance of cybersecurity and stability in cyberspace, which is critical both to EU's prosperity and security. With increasing dependency on digital technologies we become more and more exposed. The project will enhance cyber security cooperation globally and strengthens the EU's role as a global security stakeholder, as foreseen in the EU's Global Strategy on Foreign and Security Policy, as strengthened international cyber policy cooperation is high on the political agenda.

The EU has a core interest in actively contributing to discussions on the future governance of cyberspace. Therefore, in order to better promote its position and disseminate its core values, the EU should engage with wide range of stakeholders, both with internal and external via various outreach

activities. In this regard, the EEAS already has actively engaged with EU Member States by facilitating development of unified positions. The new project will facilitate taking forward agreed positions in bilateral, multilateral and regional fora (e.g. OSCE, ARF, G7, within UN bodies as appropriate, OAS, AU, etc.), as well as in the bilateral cyber dialogues and consultations that the EEAS holds with the U.S., China, Japan, the Republic of Korea, India and Brazil. The recent experience has shown that formal bilateral discussions can be successfully complemented with discussions between official and non-official actors.

The project will also support EU priorities to establish a strategic framework for conflict prevention, cooperation and stability in cyberspace, which is based on the application of existing international law, the development and implementation of voluntary non-binding norms, and promotion of regional cyber confidence building measures. With two important UN processes, UNGGE and OEWG, starting this year and taking up discussions on these matters, the EU plays a very significant role as a model for developing countries how freedom and security can, and should be, balanced in cyberspace. This project will be instrumental in supporting operationalisation of the outreach plan by providing both technical assistance and logistical support for planned activities. In addition, the project will support to follow-up the political dialogues and translate discussions and decisions into concrete partnerships and actions on the ground by sharing technical and institutional expertise and support legal and regulatory reforms to build open, free, stable and secure cyberspace. The project will also strengthen the EU's position as a reliable international interlocutor on cyber diplomacy with its multi-layered approach between bilateralism and multilateralism.

2.6 Cross-cutting issues

The action will consistently mainstream cross-cutting issues, such as gender, democracy, rule of law, human rights and fundamental freedoms, and those inherent to the Partnership Instrument, such as multilateralism, global order, EU principles and values, resilience, innovation. The selected implementing partners will be required to demonstrate in the design of the project on how the relevant cross-cutting will be incorporated in this Action when preparing and implementing individual activities.

3 ACTION DESCRIPTION

3.1 Objectives

Against the background set out above, the **overall objective** a of the project is to promote and protect a single, open, free and secure cyberspace which fully reflects and respects the core EU values of democracy, human rights and the rule of law.

The **specific objectives** of this action are to contribute to:

- Increased consensus in partner countries for open, free, and secure cyberspace, through the promotion of existing international law, norms of state behaviour and confidence building measures in cyber space and increase cyber resilience (Cyber consultations component)
- Greater convergence between partner countries and regional organisations standards, policies and best practices and those of the EU(Cooperation and Capacity Building Component)
- Raised awareness of the EU's contribution to global cyber stability and resilience in partner countries and regional and international organisations (Outreach and Public Diplomacy component).

Scope

Thematically, the key area is trust and security in cyberspace, as identified on the basis of the EU's interests and the partners' interests and needs.

Human rights and gender perspectives and adhering to the highest standards of conduct, discipline and accountability are crosscutting issues and need to be explicitly included in relevant activities supported through this action.
Geographically, the scope of the project is global, taking account that the global nature of the cyber threat and due to the need for the EU to engage with wide range of stakeholders at global level. The strong focus is also on regional engagement to complement bilateral dialogues.
The goal of this project is to strengthen the role of the EU globally that will with all certainty continue to be of high relevance and interest. As the project design is flexible, it can adjust to changes in bilateral and regional relations, and adapt according to the outcomes and developments in the international fora, ensuring that resources are spent to best effect.

Many global partners have an interest in the EU as a security actor but often lack a clear perception on the benefits, substance, and how to partner with the EU. Thus, there is scope for the EU to take cyber dialogues and discussions to a level of more concrete cooperation. The impact of this project is an increased recognition of the EU as a relevant partner in the field of cybersecurity, and with that increased its participation in cybersecurity matters globally. This will be important considering the importance of the current cyber-related discussions at the global level and both in the long and short run it will improve the EU's capacity to address cybersecurity issues of concern. In addition, the project will make a positive contribution to the application of existing international law in cyberspace and development of the cyber confidence-building measures (CBMs) and therefore to a safer cyber space.

These impacts are expected to remain beyond the implementation period of the proposed action. Indeed, activities conducted through the proposed action are expected to and will be further designed with a view to create positive spill-over effects in the partner countries/organisations.

A failure to invest at this point will mean a loss of momentum, which the EU would have to make up for later, perhaps at a higher cost. Even if the overall sustainability will depend on the global political climate, good planning, monitoring and evaluation of the project will allow establishing clear links between past, present and future actions and results.

Activities can take the form of events - including conferences, dialogue sessions, workshops, study visits, think tank research/exchanges, trainings, provision of services like technical studies and/or assistance (including technical expertise), representational activities, info-points, newsletters, audio-visual material, exhibitions, public outreach campaigns, etc.

3.2 Stakeholders

The main stakeholders for the action from EU institutions include the European Commission services, the EEAS and EU Delegations. Other EU stakeholders may include EU agencies and bodies operating in the security field (including EU Institute for Security Studies (EU ISS), EUROPOL, CEPOL, ENISA, EDA and ESDC).

Stakeholders also include EU Member States, including governmental and state authorities and institutions (including diplomatic missions) and domestic non-state actors such as academic institutions, think tanks, the private sector, and civil society organizations engaged in cybersecurity cooperation.

Correspondingly, regional and international organisations and stakeholders from the partner countries, including governmental and state authorities and institutions and domestic non-state actors such as academic institutions, think tanks, the private sector, and civil society organizations, involved in cybersecurity cooperation.

The above-mentioned key stakeholders will be included in formulation and implementation of activities of their interest within the scope of the project.

3.3 Risk assessment and management

Risk description	Risk level (High, Medium, Low)	Mitigating measure
Lack of clear perception of EU as a security actor and security partner	**M**	Outreach to officials and public diplomacy activities to disseminate knowledge of EU activities and policies in cybersecurity. Ensure clear coordination with EUMS and develop a list of clear examples and potential benefits where partner countries would profit from a partnership with the EU and its EUMS.
Overlaps with projects from other donors	**L**	Informal coordination with other donors, including Member States, to avoid overlaps. Project design also introduces necessary level of flexibility to avoid overlaps.
Overlaps with existing EU-funded projects at national and regional level	**L**	Direct involvement of EEAS/Commission geographical desks and EU DEL correspondent ensures full knowledge of parallel EU-funded activities.
Changes in the priorities of partner countries and in our bilateral relationships	**L**	Project design introduces necessary level of flexibility to adapt to such changes by focusing on particular topics and/or by involving stakeholders from a wide spectrum.
Gender equality may be seen as an extraneous and non-relevant issue by implementing partners and if	**M**	Project design will endeavour to integrate explicit and relevant gender equality components for action activities. It will include
Assumptions		
Sustained willingness of partner countries/ regional organisations/international organisations to engage with the EU as expressed in bilateral dialogues.		

3.4 Communication and EU visibility

Communication and visibility of the EU is a legal obligation for all external Actions funded by the EU.

This Action shall contain communication and visibility measures which shall be based on a specific Communication and Visibility Plan of the Action, to be elaborated at the start of implementation.

Appropriate contractual obligations shall be included in, respectively, the procurement and grant contracts, and delegation agreements.

The Communication and Visibility Manual for European Union External Action[1], which came into force on 1 January 2018, shall be used to establish the Communication and Visibility Plan of the Action and the appropriate contractual obligations.

Besides following the rules and guidelines linked to communication and visibility for the EU funded projects, this action will be particularly attentive to communicate on the actions that support the different various activities. The implementing partner(s) shall define a communication strategy, including media engagement, in order to adequately communicate the EU's contribution to trust and security in cyberspace. To ensure pertinence, impact and coherence, communication activities and visibility actions shall be coordinated with the Press and Information sections of the EU Delegations in the targeted countries.

[1] https://ec.europa.eu/europeaid/sites/devco/files/communication-visibility-requirements-2018_en.pdf

4 IMPLEMENTATION ARRANGEMENTS

4.1 Method of implementation

Direct management Grants: call for proposal

This project will be implemented through grant(s) awarded through a call for proposals.

(a) Purpose of the grant(s)

The objective of the grant is to contribute to advance an open, free and secure cyberspace through the promotion of rules-based cyber-behaviour and increased cyber resilience. The field of intervention is cyber diplomacy and cyber resilience. Expected results are: increased consensus with partner countries on how to apply existing international law in cyberspace; enhanced development of cyber norms and confidence building measures; strengthened multi-stakeholder cyber engagement; and enhanced dissemination of EU best practices in strengthening cyber resilience and protecting critical cyber infrastructure.

(b) Type of applicants targeted

Think tanks, NGOs, research institutes or other civil society organisations in the EU and partner countries. Regional and international organisations as well as specialised EU agencies are eligible to apply. Applicants must demonstrate that project activities are strictly non-profit making.

The essential selection criteria are financial and operational capacity of the applicant. The essential award criteria are relevance of the proposed action to the objectives of the call, design, effectiveness, feasibility, sustainability and cost-effectiveness of the action.

4.2 Indicative budget

Method of Implementation	**Amount in EUR**
4.1.1 Direct management - Grants: call for proposal	3 500 000
Total	**3 500 000**

4.3 Organisational set-up and responsibilities

A Project Steering Committee (PSC) will be set up and composed of representatives of relevant EU services in Headquarters. It will give overall political steer to the facility and will validate the pipeline of activities identified and proposed by the different services (with the support of the project implementation team). The PSC will meet at least every six months.

A methodology that combines the need for planning and flexibility to respond to emerging political needs as well as criteria to define the activities will be set up by the management of the programme and shared with the PSC.

EU Member States will be regularly informed of the activities at HQ (HWPCI) and at country level (Heads of Mission/ Political or sectoral Counsellors as relevant), to maximise synergies with their own activities.

Active involvement and participation of relevant global stakeholders will be sought in the different activities implemented under the project.

4.4 Performance monitoring

The day-to-day technical and financial monitoring of the implementation of this Action will be a continuous process and part of the implementing entity's responsibilities. To this end, the

implementing entity shall establish a permanent internal, technical and financial monitoring system for the Action and elaborate regular progress reports (not less than annual) and final reports.

Every report shall provide an accurate account of implementation of the Action, difficulties encountered, changes introduced, as well as the degree of achievement of its results. The progress and final reports shall provide quantified and qualitative data in relation to the logical framework indicators which will include relevant indicators from the list of core and corporate indicators.

The report shall be laid out in such a way as to allow monitoring of the means envisaged and employed and of the budget details for the Action. The final report, narrative and financial, will cover the entire period of the Action implementation.

The Commission may undertake additional Action monitoring visits both through its own staff and through independent consultants recruited directly by the Commission for independent monitoring reviews (or recruited by the responsible agent contracted by the Commission for implementing such reviews).

4.5 Evaluation and audit

For this Action, the Commission may carry out interim and/or final/ex-post evaluation(s) via independent consultants contracted by the Commission based on specific terms of reference.

Without prejudice to the obligations applicable to contracts concluded for the implementation of this Action, the Commission may, on the basis of a risk assessment, contract independent audits or expenditure verification assignments.

As the "N+1" rule applies for contracting under this decision, external evaluations and audits, as well as additional external monitoring referred to under section 4.4. above, will be funded from sources other than those allocated to this specific Action.