EN

ANNEX III

of the Commission Implementing Decision on the Annual Action Programme 2016 for Article 5 of the Instrument contributing to Stability and Peace to be financed from the general budget of the Union

Action Document for Protecting Critical Infrastructure

1. Title/basic act/ CRIS number	Protecting Critical Infrastructure CRIS number: 038-875 financed under IcSP			
2. Zone benefiting from the action/location	Miscellaneous countries			
3. Programming document	Regulation (EU) No 230/2014 establishing an Instrument contributing to Stability and Peace - Multiannual Indicative Programme 2014-2017[1]			
4. Sector of concentration/ thematic area	Cybersecurity SDG 9a on resilient infrastructure	DEV. Aid: YES		
5. Amounts concerned	Total estimated cost: EUR 11 000 000 Total amount of EU budget contribution EUR 11 000 000			
6. Aid modality(ies) and implementation modality(ies)	Project Modality Indirect management with Member State agency			
7 a) DAC code(s)	15210 - Security system management and reform			
b) Main Delivery Channel	10000 - PUBLIC SECTOR INSTITUTIONS			
8. Markers (from CRIS DAC form)	**General policy objective**	**Not targeted**	**Significant objective**	**Main objective**
	Participation development/good governance	□	□	X
	Aid to environment	X	□	□
	Gender equality (including Women In Development)	X	□	□
	Trade Development	X	□	□
	Reproductive, Maternal, New born and child health	X	□	□
	RIO Convention markers	**Not targeted**	**Significant objective**	**Main objective**
	Biological diversity	X	□	□
	Combat desertification	X	□	□
	Climate change mitigation	X	□	□
	Climate change adaptation	X	□	□
9. Global Public Goods	N/A			

[1] Thematic Strategy Paper 2014-2020 and its accompanying Multi-annual Indicative Programme 2014-2017 (C(2014) 5607 of 11.8.2014).

and Challenges (GPGC) thematic flagships	

SUMMARY

The Action "Capacity Building and Cooperation to enhance Cyber Resilience (CB4CyberResilience)" builds on the lessons learnt of the IcSP's pilot action on promoting cybersecurity (2013-2016) "Enhancing Cybersecurity: Protecting Information and Communication Networks (ENCYSEC)" and has as a specific objective to increase the security and resilience of critical information infrastructure and networks supporting the critical services of third countries while ensuring compliance with human rights and the rule of law. The specific objective will be pursued by supporting the adoption and implementation of a comprehensive set of policy, organisational, and technical measures that will increase the selected third countries' cybersecurity preparedness, following a multi-stakeholder and human rights compliant approach. The proposed Action is in line with the *European Cybersecurity Strategy* (2013) and the *Council Conclusions on Cyber Diplomacy* (2015).

It shall contribute to the implementation of the 2030 Agenda for Sustainable Development and specifically SDG 9.a *(“Facilitate sustainable and resilient infrastructure development in developing countries”)* and 16.a *("Develop effective, accountable and transparent institutions*"). It shall also contribute to the implementation of the Joint Communication on Countering Hybrid Threats [JOIN (2016)18, 06.04.2016], which aims to boost the resilience of the EU and its partners, also in relation to cybersecurity.

The Commission will ensure that measures are implemented in accordance with international law, including international human rights and humanitarian law, and in line with the EU Strategic Framework and Action Plan on Human Rights and Democracy. To ensure compliance with the obligations stipulated in Article 10 of the IcSP Regulation ("Human rights"), a clear human rights perspective will be incorporated throughout the different stages of the project cycle (elaboration of project documents; monitoring of implementation; evaluation) on the basis of the operational guidance developed to this end by the Commission, while relevant information shall be included in its regular reporting.

1 CONTEXT

1.1 Sector context/Thematic area

A secure and safe digital environment is a necessary condition for reaping the benefits of ubiquitous access to the internet and the positive impact it has on human and economic development. As the number of internet users has more than tripled in a decade, from 1 billion in 2005 to an estimated 3.2 billion by the end of 2015, the number of devices connected to the internet is also estimated to have reached 15 billion during 2015. In this unprecedented information and communications revolution in human history, addressing the threats posed by malicious cyber activities and promoting secure digital services and infrastructure is a clear priority.

The expanding use of Information and Communications Technology over the past 20 years and its contribution to the evolution – or even complete revolution – of various policy areas has resulted in the emergence of a broad policy community relying on these technologies. The increasing reliance on ICT in all spheres of life and a growing number of connections between people, processes and data has already started the transformation of our societies, and our systems of governance need to keep abreast of these changes.

However, the efforts at improving the access to ICT and the growing Internet penetration have so far underestimated the risks and challenges associated with this process. The explanation is twofold. The last decade in particular has seen a rapid growth in threats to cyberspace: according to the ITU, 6.5 million new malware was created by end of 1st quarter in 2013. At the same time, many countries have only recently started to understand risks that prevent them from reaping of the benefits of increased access to the Internet for delivery of services like banking, health care or education. It has become clear that, as countries move forward with their development programmes, they also need to pay attention to security aspects at different levels, including the infrastructure, processes or personnel. An example of the greater understanding of how critical information infrastructure protection and digital security should be addressed in combination with economic development can be found in the recent Recommendation of the OECD to its member countries on Digital Security Risks Management (September 2015), which highlights that "Digital security risk should be treated like an economic rather than a technical issue, and should be part of an organisation's overall risk management and decision-making". As a result, the challenges raised by digital security risks should not only be considered from the technical perspective, but also taking into account economic and social decision-making. Importantly, "*the 'perimeter security' paradigm that pervades today, needs revisisting, putting users –not devices– at the center of discussion, and thus implying a great role for capacity building*" as the 2016 World Development Report on Digital Dividends confirms.

In the context of hybrid threats, cybersecurity plays an ever more prominent role. The coordinated and systematic use of diverse hybrid tools is becoming more sophisticated in today's interconnected, networked world. The potential impact of hybrid threats depends on the resilience of (or lack thereof) national critical infrastructures and networks (eg. energy, telecommunications, financial, transportation, water). Therefore, efforts to strengthen cybersecurity in third countries can directly increase their abilities to protect their strategic assets and to be ready to respond to potential attacks.

1.1.1 Public Policy Assessment and EU Policy Framework

The Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [JOIN(2013) 1 final, 07.02.2013] outlines the EU's vision in the domain of cybersecurity. It offers clear priorities for the EU's international cyberspace policy including defining the EU approach to cyber capacity building and calling to step up efforts to support cyber capacity building in third countries and foster international cooperation in cyberspace issues.

In defining cybersecurity, the EU's Cybersecurity Strategy states that "*it refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its independent networks and information infrastructure. Cybersecurity strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein*".

Under the priority of "Developing capacity building on cybersecurity and resilient information infrastructures in third countries", the Strategy stresses that "*the smooth functioning of the underlying infrastructures that provide and facilitate communication services will benefit from increased international cooperation. This includes exchanging best practices, sharing information, early warning joint incident management exercises and so on*". The Strategy foresees that "*the EU will contribute towards this goal by intensifying the on-going international cooperation efforts to strengthen Critical Information Infrastructure*

Protection (CIIP) cooperation networks involving governments and the private sector". The Startegy also reaffirms the EU's support to the adoption, implementation and promotion of the Council of Europe Convention on Cybercrime as a model for a global instrument in the fight against cybercrime.

Moreover, the Council Conclusions on Cyber Diplomacy adopted on 11 February 2015 by the General Affairs Council recognise that cyberspace issues present both significant opportunities as well as continuously evolving challenges for EU external policies. The topics covered by the Council Conclusions include the promotion and protection of human rights in cyberspace; the application of international law, rule of law and norms of behaviour in cyberspace; enhancing competitiveness and prosperity of the EU; cyber capacity building and development; strategic engagement with key partners and international organisations.

Specifically on capacity building, the 2015 Cyber Diplomacy Council Conclusions "*reiterate the importance of cyber capacity building in third countries as a strategic building block of the evolving cyber diplomacy efforts of the EU towards the promotion and protection of human rights, rule of law, security, growth and development*". They further call on the EU and its Member States, amongst others to:

- develop a coherent and global approach to cyber capacity building, which on one side brings together technology, policy and skills development within a broader and overreaching EU development and security agenda, and on other side facilitates the design of an effective EU model for cyber capacity building;
- support new initiatives on cyber capacity building that take stock of, build on, and complement existing initiatives emphasising the importance of access to and use of unhindered, uncensored and non-discriminatory use of open and secure ICT for fostering open societies and enabling economic growth and social development;
- tackle growing cyber threats and challenges by increasing resilience of critical information infrastructure and by reinforcing close cooperation and coordination among international stakeholders through initiatives such as the development of confidence building, common standards, international cyber exercises, awareness raising, training, research and education, incident response mechanisms.

Moreover, the EU's cyber capacity building is strongly linked to its development cooperation commitments also in reflection of the 2030 Agenda for Sustainable Development adopted in September 2015 (SDG 9a *on resilient infrastructure*, SDG 16.4 *on combatting all forms of organised crime* and SDG 16.6 on *effective, accountable and transparent institutions*).

Capacity building of the civilian cybersecurity sector in third countries through external cooperation funds provides significant assistance in increasing their overall incidence response capacity to critical national vulnerabilities and in countering hybrid threats. In April 2016, the Commission and High Representative adopted a Joint Communication on Countering Hybrid Threats [JOIN (2016)18, 06.04.2016], which outlines actionable proposals to help counter hybrid threats and foster the resilience of the EU and its Member States as well as its partners: the fundamental role of cybersecurity in addressing hybrid threats is clear. Relevant developments will be reflected in the Global Strategy on Foreign and Security Policy currently under development.

1.1.2 Stakeholder analysis

Key stakeholders will be third country governments including cybersecurity public agencies and competent ministries (ICT, Security, Justice, etc), the private sector, civil society, and end-users. Specifically for the stakeholders at the targeted countries, within their (public, private or civil society) organisations, key duty bearers, policy makers and implementers will be identified and engaged by the Action. Participation will be based on relevance and potential impact but an important consideration will be those institutions that capture data and represent vulnerable and under-represented interests (including women).

Indicatively, other key stakeholders include regional organisations, like the African Union (AU), the Regional Economic Communities in Africa (RECs), the Organization of American States (OAS), and the Association of Southeast Asian Nations (ASEAN); the Commonwealth Telecommunications Organisation (CTO); international organisations as the United Nations agencies (including the International Telecommunication Union – ITU, UN Asian and Pacific Training Centre for Information and Communication Technology for Development UN-APCICT, United Nations Development Programme), the World Bank, the Organisation for Economic Co-operation and Development (OECD), the Meridian Process, the Council of Europe, and the World Economic Forum (WEF); as well as technical organisations such as the Forum for Incident Response and Security Teams (FIRST), AfricaCERT, Asia Pacific Computer Emergency Response Team (AP-CERT), the Trusted Introducer GEANT (TF CSIRT), and the CERT Division of the Software Engineering Institute (SEI) at Carnegie Mellon University.

Finally, at EU level there are several layers of relevant stakeholders, including the European Union Agency for Network and Information Security (ENISA), the European Cybercrime Centre at EUROPOL (EC3), EU Delegations, EU Member States' embassies and Cybersecurity Agencies, as well as EU experts, who will provide expertise and good practice.

The ultimate stakeholders are the citizens in targeted countries who will benefit from improved cybersecurity structures and response capabilities.

Given the dynamism and complexity of the cybersecurity/ critical information infrastructure field, a thorough stakeholder analysis and inclusion of these stakeholders in the context of the needs assessment shall be undertaken to build trust and transparency between different government entities as well as the private sector and civil society.

1.1.3 Priority areas for support/problem analysis

The development community has long recognised that the spread of the internet has created new ways to empower people by providing them with access to services such as banking, health or information, which would otherwise be unavailable. As global internet usage continues to expand with almost three billion people now using online platforms to communicate, work, learn or access government services, the 2030 Agenda for Sustainable Development recognises the importance of ICT and digitalisation as a cross-cutting issue and an enabling means for sustainable development in the context of innovation, with a particular focus on least developed countries (see e.g. target 9.c and 17.8) and with implications on specific areas such as education and gender equality (see e.g. target 4.d, 5.d).

In the past ten years, broad ICT strategies have been adopted by especially developing countries that seek to expand the services they provide to their citizens to boost their economic development. According to the World Bank, it is estimated that for every 10% of the population connected to the Internet, GDP grows by 1 to 2% (October 2014).

However, the promotion of ICT as a means for achieving sustainable development will be futile if it is not accompanied by a serious discussion about the need to have an underlying digital environment, including infrastructure and devices connected to it, that are safe and secure. Addressing the vulnerabilities stemming from the proliferation of ICT infrastructure and internet applications is key to allow for governments and societies to reap the benefits of the internet on human development. As highlighted by the World Development Report 2014, "the consequences of mismanaged risks may destroy lives, assets, trust, and social stability. And it is often the poor who are hit the hardest" (World Bank, 2014). The challenge is even more pressing given that the fastest growing numbers of internet users are in developing countries – in particular in Africa and Asia.

Consequently, capacity building – in addition to market mechanisms – has become a key approach which endeavours to ensure a minimum level of cybersecurity across the globe. Evidently, not all the countries in the world have equal technical capabilities, preparedness and legal framework to address cyber threats. Many policy-makers nowadays are looking for models of how to structure the capacity building efforts, what methods to use and how to measure the efficiency of these efforts.

For a successful capacity building model, best practices from development cooperation experience and cybersecurity should be identified and integrated. Lessons learnt from the EU's internal efforts to enhance its cyber capabilities particularly as elaborated by the European Union Agency for Network and Information Security (ENISA), highlights that capacity building in national cybersecurity should be coupled with efforts of building safer and more reliable connections and communication networks worldwide.

It should be recalled that critical infrastructure is often owned by the private sector.[2] The specification of critical infrastructures depends on the country but private sector involvement in both preventive measures and cybersecurity aspects has increased exponentially and needs to be included in any cybersecurity capacity building programme for it to be sustainable since the private sector needs to play an integral role in the implementation of a national cybersecurity strategy.

2 RISKS AND ASSUMPTIONS

For the good implementation of the activities, it is assumed that beneficiary countries will demonstrate good political will and be disposed for sub-regional, regional and trans-regional cooperation and exchange of information. It is also assumed that beneficiary countries will ensure sustainability and durability to the project by making available the necessary human, financial and material resources to make use and maintain the expertise, potential equipment and applications provided. Close cooperation with the relevant stakeholders in the Beneficiary Countries is crucial in order to address and mitigate potential risks. A participatory approach should be applied throughout the Implementation Phase, including with relevant local stakeholders in the decision-making process in the form of national multi-disciplinary teams that actively participate in the projects activities.

Risks	**Risk level (H/M/L)**	**Mitigating measures**
Political instability and insecurity in the	M	Flexibility in projects activities to allow for shift of

[2] Indicatively: financial services (banking, insurance, credit card companies), utilities sector (electric, gas, oil and water firms), transport sector (fuel supply, railway network, airports, and harbours, inland shipping), telecommunications sector (ISP, communication including mobile communication providers), food sector (agriculture, food production and distribution), and medical sector.

beneficiary countries that will disrupt the projects activities		country focus.
Lack of commitment by the beneficiary country authorities to cooperate	M	For the selection of priority countries, engagement will be pursued only with those demonstrating clear political will and commitment to change management.
Frequent government restructuring, lack of clear delineation of duties and responsibilities between relevant agencies and changes to government agenda reducing strategic outlook on cybersecurity	H	Risk assessments and strong involvement of implementers will mitigate this risk. In addition, for the selection of priority countries, engagement will be pursued only with those demonstrating clear political will and determination for change management.
Challenge to conduct needs assessment from both beneficiary and implementer perspective, and not only from one side	M	Ensure a multi-stakeholder approach with frequent agreement/alignment between beneficiary and implementer/donor
Lack of willingness to address CIIP capacity building on a multi-stakeholders basis and committing to the rule of law and human rights aspects	M	For the selection of priority countries, engagement will be pursued only with those demonstrating clear political will and determination for change management.
Weak institutional capacity and/or low political will to cooperate among neighbours remain a constant challenge to effectively cooperate in addressing trans-national cyber incidents	M	Through increased awareness, peer pressure for action and other means, this risk will be mitigated.
Lack of synergies between this Action and other relevant capacity building programmes at national and regional level.	L	Regular coordination with EU HQ services, EU Delegations and engaged EU MS and other donors in countries where the activities take place will be pursued.
Assumptions		
– The Governments of the beneficiary countries are committed to cooperate both at a national and regional level. – All institutions involved in the Project are committed to the overall objective and purpose of the Action throughout the duration of the Implementation Phase and ready to develop a working cooperation agenda – The responsiveness, financial and technical capacity of the beneficiary countries will not decline in the forthcoming years. – Sufficient capacities at national and (sub-)regional levels can be mobilised for participation in the activities.		

3 LESSONS LEARNT, COMPLEMENTARITY AND CROSS-CUTTING ISSUES

3.1 Lessons learnt

There are several common lessons learnt from the security-related actions implemented in the framework of IcSP. The challenging security and political context in many third countries, as well as obstacles as massive staff rotation in beneficiary institutions and agencies, can be obstacles in achieving progress or attaining significant consolidation of results. The role of partner countries in planning the activities has to be strong in order to facilitate greater ownership and to enhance the effectiveness and sustainability of the actions. A demand-driven approach on the basis of a comprehensive needs assessment is therefore necessary. In addition, the incorporation of human rights safeguards in the design and implementation of such actions is vital to ensure that EU values are reflected throughout the implementation of activities.

Specifically in the area of cybersecurity, one of the main challenges and lessons learnt is that the policy and technical communities and stakeholders do not cooperate, especially between the national security authorities and the business sector. Different communities, officials/diplomats, security experts, and law enforcement and development agencies need to work together more effectively in order to ensure greater security of networks and critical infrastructure. Evidently, cybersecurity, especially when owned by a defence, law-enforcement or intelligence community in a country can complicate trust-building between different policy communities.

On a technical level, in relation to CERT capacity building, it seems that experts are working well together due to the nature and aims of their work. On the other hand, in the strategic realm close attention is necessary for fostering a multi-stakeholder involvement. In terms of the potentially leading role academia can play, while many universities in third countries have curricula in place, there is lack of infrastructure to efficiently execute the research agenda.

3.2 Complementarity, synergy and donor coordination

In general, coordination with the EU Member States is ensured in the relevant Council Working Group, namely the Friends of Presidency Group on Cyber Issues (FoP). Coordination in the different strategy frameworks is combined with political and technical dialogue and exchange of information with EU Member States.

The EU is a founding member of the Global Forum on Cyber Expertise (GFCE) launched by the Netherlands in 2015 and its participation to the Forum will allow for exchange of information to avoid overlaps and even identify potential synergies with other donors.

In addition, coordination shall take place, most notably with the United States, Japan, and Republic of Korea, in the context of the respective EU Cyber Dialogues, as well as with and implementing agencies on the ground such as the International Telecommunications Union (ITU), the Organisation of American States (OAS) and the Commonwealth Telecommunications Organisation (CTO). An overview of donor coordination on the specific Action within this broader area of support by the IcSP shall be provided in the relevant project description of the Action.

In the context of the EU's external financing instruments, although there are several ICT and e-governance related actions, to date only IcSP has financed an action focusing entirely on cybersecurity. Indicatively, complementarity shall be pursued with the cybersecurity initiatives under the GFCE, and where appropriate with ongoing EU-funded ICT-related actions, inter alia: EUMEDCONNECT 3; Trans-Eurasia Information Network (TEIN); E@P Connect; AfricaConnect and African Internet Exchange System (AXIS).

In addition, close coordination and synergies shall be pursued with actions that are being prepared, especially the future action "Accessing the Digital Dividend in Africa" under the DCI Pan-African Programme, in order to ensure the coherent promotion of relevant, interlinked EU policies (ex. on ICT/spectrum management and internet governance) with the African partners and especially with the African Union. Coordination should also be sought with a planned cybersecurity project implemented by Lux-Dev targeting the African Union Commission.

3.3 Cross-cutting issues

All Critical Information Infrastructure Protection (CIIP) issues, also in relation to capacity building, involve a wide range of stakeholders including from national security and law enforcement agencies. Therefore, particular focus should be placed in the incorporation of safeguards in the proposed action in relation to human rights, data protection and good governance, in line with the EU Cybersecurity Strategy, the EU Strategic Framework and

Action Plan on Human Rights and Democracy, and the EU Human Rights Guidelines on Freedom of Expression Online and Offline. The 2015 EU Council Conclusions on Cyber Diplomacy reaffirm the need to "foster open and prosperous societies through cyber capacity building measures in third countries that enhances the promotion and protection of the right to freedom of expression and access to information and that enables citizens to fully enjoy the social, cultural and economic benefits of cyberspace, including by promoting more secure digital infrastructures".

In providing technical assistance and capacity building, the issue of corruption should be carefully considered, in particular with regards to the control and audit of programmatic funds. Programme implementers must observe regulatory measures to mitigate funds transfers to politically exposed persons or other individuals or entities that may abuse programmatic arrangements. To mitigate the challenges posed by endemic corruption, anti-corruption actions will be comprehensively integrated into all parts of the training and awareness raising activities.

To ensure compliance of the proposed action with the obligations stipulated in Article 10 ("Human rights") of Regulation (EU) No 230/2014, a clear human rights perspective should be incorporated throughout the different stages of the project cycle (project design/formulation; monitoring of implementation; evaluation) on the basis of the operational guidance developed to this end by the European Commission (https://ec.europa.eu/europeaid/operational-human-rights-guidance-eu-external-cooperation-actions-addressing-terrorism-organised_en). Any potential flow-on risk on the respect of human rights should be constantly monitored and mitigating measures need to be foreseen.

4 DESCRIPTION OF THE ACTION

4.1 Objectives/results and options

The **overall objective** of the proposed action is to allow the citizens of developing countries enjoy the digital dividends of an open, free, secure and resilent cyberspace.

The **specific objective** of the proposed action is to increase the security and resilience of critical information infrastructure and networks supporting the critical services of third countries while ensuring compliance with human rights and the rule of law. The specific objective will be pursued by supporting the adoption and implementation of a comprehensive set of policy, organisational, and technical measures that will increase their cybersecurity preparedness, following a multi-stakeholder and human rights compliant approach.

In order to meet the objectives mentioned above, the proposed action will be designed to deliver three results, described below.

All of these results are mutually reinforcing, building on a national, regional and transregional approach, promoting EU best practice and ensuring compliance with human rights. Given the considerable disparities in the level and maturity of Internet, telecommunication and ICT infrastructure in third countries, their needs are divergent. In addressing the security-development nexus and the mandate of the EU's "Agenda for Change" and in line with the EU's commitments in relation to the aid effectiveness agenda (2005 Paris Declaration on Aid Effectiveness, 2008 Accra Agenda for Action, 2011 Busan Partnership for Effective Development Cooperation, 2015), particular focus should be placed on local ownership in the pursuit of sustainable results. The elaboration of an assessment involving all relevant national stakeholders in establishing their needs should be the basis for the engagement with third countries in every result area described hereby.

Result 1: Increased awareness of decision-makers on cybersecurity issues and adoption of consistent, actionable national cyber strategies in priority countries by fostering a multistakeholder approach and promoting the establishment of appropriate coordination frameworks and structures amongst public sector entities themselves and also with the private sector, both at policy and operational levels.

In a constantly changing cyber threats environment, countries need to have flexible and dynamic cyber security strategies to meet new global threats. A national cyber security strategy is a plan of actions designed to improve the security and resilience of national infrastructures and services. It is a high-level policy approach to cyber security that establishes a range of national objectives and priorities that should be achieved in a specific timeframe. A National Cyber Security Strategy (NCSS) as a key policy feature, providing a framework where competing policy objectives are appropriately balanced and helping countries tackle risks which have the potential to undermine the achievement of economic and social benefits of cyberspace.

However, the increasing reliance on cyber environment has posed new challenges for both public and private sector entities tasked with the protection of critical infrastructure and sensitive information. It can no longer be assumed that an information system can be adequately protected against advanced targeted attacks. There is no such thing as absolute security, but individuals, businesses and governments must do everything to make attacks as difficult as possible and to prepare for them. It is therefore paramount that all stakeholders not only invest in the direct protection of Information and Communication Systems and Technologies but also invest in detection and response capabilities regarding threats. It is equally important to have in place the necessary organisational frameworks enabling and facilitating cooperation and information sharing between national authorities (including law enforcement) and the private sector, as well as internationally.

The public-private partnership is crucial in the cyber security domain because most of the information and communications networks are owned and operated by the private sector, both nationally and internationally. In addition, partnerships between academia and private industry are also important for innovative solutions and real world applications. A cooperative approach, promoting a network amongst these different actors, should be fostered as part of the strategy development.

Result 2: Increased local operational capacities to adequately prevent, respond to and address cyber attacks and/or accidental failures through strengthened Computer Emergency Response Teams and improved formal and informal cooperation in the national cyber ecosystem of third countries.

A Computer Emergency Response Team (CERT) is a concrete organisational entity that is assigned the responsibility for coordinating and supporting the response to computer security incidents or events. Their objective is to minimise and control the damage resulting from incidents, provide effective guidance for response and recovery and work to prevent future incidents. In order to foster effective CERTs, a thorough understanding of constituent needs is necessary, instead of generic approaches. As a result, the support provided for the development of a CERT's capacities should be based on established best practice that is adapted to the local context and provide a viable, cost effective and culturally appropriate development framework.

Assistance in the enhancement of CERTS' capabilities should focus on three main strands: organisational (internal structure, allocation of resources), technical (incident handling capabilities and proactive services) and cooperational (national inter-agency cooperation as well as international cooperation).

The security and resilience of national cyber-infrastructure is the joint responsibility of all stakeholders, including operators, service providers, software/hardware providers, end-users, public bodies and national governments. By enhancing CERTs' capacities it allows them to become a key actor in the national structure and be considered as a reliable service when an incident happens both by government institutions but also the private sector. For CERTs to meet their objectives, sustained and effective cooperation at national and international levels is indispensable. The model of cooperation promoted should fit the country's institutional structure and culture. The long-term objective through the increased capacities of national CERTs is to facilitate their introduction and consolidation in the international CERT community.

Result 3: Increased trust and enhanced regional, trans-regional and international cooperation on cybersecurity issues through the promotion of formal and informal networks for sharing of best practices and incident information.

Fostering an international approach to the problems and to the solutions, and supporting international cooperation and data sharing is fundamental in light of the trans-national nature of cybersecurity threats. Effective cooperation between communities at all levels is required to facilitate the exchange of information and knowledge needed to reduce vulnerabilities and provide effective responses to cyber incidents. The international cooperation has two aspects: cooperation with other governmental bodies regarding investigation of cyber incidents and sharing of operational information, but also cooperation among law enforcement institutions, cooperation with private entities and cooperation between CERTs.

The cooperation with "champions" in different (sub-)regions and the promotion of regional competence hubs in the regions is seen as a crucial element for the long-term success and sustainability of any capacity building initiative with a global scope. It is expected that through a phased approach, these countries/partners would encourage changes in and between their regions, and start cooperation gradually around common interest areas. In this context, involvement of existing platforms and stakeholders at regional and transregional levels should be prioritised.

4.2 Main activities

To achieve the results mentioned above, main activities will indicatively include:

- national, regional and inter-regional training modules and mentoring cycles addressing the concerned stakeholders (also via a train-the-trainers approach);
- providing technical assistance (which may be coupled with the supply of corresponding equipment where necessary and appropriate);
- undertaking of table-top exercises and mock operations;
- facilitation of operational meetings promoting inter-agency and trans-national cooperation in actual cyber incidents;
- support for the organisation of joint cyber operations and investigations;
- incorporating modules on human rights, data protection safeguards and oversight;
- preparation of handbooks;
- supporting, promoting and further consolidating existing regional networks;

- promoting liaison and virtual information and the use of IT tools.

4.3 Intervention logic

The rationale in the definition of the above-described result areas is based on the fact that these three dimensions (strategic, technical and cooperational) are the tenet of any comprehensive cybersecurity conceptual framework. From the outset, setting up the necessary strategic frameworks at a national level is fundamental in allowing third countries to assess and define their needs and identify roles and responsibilities in a structured manner through a national cybersecurity strategy.

Moreover, many developing countries have limited capacity to monitor and manage the incidents in cyberspace. To build this capacity, the introduction of both technological and organisational measures for better incident management is key. The minimum requirements are needed for setting up the national Computer Emergency Response Teams (CERTs), including specialised training, acquiring equipment and exchange of best practices within the international professional CERT networks. Effective cybersecurity capacity building needs a functioning national CERT, which will be the center of the coordination efforts in a country and feeds information to law enforcement and acts as an interface between the government agencies and the private sector. National CERT, private sector and information security networks in country need to be brought together for long-term sustainable incident response and monitoring system.

In addition, the fostering of a community of trust amongst countries at a regional, transregional and international level in order to share information and cooperate in incidence response handling is a prerequisite for effective cooperation.

A key element of engagement with the selected third countries includes the establishment of national coordination project teams, involving relevant authorities and institutions, as well as partnering with national training academies wherever applicable in order to incorporate the training courses in their curricula as a basic element of sustainability.

Given that the available resources under the external financing possibilities for third countries are limited, there is a need to prioritise any future engagement. In order to identify countries or regions where the future IcSP cybersecurity action should focus, in line with its requirement for a transregional focus, set of criteria has been developed (on the basis of lessons learnt from the on-going IcSP pilot project,) to lead the reflections and analysis at the stage of the project's inception phase. These include:

- Minimum existing ICT infrastructure (incl. existing incident response capability in the country)
- Expressed political commitment or will to engage/existing buy-in / high likelihood of local ownership and change management motivation (demand-driven approach)
- Strategic role in a (sub)region with the potential to act as a champion/influencer/regional hub and possibly have a ripple/multiplier effect
- Eagerness for international cooperation (including readiness and capability at a later stage to engage at a South-South/Triangular cooperation level)
- A non-restrictive human rights environment / a commitment to the Rule of Law (or at least the respective governments' demonstrated ambition to this end)
- Impact-orientation, ie focus on where our actions can make difference (best return for investment / risk assessment)
- Potential influence on cyber policies (ie. promotion of EU policies and values)

- Growth in internet use and penetration
- Rising cyber threat potential
- No overlap with other donors / exploration of possible synergies

5 IMPLEMENTATION

5.1 Financing agreement

In order to implement this action, it is not foreseen to conclude a financing agreement with the partner country, referred to in Article 184(2)(b) of Regulation (EU, Euratom) No 966/2012.

5.2 Indicative implementation period

The indicative operational implementation period of this action, during which the activities described in section 4.1 will be carried out and the corresponding contracts and agreements implemented, is 72 months from the date of adoption by the Commission of this Action Document.

Extensions of the implementation period may be agreed by the Commission's authorising officer responsible by amending this decision and the relevant contracts and agreements; such amendments to this decision constitute technical amendments in the sense of point (i) of Article 2(3)(c) of Regulation (EU) No 236/2014.

5.3 Implementation modalities for an action under project modality

5.3.1 Indirect management with a Member State

This action may be implemented in indirect management with a Member State in accordance with Article 58(1)(c) of Regulation (EU, Euratom) No 966/2012, and specifically with the Northern Ireland Co-Operation Overseas LTD (NI-CO)[3], on the basis of the result of a request for an expression of interest to eligible EU Member State entities. If negotiations with the above-mentioned entrusted entity (NI-CO) fail, this action may be implemented in indirect management with Expertise France International. This implementation entails to manage and be responsible for the execution of the action. This implementation is justified due to the combined nature of the activities foreseen (provision of capacity building and technical assistance to strengthen relevant actors' cyber resilience and their ability to address cyber incidents in accordance with the principles of rule of law as well as budget-implementation tasks) but also in order to reinforce the nexus between the internal and the external dimensions of the EU's security policy and to avoid duplication and overlap with similar activities.

EU Member States agencies are best placed to cover the wide range of fields of expertise required to perform interventions in the diverse fields of cybersecurity capacity building, cyber incident handling, information sharing, and regional cooperation while ensuring confidentiality.

The entrusted entity would carry out the following budget-implementation tasks: acting as contracting authority concluding, monitoring and managing contracts, carrying out payments, and recovering moneys due; management of procurement procedures for hiring staff,

[3] In collaboration with inter alia the Foreign and Commonwealth Office, the Netherland's Ministry of Foreign Affairs, the Estonian Information Systems Authority and the Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH.

purchasing goods and equipment, hiring consulting services, and any other relevant transactions.

Involvement of expertise from relevant EU Decentralised Agencies, such as the European Union Agency for Network and Information Security (ENISA), should be pursued to the extent possible subject to their mandate, priorities, procedures and resources and in coordination with their partner Directorate General of the European Commission.

5.4 Scope of geographical eligibility for procurement and grants

The geographical eligibility in terms of place of establishment for participating in procurement and grant award procedures and in terms of origin of supplies purchased as established in the basic act and set out in the relevant contractual documents shall apply.

The Commission's authorising officer responsible may extend the geographical eligibility in accordance with Article 9(2)(b) of Regulation (EU) No 236/2014 on the basis of urgency or of unavailability of products and services in the markets of the countries concerned, or in other duly substantiated cases where the eligibility rules would make the realisation of this action impossible or exceedingly difficult.

5.5 Indicative budget

	EU contribution (amount in EUR)	**Indicative third party contribution, in currency identified**
5.3.1.1. – Indirect management with MS	11 000 000	0
5.8 – Evaluation, 5.10 - Audit	will be covered by another decision	N.A.
Totals	11 000 000	0

5.6 Organisational set-up and responsibilities

The implementation of this Action will be coordinated and led by an EU Member State. The responsibilities of the implementing partner will include, *inter alia*:

In relation to the inception phase of the Action:

- Undertaking a comprehensive needs-assessment and a stakeholder mapping of the beneficiary countries;
- Defining a working plan of activities jointly with the beneficiary institutions;
- Identifying the most appropriate bodies/experts/institutions for the transfer of their know-how;
- Designing a human rights risk mitigation strategy;
- Formulating the communication and visibility strategy.

In relation to the implementation phase of the Action:

- Undertaking the tasks of each activity by mobilising the appropriate and necessary expertise and promoting EU best practice;
- Organising events of strategic dimension at a sub-regional, regional and transregional level;
- Setting up a system of indicators in order to follow up the activities and measure the results;
- Reinforcing the collaborative links of the beneficiary countries' relative institutions/bodies amongst themselves and with their counterparts in the EU;
- Promoting the dissemination of good practices and the results of the Action;

- Ensuring coordination with other donors.

In order to guarantee the global strategic orientation of the programme, the Contracting Authority together with the implementing partner will establish and co-chair a Steering Committee. This Committee will also be tasked with issuing opinions and recommendations on the working plan submitted by the implementing partner, ensuring the relevance of the indicators measuring the results of the Action as well promoting synergies with actions of bilateral and regional cooperation of the EU and its Member States and coordination with the programmes and projects financed by other donors.

5.7 Performance monitoring and reporting

In order to determine whether the cybersecurity and cyber resilience of selected third countries has improved, several independent indexes and reports mentioned in the Appendix (Logframe) will be used. Considering the sensitive isues linked to cybersecurity, such as surveillance, and data protection, civil society scrutiny reports should be also taken into account in the process of the action's performsance monitoring. The Appendix (Logframe) will be adjusted at the preparatory phase of the action in particular to provide up-to-date baseline figures, and it shall evolve during the lifetime of the action to allow for effective 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 partner’s responsibilities. To this aim, the implementing partner 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 (outputs and direct outcomes) as measured by corresponding indicators, using as reference the logframe matrix (for project modality) or the list of result indicators (for budget support). 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 project 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).

5.8 Evaluation

Having regard to the nature of the action, an ex-post evaluation will be carried out for this action or its components via independent consultants. It will be carried out for accountability and learning purposes at various levels (including for policy revision), taking into account in particular the fact that this will be the first large-scale, trans-regional action financed by IcSP focusing on cybersecurity.

The Commission shall inform the implementing partner at least two weeks in advance of the dates foreseen for the evaluation missions. The implementing partner shall collaborate efficiently and effectively with the evaluation experts, and inter alia provide them with all necessary information and documentation, as well as access to the project premises and activities. The evaluation reports shall be shared with the partner country and other key stakeholders. The implementing partner and the Commission shall analyse the conclusions and recommendations of the evaluations and, where appropriate, in agreement with the partner country, jointly decide on the follow-up actions to be taken and any adjustments necessary, including, if indicated, the reorientation of the project. The financing of the evaluation shall be covered by another measure constituting a financing decision.

5.9 Audit

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 for one or several contracts or agreements. The financing of the audit shall be covered by another measure constituting a financing decision.

5.10 Communication and 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 and supported with the budget indicated in section 5.5 above.

In terms of legal obligations on communication and visibility, the measures shall be implemented by the Commission, the partner country, contractors, grant beneficiaries and/or entrusted entities. Appropriate contractual obligations shall be included in, respectively, the financing agreement, procurement and grant contracts, and delegation agreements.

The Communication and Visibility Manual for European Union External Action shall be used to establish the Communication and Visibility Plan of the Action and the appropriate contractual obligations.

APPENDIX - INDICATIVE LOGFRAME MATRIX (FOR PROJECT MODALITY)

The activities, the expected outputs and all the indicators, targets and baselines included in the logframe matrix are indicative and may be updated during the implementation of the action, no amendment being required to the financing decision. When it is not possible to determine the outputs of an action at formulation stage, intermediary outcomes should be presented and the outputs defined during inception of the overall programme and its components. The indicative logframe matrix will evolve during the lifetime of the action: new lines will be added for including the activities as well as new columns for intermediary targets (milestones) for the output and outcome indicators whenever it is relevant for monitoring and reporting purposes. Note also that indicators should be disaggregated by sex whenever relevant.

	Results chain	Indicators	Baselines (incl. reference year)	Targets (incl. reference year)	Sources and means of verification	Assumptions
Overall objective: Impact	The citizens of developing countries enjoy the digital dividends of an open, free, secure and resilent cyberspace.	Rate of selected third countries' progress towards attaining SDGs 9a and 16a	To be determined by the implementing partner in the preparatory phase, reflecting on the selected third countries' state of play (2017)	To be determined by the implementing partner in the preparatory phase (2020)	Assessment of the project at EU dialogues with selected third countries/relevant regional organisations National progress reports on SDG Target 9a and 16a World Bank country statistical data on ICT (cyber-related aspects) UNDP Human Development Report Oxford Centre's Cyber Capability Maturity Multi-Dimemsional Model Potomac Institute's Cyber Readiness Index Evaluation(s) (Midterm review and final evaluation)	Traget countries will ensure sustainability and durability to the action by making available the necessary human, financial, and material resources The responsiveness, financial and technical capacity of the target countries will not decline in the coming years
Specific objective(s): Outcome(s)	The security and resilience of critical information infrastructure and networks supporting the critical services of third countries, while ensuring compliance with human rights and the	1. Improvement of country position at ITU's Global Cybersecurity and Cyber-wellness Index	1. Country position at ITU's Global Cybersecurity and Cyber-wellness Index (in 2017, ie at the start of the action)	1. Improvement of country position at ITU's Global Cybersecurity and Cyber-wellness Index by at least 3 places (2020)	1. Global Cybersecurity Index	The action is not disrupted by adverse events, such as a fragile security situation, natural hazards, public health crises.

	rule of law, is increased, It shall be pursued by supporting the adoption and implementation of a comprehensive set of policy, organisational, and technical measures that will increase their cybersecurity preparedness, following a multi-stakeholder and human rights compliant approach.	2. Improvement of country position at the CyberGreen Index	2. Country position at CyberGreen Index (2017)	2. Improvement of country position in the CyberGreen Index by at least 3 places (2020)	2. CyberGreen Index	Political stability in the target countries The allocated budget is sufficient both for the full duration and the full scope of the action. The application of new cybersecurity startegies and associated activities does not have an adverse impact on human righst in the target countries
		3. Improvement of country position at the Digital Evolution Index (Fletcher School, Tufts University, 2017)	3. Country position at the Digital Evolution Index (Fletcher School, Tufts University, 2017)	3. Improvement of country position at the Digital Evolution Index by at least 3 places (Fletcher School, Tufts University, 2020)	3. Digital Evolution Index	
		4. Improvement of country position at the Freedom House's Freedom on the Net report (2017)	4. Country position at the Freedom House's Freedom on the Net report (2017)	4. Improvement (or non-deterioration) of country position at the Freedom House's Freedom on the Net report by at least 3 places (2020)	4. Freedom on the Net Report	
		5. Active involvement of civil society organisations in the cybersecurity decision making processes.	5. No or marginal civil society involvement in decision making in priority countries - to be verified/determined by the implementing partner at the inception phase for each selected third country (2007)	5. Establishment of informal or formal consultation srtrucures between the government and civil society in relation to cybersecurity in all selected third countries - to be confimed by the implementing partner at the inception phase (2020)	5. Civil society scrutiny reports on oversight of national cybersecurity policies and executive measures (privacy/ surveillance, freedom of expression online, access to content)	
Outputs	Output 1: Increased awareness of decision-makers on cybersecurity issues and adoption of consistent, actionable national cyber strategies in priority countries by fostering a multistakeholder approach and promoting the establishment of appropriate coordination frameworks and	1. Number of target countries adopting national cyber strategies, Action Plans and Critical Information Infrastructure Protection policies.	1. 0 (2017)	1. From 8 to 10 (2020)	1. Project update reports National reports from cyber-coordinating Ministries ENISA reports Press releases	Good cooperation amongst Ministries and Agencies National governments actively seek the involvement of the private sector and civil society Ability of the

	structures amongst public sector entities themselves and also with the private sector, both at policy and operational levels.	2. Number of key private sector entities (especially from critical infrastructure/services) and civil society (including women representatives) participating in the development of the national cyber strategies.	2. 0 (2017)	2. To be determined by the implementing partner for each selected third country at the inception phase, depending on the local industry configuration/maturity and civil society environment.	2. Project update reports National reports from cyber-coordinating Ministries Civil society reports Press releases	implementing partner to mobilise timely the right expertise for the roll out of activities Translation and interpretation services for the roll out of activities do not create delays
		3. Number of cooperation MoUs signed between national governments and private sector actors.	3. 0 (2017)	3. At laest 2 per country (2020)	3. Project update reports National reports from cyber-coordinating Ministries Press releases	
		4. Number of countries gaining membership to international professional cyber associations.	4. 0 (2017)	4. From 7 to 10 (2020)	4. Project update reports National government reports FIRST Trusted Introducer	
	Output 2: Increased local operational capacities to adequately prevent, respond to and address cyber attacks and/or accidental failures through strengthened Computer Emergency Response Teams and improved formal and informal cooperation in the national cyber ecosystem of third countries.	1. Number of incident response organisations and national Computer Emergency Response Teams (CERTs) created and/or developed in the target countries that are recognized by the private sector and key government agencies as national and international focal points for cyber incidents	1. From 0 to 2 (2017)	From 8 to 10 (2020)	1. Project update reports National legislation on the setting up of national CERTs National government reports, including Statistical Office (NSO) progress reports National CERTs reports/ websites Project update reports	National legislative process for the establishment of CERTs is not blocked Allocation of funding from the national budget for the minimum CERT set up and staff recruitment is approved Good cooperation amongst Ministries and

		2. Number of incident management/response cases monitored and handled by national computer emergency response teams (CERTs)	2. To be determined by the implementing patrner for each selected third country at the inception phase.	2. Increase by 50% (2020)	2. Project update reports National government reports, including Statistical Office (NSO) progress reports National CERTs reports/ websites Security Incident Management Maturity Model 3 (SIM3) Assessment Results	Agencies Required software and hardware is available Trained staff remain within their institutions beyond the capacity building exercise Ability of the implementing partner to mobilise timely the right expertise for the roll out of activities Translation and interpretation services for the roll out of activities do not create delays
		3. Number of national incident response organisation or CERTs that have a training programme in place and are part of the international professional cyber associations (e.g. FIRST, Trusted Introducer)	3. From 0 to 2 (2017)	3. From 8 to 10 (2020)	3. Project update reports National CERTs reports/ websites FIRST Trusted Introducer Security Incident Management Maturity Model 3 (SIM3) Assessment Results	
		4. Number of countries where the national incident response organizations or CERTs are organizationally linked to the country's Critical Infrastructure Protection system, and there is an elected/political/democratic oversight on the activities of this technical organisation	4. To be determined by the implementing patrner for each selected third country at the inception phase.	4. To be determined by the implementing patrner for each selected third country at the inception phase.	4. Project update reports National legislation on the setting up of national CERTs and their oversight National government reports, including Statistical Office (NSO) progress reports National CERTs reports/ websites Security Incident Management Maturity Model 3 (SIM3) Assessment Results	

		5. Number of table-top exercises and mock operations undertaken within the project framework.	5. 0 (2016)	5. At least 5 per year (at national and trans-/regional level)	5. Project update reports National CERTs reports/ websites	
	Output 3: Increased trust and enhanced regional, trans-regional and international cooperation on cybersecurity issues through the promotion of formal and informal networks for sharing of best practices and incident information.	1. Number of formal or informal cyber information sharing networks created and/or enhanced in targeted regions, that facilitate incident report sharing/early warning/mitigation of serious cyber incidents.	1. 0 (2017)	1. From 3 to 5 (2020)	1. Project update reports National CERTs reports Regional organisations' reports Press releases	Minimum existing trust for good cooperation amongst countries Required software and hardware is available Trained staff remain within their institutions beyond the capacity building exercise Translation and interpretation services for the roll out of activities do not create delays Ability of the implementing partner to mobilise timely the right expertise for the roll out of activities
		2. Number of operational meetings promoting inter-agency and trans-national cooperation in actual cyber incidents.	2. 0 (2017)	2. From 2 to 5 per year	2. Project update reports National CERTs reports Regional organisations' reports Press releases	
		3. Number of joint cyber operations and investigations.	3. 0 (2017)	3. Up to 15 (2020)	3. Project update reports National CERTs reports Regional organisations' reports Press releases	