This action is funded by the European Union

ANNEX 2

of the Commission Implementing Decision on the Annual Action Programme 2016 – Part 1 in favour of ENI South countries

Action Document for 2016 Security Package

1. Title/basic act/ CRIS number	2016 Security Package CRIS number: ENI/2016/039-362 financed under the European Neighbourhood Instrument			
2. Zone benefiting from the action/location	The action shall be carried out at the following location: Neighbourhood South countries			
3. Programming document	Programming of the European Neighbourhood Instrument (ENI) - 2014-2020. Regional South Strategy Paper (2014-2020) and Multiannual Indicative Programme (2014-2017)			
4. Sector of concentration/ thematic area	Building a partnership for liberty, democracy and security	DEV. Aid: YES		
5. Amounts concerned	Total estimated cost: EUR 11 million Total amount of EU budget contribution EUR 11 million Budget line: 22 04 01 03			
6. Aid modality(ies) and implementation modality(ies)	Project Modality Indirect management with a Member State agency for the component 1 on Civil Protection. Indirect management with the Council of Europe for the component 2 on Cybercrime and with Interpol for the component 3 on Information Exchange.			
7 a) DAC code(s)	74010 - Disaster prevention and preparedness for component 1 15210 - Security system management and reform for components 2 & 3			
b) Main Delivery Channel	52000 - Other for components 1 & 3 47138 - Council of Europe for component 2			
8. Markers (from CRIS DAC form)	**General policy objective**	**Not targeted**	**Significant objective**	**Main objective**
	Participation development/good governance	☐	☐	Yes
	Aid to environment	No	☐	☐
	Gender equality (including Women In Development)	No	☐	☐
	Trade Development	No	☐	☐

	Reproductive, Maternal, New born and child health	No	☐	☐
	RIO Convention markers	**Not targeted**	**Significant objective**	**Main objective**
	Biological diversity	No	☐	☐
	Combat desertification	No	☐	☐
	Climate change mitigation	No	☐	☐
	Climate change adaptation	No	☐	☐
9. Global Public Goods and Challenges (GPGC) thematic flagships	Not applicable			

SUMMARY

All components of this action are priorities set out in the security chapter of the European Neighbourhood Policy (ENP) Review.

(i) PPRD South III (Prevention, Preparedness and Response to natural and man-made Disasters, Region South, Phase III): Complementarity with the new regulation of the Union Civil Protection Mechanism (UCPM), the objective is to strengthen partner countries' capacity to develop and implement strategies that build societal resilience against all hazards, natural and man-made, and threats through capacity building activities, legislative and institutional advice, support to cross-border co-operation frameworks, aligned to the UCPM and in cooperation with DG ECHO. The programme will be implemented by an EU Member State agency or consortia thereof.

(ii) Cybercrime@South: The objective is to strengthen the partner countries' capacity to tackle cybercrime and cooperate effectively, in compliance with the Convention on Cybercrime of the Council of Europe (Budapest Convention) which is the only binding international instrument on this issue. The project will provide judicial and law enforcement training and contribute to the drafting of policies, harmonised and effective legislation and increase the awareness of decision-makers. It will also stimulate the co-operation between law enforcement agencies and private internet service providers and contribute to financial investigations.

(iii) Interpol South: Interpol, through its EU Member States, is the largest data provider for Europol, Eurojust and Frontex. The objective is to intensify and accelerate exchange of operational information in the Neighbourhood South, and with EU, on issues related to organised crime, terrorism, smuggling of migrants, trafficking of human beings and trafficking of small arms, and, to this effect, to increase data collection (Foreign Fighters database, Stolen and Lost Documents, iArms and iTrace, notices, Stolen Art Works, etc) from the Neighbourhood South.

1 CONTEXT

1.1 Sector/Country/Regional context/Thematic area

1.1.1 EU Policy Framework

Component 1 – Civil Protection: "The EU should build up partners' early warning, prevention and preparedness capacity offering close partnerships in civil protection and co-operation with the EU's civil protection mechanism."[1]

Succeeding the Community Civil Protection Mechanism established in 2001, the Union Civil Protection Mechanism (UCPM), created by Decision No 1313/2013/EU, aims to strengthen co-operation between the Union and Member States and facilitate coordination in the field of civil protection in order to improve the effectiveness of systems for preventing, preparing for and responding to natural and man-made disasters[2].

Candidate countries and potential candidates which do not participate in the Union Mechanism, as well as countries which are part of the European Neighbourhood Policy (ENP) may also receive a limited financial support for a sub-set of UCPM actions identified in the UCPM Decision.

Component 2 - Cybercrime: "The EU will continue to promote the ratification and implementation of the Budapest Convention on cybercrime with its partners in the Neighbourhood."[3]

The proposed action is in line with the EU policies on cybersecurity and cybercrime, most notably the EU Cybersecurity Strategy[4], cybersecurity being the first line of defence against cybercrime. The communication urges all EU Member States to ratify the Budapest Convention, to implement its provisions as early as possible and to invite third countries to adhere. Cybercrime is one the three priorities of the EU Agenda on Security[5].

We can make a distinction between advanced cybercrime (such as sophisticated attacks against computer hardware and software) and cyber-enabled crime. Many 'traditional' crimes have taken a new turn with the advent of the Internet, such as crimes against children, financial crimes and even terrorism. This is becoming particularly worrying in the Neighbourhood South.

Component 3 – Interpol: As called for the European Neighbourhood Policy (ENP) Communication[6], "with Interpol, the need should be examined to build further law enforcement capacity in neighbouring countries and work on facilitating information exchanges with EU Member States and Europol."

The proposed action will contribute to strengthening a structured dialogue and co-operation between Interpol, the Commission services and the European External Action Service (EEAS). It is justified by the importance of joining forces – within

1 Communication JOIN(2015)500 final "Review of the European Neighbourhood Policy".
2 OJ L 347, 20.12.2013, p. 924.
3 Communication JOIN(2015)500 final "Review of the European Neighbourhood Policy".
4 http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf.
5 COM(2015) 185 final.
6 Communication JOIN(2015)500 final "Review of the European Neighbourhood Policy".

the framework of their respective mandates – against serious and organised cross-border crime including trafficking of human beings, cybercrime, terrorism, all priorities of the EU Agenda on Security[7]. It also recognizes the need to enhance synergies between the internal and external dimensions of security.

1.1.2 Stakeholder analysis

Component 1 – Civil Protection:

Direct beneficiaries are the civil protection agencies and national crisis or disaster risk management agencies in the beneficiary countries. The final beneficiaries are the citizens in general.

The request for civil protection co-operation with the EU was reiterated at the High-Level Round Table discussion with civil protection representatives of the Member States and Neighbourhood countries (May 2015) and reconfirmed during the Steering Committee of the PPRD South II programme (February 2016).

Several Neighbourhood South countries have expressed their interest to enter into an associated partnership with the UCPM, bringing these countries closer to the Mechanism will lead to a better co-operation in the response to disasters and a more structured exchange of knowledge and good practices on prevention and preparedness. While the associated partnerships will in principle be open to all EU Neighbourhood countries, it will be restricted in practice to bilateral activities and to countries that are ready to make a political commitment to pursuing the agreed objectives and that have the capacity to do so. Complementing this, the PPRD project would allow all neighbourhood countries to receive EU support for activities that are fully complementary with principles of the UCPM, even though this support would not be strictly speaking embedded in the UCPM. As was the case in the previous phases, PPRD South will also be the regional platform on disaster preparedness, prevention and response.

Support for the regional civil protection programme is needed since it is the only regional platform available for exchange between countries wishing to enter in an Associated Partnership, countries not ready to do so, and the EU.

Differentiation, greater focus and flexibility have, in fact, been requested by many Neighbourhood countries and are in line with the Review of the ENP.

The 2013 UCPM Decision makes it possible to extend well-defined UCPM co-operation activities (e.g. training, exercises, projects, etc. …) to interested Neighbourhood countries, whilst not being allowed to fully join the UCPM.

Some neighbourhood countries could have a status of "Associated Partner" to the UCPM, which will allow them to join in specific UCPM activities on the basis of an agreed set of principles and objectives.

Since not all countries will have the status of associated partner, this will result in co-operation for the EU Neighbourhood with different degrees of association and therefore the PPRD programme is vital to include the non-associated countries and keep the regional dimension and approach.

[7] COM(2015) 185 final.

Component 2 - Cybercrime:

Direct beneficiaries are law enforcement bodies, prosecutors, judiciary and legislative bodies in beneficiary countries. The final beneficiaries are the citizens in general.

The Budapest Convention is open for accession by any country ready to implement its provisions and to engage in co-operation. Among Southern Neighbourhood countries, Israel and Morocco have been invited to accede and are completing the process of accession. Morocco is a priority country of the joint project[8] of the EU and the Council of Europe "GLACY: Global Action on Cybercrime". The Council of Europe has furthermore been cooperating with Egypt and Jordan on domestic cybercrime legislation on the basis of the Budapest Convention. Algeria, Lebanon and Tunisia have also expressed an interest in the Budapest Convention. Morocco and Tunisia have furthermore been invited to accede to the data protection Convention 108 of the Council of Europe.

Component 3 – Interpol:

Direct beneficiaries are law enforcement bodies of the beneficiary countries. The final beneficiaries are the citizens in general.

Many countries of the Neighbourhood South under-use Interpol tools and services. For instance, despite all North Africa and Middle East countries are connected to I-24/7 (Interpol global secure police communication system), and extension to specialized units being the case in several of these countries, the use of the system by these countries is very modest. When comparing the figures of records in the nominal database (used to issue international alerts) for the year 2015, Neighbourhood South countries reach less than 4,000 compared to 40,000 for the Americas, or 90,000 for Europe. On the Stolen and Lost Travel Documents (SLTD), these same countries have fed the database with only 300,000 records compared to 30 million records for Europe, or 10 million for the Americas. These figures highlight that the capacity and awareness of these countries on a national level need to be enhanced to be able to efficiently share data in their possession with the international community. Expansion to specialized units and to border points (including airports and sea ports) should furthermore be enhanced, promoting an increasingly integrated system between national networks and I-24/7.

Several critical border posts of Neighbourhood South countries are not equipped with a Fixed or Mobile Interpol Network Database (FIND - MIND). For example, in 2013 in Jordan, only the Queen Alia international airport was equipped with a MIND pilot station. None of the other border posts with Syria, Iraq, Israel, Palestine, Saudi Arabia and the Red Sea was equipped. An ongoing bilateral programme[9] is now providing access to more than 10 additional border posts.

1.1.3 Priority areas for support/problem analysis

Component 1 – Civil protection:

[8] Funded by IcSP Art 5, managed by DEVCO B5: http://www.coe.int/en/web/cybercrime/glacy .

[9] Project ESTIJAB (CRIS 336192).

Europe and its Neighbourhood have experienced in the past similar types and magnitude of disasters. The total average economic cost of disasters in Europe is estimated at around EUR 10 billion per year (average 2002 to 2012).

The underlying drivers of these disasters – a mix of climate change, industrialisation and urbanisation – are not disappearing. On the contrary, evidence suggests that the kinds of disasters we witnessed in recent years will be more frequent, with cascading effects, and more intense in the future. In 2015, the adoption of the UN Sendai Framework for Disaster Risk Reduction (DRR) allows the international community to shift from managing disasters to addressing disaster risks, with a focus on prevention and preparedness.

Disasters can easily overwhelm the local or national capacity to respond. This is the reality for all countries. In the past few years we saw such instances happening within the EU, and in our Southern and in our Eastern Neighbourhood.

Three conclusions can be drawn from this. First, a country alone, no matter how big or rich, cannot by itself be fully prepared for all kinds of disasters. Second, coordination, joint efforts and a common response will always be more effective than any country acting on its own. And third, a holistic approach to disaster management, considering all phases of the disaster cycle, and all risks and hazards, is crucial.

In this spirit, and in line with the Union Civil Protection Mechanism and with the Sendai Framework, priority areas have been identified for the PPRD South project:

- More focus on disaster prevention, in particular the identification and assessment of disaster risks and the assessment of the partner countries' capability to manage these risks;

- Improving disaster preparedness, with further work on host nation support, training, exercises, exchanges of experts, peer reviews, advisory missions and projects.

Component 2 - Cybercrime:

Societies all over the world increasingly rely on information and communication technologies (ICT) becoming increasingly vulnerable to threats such as cybercrime. Cybercrime – that is offences against computer systems and by means of computers – affects individuals and in particular vulnerable groups, institutions and organisations as well as States.

This observation is also valid for Southern neighbourhood countries. Security, confidence and trust in ICT are needed to allow these societies exploit the human development potential of ICT.

Governments increasingly consider cybercrime and cybersecurity as matters of national security in particular in the light of terrorist use of the Internet, transnational organised crime in cyberspace and reports on attacks and computer intrusions by States or by non-state cyber actors. In some countries, such threats may trigger repressive measures that in turn may threaten rule of law and human rights principles. It is necessary, therefore, to reconcile the positive obligation of governments to protect society and individuals against crime with rule of law, human rights and data protection requirements.

The approach of the Council of Europe on cybercrime addresses this challenge. It is built on the Budapest Convention on Cybercrime and related instruments, such as

Data Protection Convention 108 and others. Joining the Budapest Convention entails membership in the Cybercrime Convention Committee (T-CY) and thus co-operation with currently 66 States. Furthermore, the Budapest Convention and the work of the T-CY are supported by the implementation of capacity building programmes.

While the overall context of democratic governance, rule of law and human rights is difficult in this region, it should be feasible to cooperate with some priority countries more intensively and associate others to the extent possible. This is explained in the intervention logic.

Component 3 – Interpol:

The success of international police investigations is dependent upon the availability of up-to-date, global data. Interpol facilitates global information sharing by managing a range of criminal information databases which enable the global law enforcement community to connect seemingly unrelated pieces of data, thereby facilitating investigations and enhancing international police co-operation.

Promoting a more intensive use also implies promoting a more active feeding of the available databases. The more data are fed into the systems, the more opportunities are created for detection and interdiction of criminals. More intensive use also assumes more access to the databases through appropriate ICT equipment and connections.

Nowadays, crime has an increasing transnational nature. Criminal actions originate in one country and terminate in another with spill over effects on a regional and sometimes global level. Criminal groups and terrorists work in networks and take advantage of the lack of information sharing by countries to carry out their illegal actions in different jurisdictions. The objective of the international law enforcement community is to neutralize these networks by increasing the capacity to collect, analyse and share information across countries and regions.

As criminal networks increase their capacity to move and communicate transnationally, the international community should counter this phenomenon by using an international law enforcement network ready to share real-time information such as: biometrics, names, stolen passports, DNA, fingerprints and information about firearms. Interpol has the capacity to act as a central multilateral platform to help member countries to populate and make an efficient use of its databases and its secure communication system I-24/7. The possibility given to Interpol member states to share information in a timely manner could help prevent criminal actions and the movement of wanted individuals.

Interpol systems for promoting international exchange of police information do not only consist of the databases and the encrypted network, but also of available specialised task forces such as FUSION for counterterrorism or ISON for the smuggling of migrants.

2 RISKS AND ASSUMPTIONS

Risks	Risk level	Mitigating measures

	(H/M/L)	
Risk of political tensions between partner countries.	M	Partner countries can choose between different schemes of co-operation and actions do not necessarily concern all countries.
Political instability within some of the partner countries.	H	Non-inclusion of countries in crisis will not hamper project implementation, as this is a regional project that can be flexible in the countries it targets.
Lack of commitment to project implementation.	M	Partner countries can choose between different levels of partnerships.
Law enforcement authorities benefiting from training on investigative techniques in cybercrime without the necessary rule of law and human rights safeguards.	H	Applying a differentiated and phased approach. Priority countries Algeria, Morocco, Tunisia and Jordan will benefit of the full support provided the human rights and rule of law safeguards are present. Co-operation with other countries would focus on the strengthening of legislation human rights and rule of law conditions for cybercrime and electronic evidence followed by gradual involvement – if feasible – in the other project activities.
No guaranteed commitment of the partner country to cover the maintenance and operating costs of I24/7	L	If equipment will be provided, this will be a pre-condition.
Assumptions		
Partner countries are willing to reach a higher degree of co-operation within the region and with EU. Partner countries will ensure sustainability and durability to the respective projects by making available the necessary human, financial and material resources.		

3 LESSONS LEARNT, COMPLEMENTARITY AND CROSS-CUTTING ISSUES

3.1 Lessons learnt

Component 1 – Civil Protection:

The preparatory phases and PPRD South I and II were a project-based approach based on service contracts with almost no transition from one phase to the other and no proper handover between contractors. As an example, each contractor had a dedicated website with secured access to information, which at the end of the contract was simply closed. Thus continuity and sustainability were not guaranteed.

The only way to reach continuity and sustainability is to hook up the programme more firmly to a permanent framework, i.e. the UCPM, moving to a more policy-driven approach and institutional relationship, which is more conducive for sustainability.

Not all partner countries are facing the same level of difficulties and the same needs. And not all countries want to reach the same level of co-operation with EU.

In line with the principle of differentiated and demand-driven approach, the outcomes will vary from a simple alignment of countries to best practices, international standards, or EU legislation, to an associated partnership with the Union Civil Protection Mechanism.

Component 2 – Cybercrime:

The EU and the Council of Europe have implemented joint projects against cybercrime within Europe, focusing mainly on the Budapest Convention. These joint projects against cybercrime have been positive, leading to their replication outside the EU.

Within the EU, much experience has been gained during the past decade in particular with respect to the development of standardised and scalable training, co-operation and information sharing between specialised cybercrime units and other fields. The creation of the European Cybercrime Centre (EC3), including the European Cybercrime Training and Education Group (ECTEG) and the EU Cybercrime Task Force, have been pivotal steps for enhancing the EU's capacity in this area and shall allow to share this experience with third countries.

As mentioned below, projects such as GLACY have demonstrated the relevance and feasibility of capacity building activities on cybercrime.

Component 3 – Interpol:

There is a tendency to divide the fight against organised crime and terrorism into vertical specialties such as drug trafficking, trafficking of human beings, cybercrime, terrorism, trafficking of small and light weapons, etc...

Information is collected by different services in different databases, first at national level.

In-depth analysis is only possible if access to the different Interpol databases is available and compatible, allowing for cross-checking.

Information exchange at regional and international level is only possible if these data are uploaded in the Interpol systems. It is of course a question of national sovereignty to decide which information is uploaded. Some countries need to be more convinced about the advantages they can get in return by sharing more information and data via Interpol.

The data must also be compatible with Interpol systems and the processing and sharing of data must also comply with prevailing international standards for human rights, rule of law and data protection, which can require particular training and ex-ante checks. Training is also required on the different possibilities offered by these tools especially through cross-checks for analysis.

Once information is uploaded, access must be available online via secure systems but this is not always the case. Several critical border posts do simply not have this access.

If the action foresees the delivery of equipment, there must be a commitment of the recipient country to provide the necessary resources for operations and maintenance.

During inception, enough time must be foreseen to reach agreement between Interpol, the National Central Bureaus and the Central Authorities in charge of internal security issues of the recipient country since in some countries police services are not the only ones to decide on information exchange. This was exemplified in the project ESTIJAB in Jordan.

3.2 Complementarity, synergy and donor coordination

Component 1 – Civil Protection:

ENI funding will be complementary to ECHO's support to priority ENP country on selected UCPM activities.

In line with the international agreements such as the 2015-2030 Sendai framework, the Sustainable Development Goal and the Paris Climate Agreement, the programme will seek to create synergies with projects engaged more specifically in crisis response and preparedness to natural and man-made disasters at strategic, operational and tactical levels.

Additionally, coordination and complementarities with similar regional or bilateral initiatives in the Western Balkans and in the Eastern Neighbourhood, with ENI and IPA funding, will also be ensured through regular exchanges and the common anchoring to the UCPM.

At bilateral level, a twinning on civil protection was launched in Algeria and different countries have used the TAIEX programme. Algeria, Egypt, Palestine, Tunisia, Israel, Jordan and Morocco have benefited from the call for proposals for prevention and preparedness in Civil Protection projects under the UCPM (2014 and 2015).

The Neighbourhood South Countries (except Egypt, Israel and Syria) are also beneficiaries of the CBRN[10] Centres of Excellence initiative funded by the Instrument contributing to Stability and Peace.

Component 2 - Cybercrime:

Morocco is a priority country under the GLACY project financed by EU through the Instrument contributing to Stability and Peace. Under GLACY, the feasibility of capacity building activities on cybercrime legislation, training of judges on cybercrime and electronic evidence, law enforcement training, and public/private and international co-operation has already been demonstrated. The tools and materials developed and applied in that context could be adapted for use in other countries of this region.

GLACY will be followed by GLACY+ (Global Action on Cybercrime Extended) from 2016 to 2020. It is proposed that Morocco participates in the Cybercrime@South project with a focus on country-specific capacity building activities and regional activities involving the Neighbourhood South region, while at the same time it will continue to participate in GLACY+ as a regional hub for West Africa. This delineation will ensure non-duplication between the two EU-funded

[10] Chemical Biological Radiological Nuclear risks: http://www.cbrn-coe.eu/

projects. Morocco would thus serve as a link between the two projects and help share new tools and practices developed under GLACY+ with the countries participating in Cybercrime@South.

Furthermore, the project would benefit from the experience of joint EU/Council of Europe projects in the Eastern Partnership region (Cybercrime@EAP) and in South-Eastern Europe (iPROCEEDS under the Instrument of Pre-Accession) which cover public/private co-operation and the confiscation of proceeds from online crime. An annual meeting will gather the 3 projects in the same event, and joint communication activities will be developed. This cross-fertilisation will help draw the Southern Neighbourhood region into mainstream policies and strategies on cybercrime pursued by the EU and the Council of Europe.

There will be close co-operation with Interpol Global Complex for Innovation in Singapore. Partnerships will be established with the European Cybercrime Centre (EC3) and other partners, including EU Member States entities, mainly through GLACY+.

Coordination with the EU Member States is ensured through the Friends of Presidency Group for Cyber Issues.

Close contacts will be maintained with the ongoing Euromed Police IV and Euromed Justice IV projects[11], but also with United Nations Office on Drugs and Crime (UNODC), which has an ongoing cybercrime programme in Tunisia.

Component 3 – Interpol:

Interpol is the world's largest international police organisation, with 190 member countries and as such is a key partner for the EU and many other donors, in the field of operational police co-operation.

It also provides linkages to regional organisations such as Europol and the newly created AFRIPOL.

The European Union currently contributes to the funding of several different Interpol projects, including:

- WAPIS – West African Police Information System

- iArms III – Illicit Arms Records and Tracing Management System

- I-24/7 Extension – Jordan

Interpol is also closely involved in other EU-funded projects such as Fight against trafficking along the Heroine Route, Container Control Programme around the Black Sea and AIRCOP and Euromed Police IV.

3.3 Cross-cutting issues

Component 1 – Civil Protection:

Co-operation with the Neighbourhood aims not only to prevent, prepare and respond to disasters in these partner countries and the EU, but also to contribute to social and

[11] C(2014)5948 COMMISSION IMPLEMENTING DECISION of 25.8.2014 on the Annual Action Programme 2014 - Part 1 in favour of the ENI South countries to be financed from the general budget of the European Union, Annex 2.

political stability. Climate change adaptation will be factored into the project, as it will have a strong emphasis on disaster risk reduction and preparedness. The Sendai Framework for Disaster Risk Reduction emphasizes also the role of vulnerable groups (including women, children, youth older persons or persons with disabilities) and advocates for resilient communities and an inclusive and all-of-society disaster risk management. To this effect, awareness and understanding of cultural specificities and differences should also be taken into account.

Component 2 - Cybercrime:

The Commission will ensure that measures are implemented in accordance with international law, including international humanitarian law and in accordance with the EU Strategic Framework and Action Plan on Human Rights and Democracy. A human rights perspective will also be present in the measure on cybercrime, in accordance with the safeguards foreseen in the 2013 Cybersecurity Strategy of the European Union and the Budapest Convention on Cybercrime.

Amongst others, the cybercrime programme also contributes to a better protection of internet users against abuse and misuse. It also directly concerns the youth and women, victims in the field of sexual crimes.

Component 3 – Interpol:

Interpol continually strives to promote respect for and the observance of human right principles, as stated in its mandate. Secondly, Interpol ensures that human rights are respected during the processing of personal information. The oversight role is fulfilled by the General Secretariat itself and by the Commission for the Control of Interpol's Files, which is also responsible for processing requests for access to Interpol's files, including requests for correction or deletions.

By increasing the number of detections and interdictions, this component also indirectly contributes to a better protection of potential victims, mostly vulnerable groups such as in the trafficking of human beings and the smuggling of migrants.

4 DESCRIPTION OF THE ACTION

4.1 Objectives

Component 1 – Civil Protection:

The global objective is to contribute to increasing resilience and reducing the social, economic and environmental costs of natural and man-made disasters in the ENP South region.

The specific objectives are:

– National approaches to disaster management are further developed, based on prevention, mitigation, and preparedness rather than on response, with the involvement of all relevant governmental actors as well as of civil society stakeholders;

– Intra-regional, and where appropriate regional, co-ordination and co-operation is enhanced, in order to have coordinated responses of countries of the Mediterranean Basin affected by the same disaster; and institutional co-operation between the Union

Civil Protection Mechanism and the ENP South partner countries' civil protection agencies is strengthened.

Component 2 – Cybercrime:

The global objective of the project is to contribute to the prevention of and fight against cybercrime, in line with international human rights and rule of law standards and good practices.

The specific objective of the project is:

- The national legislations and institutional capacities on cybercrime and electronic evidence in the region of Southern Neighbourhood are strengthened.

Component 3 – Interpol:

The global objective of the project is to contribute to a better detection and interdiction of organised crime and terrorist individuals or groups.

The specific objectives of the project are:

- Information exchange and data collection is increased, on issues related to organised crime, terrorism, human smuggling and trafficking of small arms and human beings, using Interpol systems such as databases, the encrypted network and the specialised task forces;

- The quality of analytical reports is improved, for the beneficiary countries but also for Interpol, Europol, Eurojust and Frontex.

4.2 Expected results and main activities

Component 1 – Civil Protection:

The expected results are:

- Enhanced co-operation, exchange of good practices and support for capacity building in prevention actions (including risk assessment, risk management capability, risk prevention measures, risk mapping, early warning and awareness raising),

- Improved knowledge base on disaster risks and disaster prevention policies, and awareness raised on disaster prevention,

- Good practices are readily identified, shared and adopted by relevant stakeholders,

- A training network is established and maintained, effectively linking all relevant stakeholders.

To the maximum possible extent, the choice and design of the PPRD activities will be aligned with those provided by DG ECHO to priority ENP countries in the UCPM framework, and more broadly with the principles and approaches underlying the UCPM.

The main activities are:

- Launch a Technical Assistance Facility:

The Technical Assistance Facility will provide a maximum degree of flexibility in the selection of individual measures that are deployed to address common capacity

building needs identified by the ENI SPC within a demand-driven approach defined in the regional and national priorities and not provided by the activities below.

- Implement an Exchange Programme:

The Programme will give civil protection experts the opportunity to share experiences, gain valuable knowledge and strengthen operational skills by a system of exchange. Experts can either apply to go on an exchange mission, or civil protection organisations can invite expert(s).

- Provide Training courses:

The programme will offer a wide range of courses from basic training to high-level courses for future mission leaders, such as coaching on establishing national response teams, support the development of guidelines on receiving international teams (HNS) or sending national teams abroad. Training on gender mainstreaming and gender analysis in disaster risk management will be provided.

- Organise Joint Simulation Exercises:

Simulation exercises are fundamental to prepare civil protection teams to react fast when disasters occur. Exercises at European and Neighbourhood level, involving a number of countries at a time, contribute to enhancing collaboration in disaster preparedness across borders.

- Provide access to an online knowledge base and e-learning and organise workshops and conferences.

- Launch Call for proposals for Prevention and Preparedness projects.

The calls will be targeted to the specific needs of the region and sub region in full alignment with the UCPM calls.

Component 2 – Cybercrime:

Result 1: National criminal law frameworks reviewed, in line with the Budapest Convention on Cybercrime, including rule of law and human rights safeguards

Activities:

- Review of domestic legislation
- Support to domestic law drafting working groups
- Training activities on conditions and safeguards as well as data protection
- Regional meetings for the sharing of experience

Result 2: Specialised police and prosecution services and interagency co-operation strengthened

Activities:

- Review of institutional capacities for cybercrime investigations and prosecutions as well as computer forensics
- Advice, sharing experience and study visits on the establishment or strengthening of specialized services

- Support to law enforcement training and incorporation of the courses in the curricula of the training academies

- Support to standard operating procedures for the use of electronic evidence

- Promotion of interagency co-operation amongst cybercrime units, financial investigators and financial intelligence units in the search, seizure and confiscation of online crime proceeds

- Promotion of public/private co-operation, in particular on law enforcement and service provider co-operation on access to electronic evidence

Result 3: Modules on cybercrime and electronic evidence better mainstreamed into the curricula of judicial training institutions

Activities:

- Adaptation of training materials

- Training of trainers

- Support to delivery of courses at training academies and the mainstreaming of the courses into the curricula of training academies

Result 4: More efficient international co-operation

Activities:

- Review of rules, procedures and institutional capacities for international co-operation on cybercrime and electronic evidence

- Training and advice for 24/7 points of contact

- Support to participation in international initiatives

Result 5: Cybercrime and cybersecurity policies and strategies reviewed

Activities:

- Review of current policies/strategies and sharing of experience

- Workshops and advice on policies and strategies

Component 3 – Interpol:

The expected results are:

- Selected border posts equipped with the Interpol's secure global communications network (I-24/7),

- Increased information sharing through the further deployment of Interpol I24/7 and the correspondent databases,

- Increased data collection by Neighbourhood South countries

The main activities will be:

Promote the use of Interpol systems:

- Baseline study on the present use of Interpol databases in MENA

- Identification of the reasons for underutilisation

- Awareness campaigns for the promotion of a better use of existing available data and for an increased feeding of the databases (this is of particular importance especially in countries with multiple layers of agencies involved in law enforcement and rather reluctant to add information)

- Needs assessment for capacity building and training per country on the use of the Interpol systems (how to consult and how to feed the databases but also how to analyse the data and cooperate with the specialised task forces)

- Perform capacity building and specialised trainings (where necessary, these trainings will also tackle the issues of rule of law, human rights and data protection; where relevant, these trainings will also take into account co-operation with the different actors involved in the prevention of crime and protection and assistance of the victims, especially in the case of trafficking of human beings and smuggling of migrants)

Equipment of critical border posts (the material deployment of the I 24/7 should remain exceptional and should only target a limited number of critical border posts important at a regional level):

- Needs assessment for the deployment of equipment

- Analysis of the forecasted investment plans of the partner countries but also foreseen in ongoing and planned projects by bilateral or international donors

- Selection of critical border posts to be equipped and supply of equipment

- On the spot training in the newly equipped posts

Table-top exercises:

- Operations through table top exercises and if feasible joint cross-border operations based on the Interpol Spartacus Operation model. These table-top exercises will allow to analyse the effectiveness of the increased deployment of the Interpol systems: databases, encrypted networks and specialised task forces.

4.3 Intervention logic

Component 1 – Civil Protection:

Among all UCPM activities identified in the corresponding Decision, only some are open to the full participation of Neighbourhood countries (as defined in Art. 28.2).

Within the Mechanism, several service contracts managed and funded by ECHO are already ongoing, for example on training, expert exchange, improving the knowledge base, meetings, conferences and others, calls for proposals are launched for organising exercises, modules exercises, prevention and preparedness projects.

ECHO's Annual Work Plans (AWP) includes a financial provision for the implementation of the UCPM in third countries, but in principle priority ENP countries (Jordan, Algeria and Tunisia for the South) will be targeted. These countries were selected by ECHO based on their degree of commitment and progress vis-à-vis the UCPM.

In light of the above, the PPRD III project will be complementary to ECHO’s support as it will allow a more regional and sub-regional focus including:

- To provide support to non-priority ENP South countries,

- To provide support to all ENP South countries on activities outside the scope of Art 28.2 of the UCPM Decision. Such support will not be strictu sensu part of the UCPM, i.e. joint with EU MS, but it will be aligned with the UCPM principles and approaches,
- To organise (sub) regional activities.

In order to comply with individual requests from partner countries a Technical Assistance Facility will provide tailored capacity building in priority areas, through a maximum degree of flexibility in the selection of individual measures that are deployed to address common capacity building needs identified by the ENI SPC within a demand-driven approach.

The action may be implemented with EU Member States Agencies which shall compose a consortium with at least three Member States and one ENP civil protection authorities or agencies acting on a nation-wide basis as a central authority or central agency in the area of civil protection.

Component 2 – Cybercrime:

Under each result, activities will start with an assessment of capabilities and issues and will end with a performance review to determine progress made.

There will be a combination of regional and bilateral activities. Close coordination will thus be sought with EU Delegations and other organisations to avoid duplication of efforts and to make use of synergies with country-specific projects.

The project will build on achievements of the Cybercrime@EAP, iPROCEEDS, GLACY and GLACY+, as well as regional and bilateral ongoing actions.

Contrary to the EU-funded cybercrime projects in the Neighbourhood East and the Balkans, the approach is less ambitious in the Neighbourhood South. Many activities are about reviewing and assessing needs, advising, promoting and building capacity. While for example for Eastern Partner countries conditions for a structured process of public/private co-operation on cybercrime is underway and agreements can be concluded, the approach for the Southern Partner countries is more at the stage of awareness raising and identifying the first steps necessary to engage in such processes.

The project will apply a differentiated and phased approach.

Algeria, Jordan, Morocco and Tunisia could be considered priority countries which may benefit from the full range of support provided they have the necessary human rights and rule of law safeguards.

Co-operation with other countries would focus on the strengthening of legislation, human rights and rule of law conditions for cybercrime and electronic evidence followed by gradual involvement – if feasible – in the other project activities.

In this way, it should be possible to strengthen legal and institutional frameworks and practices, including rule of law and human rights safeguards, in some countries of this region with the ambition that they would serve as examples of good practice to others, fostering a regional dynamic for the promotion of due process compliant standards in addressing cybercrime, in line with the Budapest Convention provisions. This approach would help prevent the risk of law enforcement authorities benefiting

from training on investigative techniques without the necessary rule of law and human rights safeguards.

Component 3 – Interpol:

Increasing information exchange and data collection (objective 1) will require capacity building and further deployment of I24/7 and I-link in the Neighbourhood South partner countries.

Activities commence with an assessment of capabilities and needs in order to prepare an adapted capacity building programme and an investment plan where required.

Interpol will enhance the current activities of its Counter Terrorism Fusion Sub-directorate (CTF) responsible for the region, to serve the purpose of information sharing, identification of travel routes of terrorists, detection of firearms flows. The regional project "Al Qabdah", offers the partner countries, the EU Member States and the EU agencies (Europol, Eurojust, Frontex) additional possibilities to collect, analyse and share relevant information on terrorist groups (their membership and affiliates). The development of a virtual regional bureau for Middle East and North Africa (MENA) will become the first step of a standing regional bureau.

Interpol will also activate operational work to enhance detection capabilities of the routes used or potentially used by Foreign Terrorist Fighters (FTF) to reach the conflict zones (Syria, Iraq, Yemen and Libya) or by FTF "returnees" to reach the MENA countries or Europe.

The project will also contribute to the specialised task force ISON for smuggling of migrants.

5 IMPLEMENTATION

5.1 Financing agreement

In order to implement this action, it is not foreseen to conclude a financing agreement with the partner countries, 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 4.2 will be carried out and the corresponding contracts and agreements implemented, is 48 months for component 1 and 36 months for components 2 & 3.

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

5.3.1 Indirect management with a Member State agency

Component 1 (Civil Protection) of this action may be implemented in indirect management with Member State agencies in accordance with Article 58(1)(c) of Regulation (EU, Euratom) No 966/2012.

This implementation entails capacity building, technical assistance, training, exchange of experts but also launching call for proposals for the implementation of joint exercises, prevention and preparedness projects.

This implementation is justified because the project requires the involvement of EU Member States Civil Protection Agencies which on their own do not necessarily have the project management capacity.

The entrusted entity would carry out budget-implementation tasks necessary to achieve the results outlined in section 4.2.

The entrusted entity will be selected after negotiations resulting from a call for manifestation of interest addressed to all EU Member States agencies eligible for indirect management (from the list of the pillar-assessed agencies).

5.3.2 Indirect management with an international organisation

Component 2 (Cybercrime) of this action may be implemented in indirect management with the Council of Europe in accordance with Article 58(1)(c) of Regulation (EU, Euratom) No 966/2012.

This implementation entails to strengthen the capacities of the Neighbourhood South partner countries to apply legislation on cybercrime and electronic evidence and enhance their abilities for effective international co-operation in this area.

This implementation is justified because the Council of Europe has a unique expertise in the domains the proposed action intends to address and falls within the call of the 2013 EU Cyber Security Strategy to engage with international partners and organisations to support global capacity-building. Having more than 10 years of experience in cybercrime capacity building efforts, as well as being the guardian of the Budapest Convention on Cybercrime, the Council of Europe has the required know-how and capacity to undertake such initiatives in third countries. The entrusted entity would carry out budget-implementation tasks necessary to achieve the results outlined in section 4.2.

Component 3 (Interpol) of this action may be implemented in indirect management with Interpol in accordance with Article 58(1)(c) of Regulation (EU, Euratom) No 966/2012.

This implementation entails capacity building and further deployment of I24/7 in the Neighbourhood South partner countries.

This implementation is justified because Interpol is the world’s largest international police organisation (190 member countries). Its mission is to facilitate international police co-operation even where diplomatic relations do not exist between the countries concerned, and to provide support and assistance to all services, organisations and authorities working to prevent and fight crime.

The entrusted entity would carry out budget-implementation tasks necessary to achieve the results outlined in section 4.2.

5.3.3 Changes from indirect to direct management mode due to exceptional circumstances

In case of exceptional circumstances, should the above mentioned modality not be possible for component 3, it could be implemented in direct management through a direct award of a grant.

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, subject to the following provisions.

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 Component 1 – Indirect management with a Member State agency	5,000,000	
5.3.2 Component 2 – Indirect management with the Council of Europe	3,000,000	
5.3.2 Component 3 – Indirect management with Interpol	3,000,000	
Totals	11,000,000	

5.6 Organisational set-up and responsibilities

Component 1 (Civil Protection) may be directly implemented by a group of EU Member State Civil Protection Agencies. The Commission will manage the agreement in close liaison with the EU Delegations in the ENP South partner countries.

A Steering Committee will be established with the participation of the relevant Commission services as well as representatives from the Civil Protection Authorities and the focal points established under this project. ECHO will be closely involved in the design and monitoring of project activities.

Component 2 (Cybercrime) will be directly implemented by the Council of Europe.

An appropriate management structure will be established to ensure the coherence of the project and synergies with the similar projects ongoing in the Neighbourhood East, the Western Balkans and the global project GLACY+. The Council of Europe will be responsible for the overall management of the project.

Component 3 (Interpol) will be directly implemented by Interpol. Interpol will be responsible for the overall management of the project in close relation with the National Central Bureaus of the partner countries (NCB).

5.7 Performance monitoring and reporting

The day-to-day technical and financial monitoring of the implementation of this action will be a continuous process and part of the implementing partners' responsibilities. To this aim, the implementing partners 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 importance of the action, an ex-post evaluation will be carried out for this action or its components via independent consultants contracted by the Commission.

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 these are innovative approaches.

The Commission shall inform the implementing partners at least 3 months in advance of the dates foreseen for the evaluation missions. The implementing partners 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 countries and other key stakeholders. The implementing partners and the Commission shall analyse the conclusions and recommendations of the evaluations and, where appropriate, in agreement with the partner countries, 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 countries, 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.

6 PRE-CONDITIONS

Not applicable

APPENDIX - INDICATIVE LOGFRAME MATRIX

	Results chain	Indicators	Baselines (incl. reference year)	Targets (incl. reference year)	Sources and means of verification	Assumptions
Overall objective: Impact	**C1: Civil Protection** - contribute to increasing resilience and reducing the social, economic and environmental costs of natural and man-made disasters **C2: Cyber** - prevent and fight cybercrime in line with human rights and rule of law **C3: Interpol** - better detect and interdict organised crime and terrorist individuals or groups by increasing the use of existing tools for data collection and sharing	C1: Civil protection - progress towards Sendai Framework targets C2: Cyber - number of domestic and international prosecutions and cases adjudicated on cybercrime in line with rule of law and human rights C3: Interpol - number of hits worldwide on data SLTD provided by Neighbourhood South countries	C1: Civil protection - to be defined with DG ECHO in the preparatory and implementation phase C2: Cyber - to be defined by Council of Europe in the preparatory phase C3: Interpol - data subject to confidentiality at this stage - to be defined by Interpol in the preparatory phase	C1: Civil protection - to be defined with DG ECHO in the preparatory and implementation phase C2: Cyber - to be defined by Council of Europe in the preparatory phase C3: Interpol - increase of 20%	C1: Civil protection DG ECHO reports EM-DAT website (the international disaster database) UNISDR reports C2: Cyber Project progress reviews C3: Interpol Statistics provided by Interpol Information Systems and Technology Directorate	

Specific objective(s): Outcome(s)	**C1: Civil Protection** - national approaches to disaster management are further developed, based on prevention, mitigation, and preparedness rather than on response - intra-regional and regional co-ordination and co-operation is enhanced and institutional co-operation between the UCPM and the ENP South partner countries is strengthened **C2: Cyber** - strengthen the capacities of the countries to apply legislation on cybercrime and electronic evidence and enhance their abilities for effective international co-operation **C3: Interpol** - increase information exchange on issues related to organised crime, terrorism, smuggling of migrants, trafficking of human beings and trafficking of small arms and increase data collection - increase the quantity and quality of analytical reports	C1: Civil protection - availability of operational DRR National Action Plans per country - number of active associated partnerships in place C2: Cyber - number of countries signing the Budapest Convention or applying legislation in line with the Budapest Convention C3: Interpol - number of hits in Europe on data provided by Neighbourhood South countries - number of new available data from the Neighbourhood South - number of contributions of ENP South countries to the specialised task forces	C1: Civil protection - 1 - 0 C2: Cyber - 0 ratifications - 2 applying legislation C3: Interpol - data subject to confidentiality at this stage - to be defined by Interpol in the preparatory phase - to be defined by Interpol in the preparatory phase	C1: Civil protection - + 3 - + 3 C2: Cyber - +2 ratifying - +2 applying legislation C3: Interpol - increase of 20%	C1: Civil protection DG ECHO reports MoU with DG ECHO C2: Cyber Council of Europe Treaty Office C3: Interpol Statistics provided by Interpol Information Systems and Technology Directorate Analytical reports provided by Europol and Frontex	Partner countries are willing to reach a higher degree of co-operation within the region, intra region and with EU.

Outputs	**C1: Civil protection** - enhanced co-operation, exchange of good practices and support for capacity building in prevention actions - improved knowledge base on disaster risks and disaster prevention policies and good practices are readily identified, shared and adopted - training network is established and maintained **C2: Cyber** - national criminal law frameworks reviewed, in line with the Budapest Convention on Cybercrime, including rule of law safeguards - specialised police and prosecution services and interagency co-operation strengthened - modules on cybercrime and electronic evidence better mainstreamed into the curricula of judicial training institutions - more efficient international co-operation - cybercrime and cybersecurity policies and strategies reviewed **C3: Interpol** - selected border posts equipped with the Interpol's secure global communications network (I-24/7), - increased information sharing through the further deployment of Interpol I24/7 and the correspondent databases, - increased data collection Neighbourhood South countries	C1: Civil protection - number of joint operations including non-associated countries - online knowledge base available also for non-associated countries - number of readily available training packages available also for non-associated countries C2: Cyber - number of draft laws or amendments in line with the Budapest Convention - availability of training modules - number of cybercrime strategies and policies including interagency co-operation and international co-operation C3: Interpol (in the Neighbourhood South countries) - expansion of Interpol I 24/7 beyond National Central Bureaus - number of records fed into the database SLTD - number of searches in SLTD - number of hits in SLTD	C1: Civil protection - 0 - no base available - no access C2: Cyber - to be defined by Council of Europe in the preparatory phase C3: Interpol - data per country subject to confidentiality at this stage - to be defined by Interpol in the preparatory phase	C1: Civil protection - + 4 - base available on a permanent basis - acces to online training C2: Cyber - to be defined by Council of Europe in the preparatory phase C3: Interpol - for the deployment of I 24/7: at least 5 critical border posts - concerning the use: for MENA countries + 20% above the yearly worldwide average statistical increase	C1: Civil protection DG ECHO reports C2: Cyber Project progress reviews C3: Interpol Individual statistics per country provided by Interpol Information Systems and Technology Directorate	Partner countries will ensure sustainability and durability to the respective projects by making available the necessary human, financial and material resources.